Trend Micro Apex Central™

Patch 10

Handbuch für Widget- und Richtlinienverwaltung

Zentralisierte Sicherheitsverwaltung für Endpunkte

Trend Micro Incorporated behält sich das Recht vor, Änderungen an diesem Dokument und den hierin beschriebenen Produkt ohne Vorankündigung vorzunehmen. Lesen Sie vor der Installation und Verwendung von Produkt die Readme-Dateien, die Anmerkungen zu dieser Version und/oder die neueste Version der auf der Trend Micro Website verfügbaren Dokumentation durch:

http://docs.trendmicro.com/de-de/enterprise/apex-central.aspx

Trend Micro, das Trend Micro T-Ball-Logo, Trend Micro Apex Central, Trend Micro Apex One, Control Manager und OfficeScan sind Marken oder eingetragene Marken von Trend Micro Incorporated. Alle anderen Produkt- oder Firmennamen können Marken oder eingetragene Marken ihrer Eigentümer sein.

Copyright © 2024. Trend Micro Incorporated. Alle Rechte vorbehalten.

Dokument-Nr.: APGM99927/240733

Release-Datum: Dezember 2019

Geschützt durch U.S. Patent-Nr.: 5.623.600; 5.889.943; 5.951.698; 6.119.165

Diese Dokumentation enthält eine Beschreibung der wesentlichen Funktionen von Produkt und/oder Installationsanweisungen für eine Produktionsumgebung. Lesen Sie die Dokumentation vor der Installation und Verwendung von Produkt.

Detaillierte Informationen zur Verwendung bestimmter Funktionen in Produkt können Sie in der Trend Micro Online-Hilfe und/oder der Trend Micro Knowledge Base finden.

Trend Micro ist stets bemüht, die Dokumentation zu verbessern. Setzen Sie sich mit uns in Verbindung, wenn Sie Fragen, Kommentare oder Vorschläge zu diesem oder einem anderen Trend Micro Dokument haben: docs@trendmicro.com.

Inhaltsverzeichnis

Vorwort

Vorwort 1
Dokumentation 2
Zielgruppe 3
Dokumentationskonventionen 3
Begriffe 4

Teil I: Einführung

Kapitel 1: Das Dashboard

Info über das Dashboard 1-2
Registerkarten und Widgets 1-2
Mit Registerkarten arbeiten 1-2
Arbeiten mit Widgets 1-4
Registerkarte Sicherheitsstatus 1-6
Konformitätsindikatoren 1-7
Kritische Bedrohungen 1-8
Behobene Ereignisse 1-9
Sicherheitsstatus-Diagramm 1-10
Einzelheiten Sicherheitslage Bereich 1-11
Registerkarte „Zusammenfassung“ 1-15
Kritische Bedrohungen – Widget 1-15
Benutzer mit Bedrohungen – Widget 1-18
Endpunkte mit Bedrohungen – Widget 1-20
Apex Central – häufigste Bedrohungen – Widget 1-21
Produktkomponentenstatus – Widget 1-22
Verbindungsstatus des Produkts – Widget 1-24
Ransomware-Prävention – Widget 1-25

Registerkarte 'Prävention vor Datenverlust' 1-25
DLP-Vorfallstrends nach Benutzer – Widget 1-26
DLP-Vorfälle nach Schweregrad und Status – Widget 1-27
DLP-Vorfälle nach Benutzer – Widget 1-28
DLP-Vorfälle nach Kanal – Widget 1-29
DLP-Vorlagenübereinstimmungen – Widget 1-31
Häufigste Quellen für DLP-Vorfälle – Widget 1-31
DLP-Richtlinienverstoß – Widget 1-32
Registerkarte 'Konformität' 1-32
Einhaltung von Richtlinien für Produktanwendung – Widget 1-32
Produktkomponentenstatus – Widget 1-34
Verbindungsstatus des Produkts – Widget 1-36
Verbindungsstatus des Agents – Widget 1-37
Bedrohungsstatistik-Registerkarte 1-38
Apex Central – häufigste Bedrohungen – Widget 1-38
Apex Central Bedrohungsstatistiken – Widget 1-39
Bedrohungserkennungsergebnisse – Widget 1-42
Erkannte Richtlinienverstöße – Widget 1-43
C&C-Callback-Ereignisse – Widget 1-44

Kapitel 2: Richtlinienverwaltung

Richtlinienverwaltung 2-3
Neue Richtlinie erstellen 2-3
Filtern nach Kriterien 2-7
Endpunkte gefilterten Richtlinien zuweisen 2-9
Richtlinienziele angeben 2-11
Bezeichnungen 2-13
Mit Einstellungen für übergeordnete Richtlinien arbeiten 2-13
Richtlinieneinstellungen kopieren 2-17
Richtlinieneinstellungen übernehmen 2-18
Richtlinien ändern 2-20
Richtlinien importieren und exportieren 2-23
Richtlinie löschen 2-24

Richtlinienbesitzer ändern 2-25
Grundlegendes zur Richtlinienliste 2-26
Richtlinienliste neu ordnen 2-30

Richtlinienstatus 2-31

Kapitel 3: Richtlinienressourcen

Application Control-Kriterien 3-2

Definieren von Kriterien für erlaubte Anwendungen 3-4
Kriterien für gesperrte Anwendungen definieren 3-7
Anwendung Übereinstimmungsmethoden 3-9
Anwendungsverbreitungsliste 3-9
Dateipfade 3-10
Beispielverwendung des Dateipfads 3-12
Zertifikate 3-14
Hash-Werte 3-15

Prävention vor Datenverlust 3-16

Datenbezeichnertypen 3-17
Ausdrücke 3-18
Vordefinierte Ausdrücke 3-18
Einstellungen für vordefinierte Ausdrücke anzeigen 3-19
Benutzerdefinierte Ausdrücke 3-19
Kriterien für benutzerdefinierten Ausdruck 3-20
Benutzerdefinierte Ausdrücke erstellen 3-21
Benutzerdefinierte Ausdrücke importieren 3-23
Dateiattribute 3-23
Eine Dateiattributliste erstellen 3-24
Eine Dateiattributliste importieren 3-25
Schlüsselwörter 3-26
Vordefinierte Schlüsselwortlisten 3-26
Wie funktionieren Schlüsselwortlisten 3-27
Bedingung "Anzahl der Schlüsselwörter" 3-27
Abstandsbedingung 3-27
Benutzerdefinierte Schlüsselwortlisten 3-28
Kriterien für benutzerdefinierte Schlüsselwortliste 3-28

Schlüsselwortlisten erstellen 3-30
Schlüsselwortlisten importieren 3-32
Vorlagen für 'Prävention vor Datenverlust' 3-33
Vordefinierte DLP-Vorlagen 3-33
Benutzerdefinierte DLP-Vorlagen 3-34
Bedingungsanweisungen und logische pperatoren 3-34
Vorlagen erstellen 3-35
Vorlagen importieren 3-37
Regeln zum Eindringschutz 3-38
Eigenschaften der Regeln zum Eindringschutz 3-40
Zulässige Geräte – Gerätesteuerung 3-42

Teil II: Apex Central Widgets

Kapitel 4: Apex Central Dashboard-Widgets

Apex Central – häufigste dateibasierte Bedrohungen – Widgets 4-2
Endpunktschutzüberprüfung – Widget 4-3
Hosts mit C&C-Callback-Versuchen – Widget 4-4
Richtlinienstatus 4-5
Schnellstart 4-6
Eindeutige infizierte Hosts im Zeitverlauf – Widget 4-7

Teil III: Apex One Widgets

Kapitel 5: Apex One Dashboard-Widgets

Erkennungs-Widget der Angriffserkennung 5-2
Widget für schnelle Untersuchung 5-2
Top gesperrte Anwendungen 5-3

Top Endpunkte, die von IPS-Ereignissen betroffen sind Widget 5-3
Häufigste IPS-Angriffsquellen 5-3
Top-IPS-Ereignisse 5-4
Top verletzte Application Control-Kriterien 5-5

Teil IV: Apex One Server-Richtlinieneinstellungen

Kapitel 6: Apex One Server-Richtlinieneinstellungen

Endpoint Sensor-Servereinstellungen konfigurieren 6-2

Teil V: Apex One Security Agent Richtlinien

Kapitel 7: Agentenkonfigurationen

Update Agents 7-2
Security Agents als Update-Agents zuweisen 7-2
Berechtigungen und andere Einstellungen 7-2
Agent-Berechtigungen konfigurieren 7-3
Andere Agent-Einstellungen konfigurieren 7-9
Security Agent Eigenschutz 7-12
Security Agent-Dienste schützen 7-12
Dateien im Security Agent-Installationsordner schützen 7-13
Security Agent-Registrierungsschlüssel schützen 7-14
Security Agent-Prozesse schützen 7-14
Cache-Einstellungen für die Suche 7-15
Digitaler Signatur-Cache 7-15
Cache für die On-Demand-Suche 7-16
POP3 Mail Scan 7-18
Zusätzliche Diensteinstellungen 7-19
Konfigurieren zusätzlicher Security Agent-Dienste 7-20

Kapitel 8: Application Control-Richtlinieneinstellungen

Application Control 8-2
Konfigurieren der Einstellungen zur Anwendungssteuerung (Agent) 8-2

Kapitel 9: Einstellungen der Verhaltensüberwachungs-Richtlinie

Verhaltensüberwachung 9-2
Verhaltensüberwachungsregeln 9-2
Ausnahmeliste für Verhaltensüberwachung 9-11
Ausnahmeliste, Unterstützung von Platzhaltern 9-11
Ausnahmeliste, Unterstützung von Umgebungsvariablen 9-17
Regeln und Ausnahmen der Verhaltensüberwachung konfigurieren 9-17

Kapitel 10: Anti-Malware-Scans

Allgemeine Einstellungen 10-2
Richtlinien für das Wechseln der Suchmethoden 10-3
Echtzeitsuche 10-5
Einstellungen der Echtzeitsuche konfigurieren 10-5
Echtzeitsuche: Registerkarte "Ziel" 10-6
Echtzeitsuche: Registerkarte "Aktion" 10-11
Echtzeitsuche: Registerkarte "Suchausschluss" 10-15
Zeitgesteuerte Suche 10-18
Einstellungen für zeitgesteuerte Suche konfigurieren .. 10-18
Zeitgesteuerte Suche: Registerkarte "Ziel" 10-19
Zeitgesteuerte Suche: Registerkarte "Aktion" 10-25
Zeitgesteuerte Suche: Registerkarte "Suchausschluss" 10-29
Manuelle Suche 10-32
Manuelle Suche: Registerkarte "Ziel" 10-33
Manuelle Suche: Registerkarte "Aktion" 10-36
Manuelle Suche: Registerkarte "Suchausschluss" 10-40

Jetzt durchsuchen 10-43
Einstellungen von Jetzt durchsuchen konfigurieren 10-43
Jetzt durchsuchen: Registerkarte "Ziel" 10-44
Jetzt durchsuchen: Registerkarte "Aktion" 10-47
Jetzt durchsuchen: Registerkarte "Suchausschluss" 10-51
Suchaktionen 10-54
ActiveAction 10-54
Aktionen bei der benutzerdefinierten Suche 10-56
Quarantäne-Verzeichnis 10-57
Dateien, die nicht gesäubert werden können 10-59
Mit Trojanern infizierte Dateien 10-62
Mit Würmern infizierte Dateien 10-62
Infizierte, schreibgeschützte Dateien 10-63
Kennwortgeschützte Dateien 10-63
Sicherungsdateien 10-63
Unterstützung der Suchausschlüsse 10-63
Trend Micro Produktverzeichnis, Ausschlüsse 10-63
Ausnahmen mit Platzhaltern 10-64

Kapitel 11: Einstellungen der Web-Reputation-Richtlinie

Web Reputation 11-2
Eine Web-Reputation-Richtlinie konfigurieren 11-2
Unterstützung der HTTPS-URL-Suche 11-8

Kapitel 12: Schutz vor unbekannten Bedrohungen

Vorausschauendes Maschinenlernen 12-2
Konfigurieren der Einstellungen für das Vorrausschaunde Maschinenlernen 12-5
Konfigurieren der Einstellungen für die Exemplar Zusendung 12-8
Verdächtige Verbindungseinstellungen konfigurieren 12-8

Kapitel 13: Einstellungen der Gerätesteuerungsrichtlinien

Gerätesteuerung 13-2
Einstellungen der Gerätesteuerung konfigurieren 13-2
Berechtigungen für Geräte 13-6
Unterstützung von Platzhalterzeichen für die Liste zulässiger Programme der Gerätesteuerung 13-9
Anbieter der digitalen Signatur festlegen 13-10

Kapitel 14: Ausnahmen

Liste der vertrauenswürdigen Programme 14-2
Liste der vertrauenswürdigen Programme konfigurieren 14-2
Regelausnahmen 14-3
Konfigurieren von Ausnahmeregeln 14-4
Liste der zulässigen Spyware/Grayware 14-5
Die Liste der zulässigen Spyware/Grayware verwalten ... 14-5

Kapitel 15: Richtlinieneinstellungen für Endpoint Sensor

Endpoint Sensor 15-2
Konfigurieren von Einstellungen für Endpoint Sensor 15-2

Kapitel 16: Vulnerability Protection – Policy-Einstellungen

Vulnerability Protection 16-2
Konfigurieren der Einstellungen für den Vulnerability Protection 16-2
Erweiterte Protokollierungsrichtlinienmodi 16-6

Teil VI: Apex One-Richtlinien für die Prävention vor Datenverlust

Kapitel 17: Apex One Data Discovery Dashboard-Widgets

Wichtigste Richtlinienfunde für vertrauliche Dateien – Widget 17-2

Die wichtigsten Endpunkte mit vertraulichen Dateien – Widget 17-4

Häufigste Übereinstimmungen für Data Discovery-Vorlagen – Widget 17-6

Häufigste Dateien mit vertraulichen Dateien – Widget 17-7

Kapitel 18: Apex One Einstellungen für die Datenerkennungsrichtlinie

Data Discovery-Richtlinien erstellen 18-2

Kapitel 19: Apex One Einstellungen der Richtlinien für 'Prävention vor Datenverlust'

Prävention vor Datenverlust (Data Loss Prevention, DLP) 19-2

Richtlinie für die Prävention vor Datenverlust konfigurieren 19-3

Regeln für die Funktion "Prävention vor Datenverlust" konfigurieren 19-5

Übertragungsumfang und -ziele für Netzwerkkanäle 19-7

Netzwerkkanäle 19-8

E-Mail-Clients 19-8

System- und Anwendungskanäle 19-10

Gerätelisten-Tool 19-10

Das Gerätelisten-Tool ausführen 19-11

Aktionen der Funktion "Prävention vor Datenverlust" 19-11

Ausnahmen für Prävention vor Datenverlust 19-15

Nicht überwachte und überwachte Ziele definieren 19-15

übertragungsumfang: Alle übertragungen 19-16

übertragungsumfang: Nur übertragungen außerhalb des lokalen Netzwerks 19-18

Dekomprimierungsregeln 19-19

Teil VII: Apex One (Mac)-Widgets und Richtlinien

Kapitel 20: Apex One (Mac) Dashboard-Widgets

Leistungsindikatoren-Widget 20-2
Leistungsindikatoren konfigurieren 20-2
Widget-Einstellungen konfigurieren 20-3

Kapitel 21: Apex One (Mac)-Richtlinieneinstellungen

Anti-Malware-Suchen 21-2
Allgemeine Einstellungen 21-2
Suchmethoden im Vergleich 21-3
Wechsel von der intelligenten Suche zur herkömmlichen Suche 21-4
Wechsel von der herkömmlichen Suche zur intelligenten Suche 21-6
Echtzeitsuche 21-8
Einstellungen der Echtzeitsuche konfigurieren 21-8
Echtzeitsuche: Registerkarte "Ziel" 21-9
Echtzeitsuche: Registerkarte "Aktion" 21-10
Unterstützte komprimierte Dateitypen 21-11
Suchaktionen 21-12
Manuelle Suche 21-14
Einstellungen für manuelle Suche konfigurieren ... 21-15
Manuelle Suche: Registerkarte "Ziel" 21-15
Manuelle Suche: Registerkarte "Aktion" 21-17
Unterstützte komprimierte Dateitypen 21-17
Suchaktionen 21-18
Zeitgesteuerte Suche 21-20
Einstellungen für zeitgesteuerte Suche konfigurieren 21-21
Zeitgesteuerte Suche: Registerkarte "Ziel" 21-21
Zeitgesteuerte Suche: Registerkarte "Aktion" ... 21-23
Unterstützte komprimierte Dateitypen 21-25
Suchaktionen 21-26

Advanced Threat Protection 21-28
Einstellungen für Vorausschauendes Maschinenlernen 21-28
Web Reputation 21-29
Web-Reputation-Einstellungen konfigurieren 21-29
Listen genehmigter und gesperrter URLs konfigurieren 21-32
Gerätesteuerung 21-33
Einstellungen der Gerätesteuerung konfigurieren . 21-34
Berechtigungen für Speichergeräte 21-35
Erkennung und Reaktion 21-36
Endpoint Sensor 21-36
Konfigurieren von Einstellungen für Endpoint Sensor 21-36
Ausnahmen 21-37
Suchausschlüsse 21-37
Suchausschlusslisten konfigurieren 21-37
Ausnahmelisten 21-41
Liste der vertrauenswürdigen Programme konfigurieren 21-41
Agent-Konfigurationen 21-43
Update-Einstellungen 21-43
Einschränkungen bei reinen IPv6-Agents 21-45
Update-Einstellungen für Agent konfigurieren 21-46
Cache-Einstellungen für die Suche 21-47
Berechtigungen und andere Einstellungen 21-48
Geschützte Security Agent Dateien 21-49

Teil VIII: Deep Discovery Widgets und Richtlinien

Kapitel 22: Deep Discovery Analyzer- und Email Inspector-Dashboard (Widgets)

Deep Discovery Analyzer (Widgets) 22-2
Virtual Analyzer – Überblick – Widget 22-2

Deep Discovery Email Inspector (Widgets) 22-3
E-Mail-Nachrichten mit komplexen Bedrohungen – Widget 22-3
Die häufigsten E-Mail-Empfänger komplexer Bedrohungen – Widget 22-3

Kapitel 23: Integration und Richtlinieneinstellungen für Deep Discovery Inspector

Übersicht über die Integration von Deep Discovery Inspector 23-2
Von Deep Discovery Inspector betroffene Hosts – Widget 23-4
Von Deep Discovery Inspector betroffene Hostfunde 23-5
Deep Discovery Inspector – Systemstatus – Widget 23-7
Richtlinieneinstellungen für Deep Discovery Inspector 23-10
Liste 'Verweigern'/Liste 'Zulassen' 23-10
Benutzerdefinierte Liste 'Verweigern' erstellen 23-11
Benutzerdefinierte Liste 'Zulassen' erstellen 23-11
Benutzerdefinierte Listen 'Verweigern' oder 'Zulassen' importieren/exportieren 23-12
Überwachte Netzwerkgruppen hinzufügen 23-12
Registrierte Dienste hinzufügen 23-14
Einstellungen für Virtual Analyzer konfigurieren 23-15

Teil IX: Deep Security Manager Widgets

Kapitel 24: Deep Security Manager Dashboard Widgets

Deep Security – Anti-Malware-Ereignisverlauf – Widget 24-2
Deep Security – Anti-Malware-Status (Malware) – Widget 24-2
Deep Security – (erkannte) Aktivität des Anwendungstyps – Widget 24-4
Deep Security – (verhinderte) Aktivität des Anwendungstyps – Widget 24-5

Deep Security – Überblick über die Komponenten – Widget 24-6

Deep Security – Funktionsübersicht – Widget 24-7

Deep Security – (erkannte) Firewall-Aktivität – Widget 24-9

Deep Security – (verhinderte) Firewall-Aktivität – Widget 24-9

Deep Security – Firewall-Ereignisverlauf – Widget 24-10

Deep Security – Aktivität der Integritätsüberwachung – Widget 24-11

Deep Security – Ereignisverlauf der Integritätsüberwachung – Widget 24-12

Deep Security – Ereignisverlauf des Eindringschutzes – Widget 24-13

Deep Security – (erkannte) IPS-Aktivität – Widget 24-14

Deep Security – (verhinderte) IPS-Aktivität – Widget 24-15

Deep Security – Protokollinspektionsaktivität – Widget 24-15

Deep Security – Ereignisverlauf der Protokollinspektion – Widget 24-16

Deep Security – Ereignisverlauf der Aufklärungssuche – Widget 24-17

Deep Security – Statusüberblick – Widget 24-18

Deep Security – Web-Reputation-Ereignisverlauf – Widget . 24-20

Deep Security – Aktivität der Web-Reputation-URLs – Widget 24-21

Teil X: Endpoint Application Control – Widgets und Richtlinien

Kapitel 25: Endpoint Application Control-Dashboard – Widgets

Endpoint Application Control – Wichtigste Leistungsindikatoren – Widget 25-2

Endpoint Application Control Regelverwaltung 25-7

Endpoint Application Control-Benutzer und -Endpunkte – Zusammenfassung – Widget 25-8

Endpoint Application Control-Anwendungs-, Regel- und Richtlinienereignisse – Widget 25-13

Kapitel 26: Endpoint Application Control – Richtlinieneinstellungen

Richtlinienregeln 26-2

Protokollierung von Richtlinien 26-3

Richtlinienbereitstellung 26-5

Policy Server-Verbindung 26-6

Richtlinien – Benutzererlebnis 26-7

Teil XI: Endpoint Encryption-Widgets und -Richtlinien

Kapitel 27: Endpoint Encryption-Dashboard-Widgets

Endpoint Encryption Benutzer 27-2

Endpoint Encryption Geräte 27-9

Full Disk Encryption Status 27-15

Erfolglose Anmeldeversuche an Endpoint Encryption-Geräten 27-18

Erfolglose Anmeldeversuche von Endpoint Encryption-Benutzern 27-20

Endpoint Encryption Geräte-Sperre 27-22

Bericht über Verstöße gegen die Endpoint Encryption Sicherheit 27-24

Kapitel 28: Endpoint Encryption-Richtlinieneinstellungen

Authentifizierungsübersicht 28-2

Endpoint Encryption Benutzerregeln konfigurieren 28-6
Full Disk Encryption Regeln konfigurieren 28-9
File Encryption Regeln konfigurieren 28-12
Allgemeine Regeln für Richtlinien konfigurieren 28-15
Gruppen zu Apex Central migrieren 28-20

Teil XII: Endpoint Sensor-Widgets und Richtlinien

Kapitel 29: Trend Micro Endpoint Sensor-Dashboard-Widgets

Endpoint Sensor-Untersuchung 29-2
Intelligente Überwachung, Übersicht nach Host 29-4
Kritischste Bedrohungen nach Verweilzeit – Widget 29-5

Kapitel 30: Trend Micro Endpoint Sensor Server-Integration und Richtlinieneinstellungen

Endpoint Sensor-Integration 30-2
Bei Apex Central registrieren 30-2
Endpoint Sensor-Widgets hinzufügen 30-3
Apex Central zur Statusüberprüfung verwenden 30-5
Widget „Endpoint Sensor-Untersuchung“ verwenden 30-6
Automatische Updates verwenden 30-7
Trend Micro Endpoint Sensor-Richtlinie 30-9
Server für die Richtlinienbereitstellung vorbereiten 30-9
Richtlinien erstellen und verteilen 30-10
Überwachungsregeln verwalten 30-10
Übermittlungseinstellungen verwalten 30-13

Teil XIII: InterScan-Sicherheitsrichtlinien

Kapitel 31: Richtlinieneinstellungen für InterScan Messaging Security Suite

IMSS-Regeln 31-2

IMSS-Regeln hinzufügen 31-2

Schritt 1: Regelnamen festlegen 31-3
Schritt 2: Empfänger und Absender auswählen 31-3
Ausnahmen konfigurieren 31-4
Sternchen als Platzhalterzeichen verwenden 31-5
Schritt 3: Vorlagen auswählen 31-6
Schritt 4: Aktionen auswählen 31-6

Vorhandene IMSS-Regeln ändern 31-7

IMSS-Regeln löschen 31-8

Kapitel 32: Richtlinieneinstellungen für InterScan Messaging Security Virtual Appliance

IMSVA-Regeln 32-2

IMSVA-Regeln hinzufügen 32-2

Schritt 1: Regelnamen festlegen 32-3
Schritt 2: Empfänger und Absender auswählen 32-3
Ausnahmen konfigurieren 32-4
Sternchen als Platzhalterzeichen verwenden 32-5
Schritt 3: Vorlagen auswählen 32-6
Schritt 4: Aktionen auswählen 32-6

Vorhandene IMSVA-Regeln ändern 32-7

IMSVA-Regeln löschen 32-7

Kapitel 33: Richtlinieneinstellungen für InterScan Web Security Suite

Regelliste für die Funktion 'Prävention vor Datenverlust' 33-2

Schritt 1: Regelnamen festlegen 33-2
Schritt 2: Konten auswählen 33-3
Schritt 3: Zu sperrende Vorlagen zur Einhaltung von Richtlinien auswählen 33-3

Schritt 4: Zu überwachende Vorlagen zur Einhaltung von Richtlinien auswählen 33-4

Kapitel 34: Richtlinieneinstellungen für InterScan Web Security Virtual Appliance

Regelliste für die Funktion 'Prävention vor Datenverlust' 34-2

Schritt 1: Regelnamen festlegen 34-2
Schritt 2: Konten auswählen 34-3
Schritt 3: Zu sperrende Vorlagen zur Einhaltung von Richtlinien auswählen 34-3
Schritt 4: Zu überwachende Vorlagen zur Einhaltung von Richtlinien auswählen 34-4

Teil XIV: ScanMail for Microsoft Exchange – Richtlinien

Kapitel 35: ScanMail for Microsoft Exchange – Richtlinieneinstellungen

Richtlinie für die Prävention vor Datenverlust konfigurieren 35-2

Konten auswählen 35-2
DLP-Ziele konfigurieren 35-3
DLP-Aktionen konfigurieren 35-4
DLP-Benachrichtigungen konfigurieren 35-5
DLP-Richtlinie aktivieren 35-6

Teil XV: Widgets für Smart Protection Server

Kapitel 36: Dashboard-Widgets für Smart Protection Server

Aktive Benutzer der File Reputation 36-2

Aktive Benutzer der Web Reputation 36-2

Bericht über HTTP-Datenverkehr der File Reputation 36-3

Bericht über HTTP-Datenverkehr der Web Reputation 36-3

Echtzeitsuche - Status 36-4
Die 10 am häufigsten infizierten Computer für File Reputation 36-5
Die 10 am häufigsten gesperrten Computer für Web Reputation 36-6

Teil XVI: Trend Micro Mobile Security – Widgets und Richtlinien

Kapitel 37: Trend Micro Mobile Security Dashboard-Widgets

Zustandsstatus von Android-Geräten 37-2
Verschlüsselungsstatus des Android Gerätes – Überblick – Widget 37-2
Android-Betriebssystemversionen – Überblick – Widget 37-2
Root-Status von Android-Geräten – Überblick – Widget 37-3
Sicherheitsstatus von Android-Geräten – Widget 37-3
Android-Malware-Suche – Überblick – Widget 37-3
Suche nach geänderten Android-Anwendungen – Überblick – Widget 37-4
Android Datenschutz-Lecksuche – Überblick – Widget 37-4
Android-Schwachstellensuche – Überblick – Widget 37-5
Status des Komponenten-Updates – Widget 37-5
Cybersicherheit für Mobilgeräte – Neuigkeiten – Widget 37-6
iOS-Geräte – Überblick über den Verschlüsselungsstatus – Widget 37-6
Zustandsstatus von iOS-Geräten – Widget 37-6
Sicherheitsstatus von iOS-Geräten – Widget 37-7
Jailbreak-Status von iOS-Geräten – Überblick – Widget 37-7
iOS-Betriebssystemversionen – Überblick – Widget 37-8

iOS-Malware-Suche – Überblick – Widget 37-8
Mobilgerät, App-Kontrollstatus – Überblick – Widget 37-8
Mobilgeräte – Überblick über den Verschlüsselungsstatus – Widget 37-9
Zustandsstatus von Mobilgeräten – Widget 37-9
Jailbreak-Status von Mobilgeräten – Überblick – Widget 37-10
Mobilgeräte-Betriebssystemversionen – Überblick – Widget 37-10
Suche nach Ransomware auf Mobilgeräten – Überblick – Widget 37-10
Sicherheitsstatus von Mobilgeräten – Widget 37-11
Mobilgeräteanbieter – Überblick – Widget 37-11
Richtlinienaktualisierungsstatus – Überblick – Widget 37-11
Zustandsstatus der Serverkomponente – Überblick – Widget 37-12
Netzbetreiber – Überblick – Widget 37-12
Die 10 am häufigsten installierten Anwendungen – Widget 37-12
Die fünf am häufigsten erkannten Android-Ransomware-Programme – Widget 37-13
Die 5 am häufigsten gesperrten Websites – Widget 37-13
Fünf häufigste erkannte iOS-Ransomware-Programme 37-13
Die 5 häufigsten Malware-Funde – Widget 37-13
Windows Phone – Überblick über den Verschlüsselungsstatus von Geräten – Widget 37-14
Zustandsstatus von Windows Phone-Geräten – Widget 37-14
Windows Phone-Betriebssystemversionen – Überblick – Widget 37-14

Kapitel 38: Trend Micro Mobile Security-Richtlinieneinstellungen

Geräte mit Richtlinien schützen 38-2
Allgemeine Richtlinie im Verteilungsmodus der Vollversion 38-4
Allgemeine Richtlinie im Verteilungsmodus der Sicherheitssuche 38-6
Wi-Fi-Richtlinie 38-6
Exchange ActiveSync-Richtlinie 38-7
Zertifikatrichtlinie 38-7
VPN-Richtlinie 38-7
Allgemeine HTTP-Proxy-Richtlinie 38-7
Single Sign-On-Richtlinie 38-7
Mobilfunknetzrichtlinie 38-9
AirPlay/AirPrint-Richtlinie 38-9
Design-Richtlinie 38-9
Richtlinie für verwaltete Domänen 38-9
Sicherheitsrichtlinie im Bereitstellungsmodus der Vollversion 38-10
Sicherheitsrichtlinie im Bereitstellungsmodus der Sicherheitssuche 38-13
Spamschutzrichtlinie 38-15
Richtlinien für SMS-Spamschutz 38-15
Spamschutzrichtlinie für WAP-Push 38-17
Anruffilterrichtlinie 38-19
Richtlinie zum Schutz vor Internet-Bedrohungen 38-21
Schutz vor Internet-Bedrohungen für Android-Mobilgeräte 38-21
Schutz vor Internet-Bedrohungen für iOS-Mobilgeräte 38-23
Kennwortrichtlinie 38-24
Richtlinie zur Funktionssperre 38-24
Unterstützte Betriebssystemfunktionen für Mobilgeräte 38-25
Konformitätsrichtlinie 38-47
Richtlinie zur Anwendungsüberwachung und -kontrolle 38-48

Richtlinie zum Volumenkaufprogramm 38-51
Anwendung hinzufügen 38-51
Container-Richtlinie 38-53

Teil XVII: Widgets für Virtual Mobile Infrastructure

Kapitel 39: Dashboard-Widgets für Virtual Mobile Infrastructure

Die 5 am häufigsten gestarteten Trend Micro Virtual Mobile Infrastructure-Anwendungen – Widget 39-2

Die 5 am häufigsten gestarteten Trend Micro Virtual Mobile Infrastructure-Webanwendungen – Widget 39-2

Die 5 häufigsten Online-Benutzer von Trend Micro Virtual Mobile Infrastructure – Widget 39-2

CPU-Auslastungsstatus des Trend Micro Virtual Mobile Infrastructure-Servers – Widget 39-3

Festplattennutzungsstatus von Trend Micro Virtual Mobile Infrastructure-Servern – Widget 39-3

Speicherauslastungsstatus des Trend Micro Virtual Mobile Infrastructure Servers 39-4

Trend Micro Virtual Mobile Infrastructure-Benutzerstatus – Widget 39-4

Teil XVIII: Vulnerability Protection – Widgets

Kapitel 40: Widgets für Vulnerability Protection Dashboard

Vulnerability Protection nach (erkanntem) Anwendungstyp – Widget 40-2

Vulnerability Protection nach (verhindertem) Anwendungstyp – Widget 40-3

Überblick über die Funktionen von Vulnerability Protection – Widget 40-4

Vulnerability Protection Firewall – Ereignisverlauf – Widget 40-5

Vulnerability Protection zur Erkennung von Eindringlingen – Ereignisverlauf – Widget 40-6

Vulnerability Protection – (erkannte) IPS-Aktivität – Widget 40-7

Vulnerability Protection – (verhinderte) IPS-Aktivität – Widget 40-8

Wichtigster Leistungsindikator für Vulnerability Protection – Widget 40-9

Vulnerability Protection Aufklärungssuche – Ereignisverlauf – Widget 40-9

Vulnerability Protection – Statusüberblick – Widget 40-10

Vulnerability Protection für gefährdete Endpunkte – Widget 40-11

Stichwortverzeichnis

Stichwortverzeichnis IN-1

Vorwort

Vorwort

Hinweis

Die Online-Hilfe für die Apex Central wurde für Sie maschinell Übersetzt. Es wurden angemessene Maßnahmen ergriffen, um Ihnen eine genaue Übersetzung bereitzustellen, jedoch ist keine automatisierte Übersetzung makellos.

Die offizielle Version der Online-Hilfe für die Apex Central ist die englische Version. Unstimmigkeiten oder Abweichungen in der Übersetzung sind nicht rechtsverbindlich und haben keine rechtlichen Wirkung für Compliance- oder Durchsetzungszwecke.

Willkommen beim Trend Micro Apex Central™*Widget- und Richtlinienverwaltungshandbuch*. In diesem Dokument wird die Konfiguration der Widgets **Dashboard** und der Einstellungen **Richtlinienverwaltung** auf Trend Micro Apex Central erläutert.

Themen in diesem Abschnitt:

Dokumentation

Trend Micro Apex Central Dokumentation umfasst Folgendes:

Dokument	Beschreibung
Readme-Datei	Enthält eine Liste bekannter Probleme und kann auch aktuelle Produktinformationen enthalten, die noch nicht in der Online-Hilfe oder in gedruckter Form zur Verfügung stehen
Administratorhandbuch	Ein PDF-Dokument mit detaillierten Anweisungen zur Konfiguration und Verwaltung von Trend Micro Apex Central und verwalteten Produkten sowie Erklärungen zu den Konzepten und Funktionen von Trend Micro Apex Central
Online-Hilfe	Im WebHelp-Format erstellte HTML-Dateien, die Anleitungen, allgemeine Benutzerhinweise und oberflächenspezifische Informationen enthalten. Der Zugriff auf die Hilfe kann auch über die Trend Micro Apex Central-Konsole erfolgen
Widget- und Richtlinienverwaltungshandbuch	Enthält Informationen, die erklären, wie Dashboard-Widgets und Richtlinieneinstellungen in Trend Micro Apex Central konfiguriert werden Um auf diesen Leitfaden zuzugreifen, gehen Sie zu https://docs.trendmicro.com/de-de/enterprise/apex-central-as-a-service-widget-and-policy-management-guide/preface-wpg-.aspx.
Automation Center	Online-Benutzerhandbücher und Referenzen, die erklären, wie die Trend Micro Apex Central Automatisierungs-APIs verwendet werden: https://automation.trendmicro.com/apex-central/home
Datenschutzliste (nur Kapitel 1)	Ein PDF-Dokument, in dem vordefinierte Datenbezeichner und Vorlagen für die Prävention vor Datenverlust aufgeführt sind
Wissensdatenbank	Eine Online-Datenbank mit Informationen zur Problemlösung und Fehlerbehebung. Sie enthält aktuelle Hinweise zu bekannten Softwareproblemen. Die Wissensdatenbank finden Sie im Internet unter folgender Adresse: http://success.trendmicro.com

Sie können die neueste Version der PDF-Dokumente und Readme-Dateien von der folgenden Adresse herunterladen:

http://docs.trendmicro.com/de-de/enterprise/apex-central.aspx

Zielgruppe

Die Trend Micro Apex Central Dokumentation ist für die folgenden Benutzergruppen gedacht:

- Trend Micro Apex Central Administratoren: Verantwortlich für die Installation, Konfiguration und Verwaltung von Trend Micro Apex Central. Von diesen Benutzern wird erwartet, dass sie über detaillierte Kenntnisse im Zusammenhang mit der Netzwerk- und Serververwaltung verfügen.
- Administratoren des verwalteten Produkts: Benutzer, die Trend Micro Produkte verwalten, die mit Trend Micro Apex Central vernetzt sind. Von diesen Benutzern wird erwartet, dass sie über detaillierte Kenntnisse im Zusammenhang mit der Netzwerk- und Serververwaltung verfügen.

Dokumentationskonventionen

Die Dokumentation verwendet die folgenden Konventionen:

TABELLE 1. Dokumentationskonventionen

KONVENTION	BESCHREIBUNG
GROSSSCHRIFT	Akronyme, Abkürzungen und die Namen bestimmter Befehle sowie Tasten auf der Tastatur
Fettdruck	Menüs und Menübefehle, Schaltflächen, Registerkarten und Optionen
Kursivdruck	Verweise auf andere Dokumente
`Schreibmaschinenschrift`	Muster für Befehlszeilen, Programmcode, Internet-Adressen, Dateinamen und Programmanzeigen
Navigation > **Pfad**	Der Navigationspfad zu einem bestimmten Fenster **Datei** > **Speichern** bedeutet beispielsweise, dass Sie in der Benutzeroberfläche im Menü **Datei** auf **Speichern** klicken

Konvention	Beschreibung
Hinweis	Konfigurationshinweise
Tipp	Empfehlungen oder Vorschläge
Wichtig	Informationen zu den erforderlichen oder standardmäßigen Konfigurationseinstellungen und Produktbeschränkungen
Warnung!	Wichtige Aktionen und Konfigurationsoptionen

Begriffe

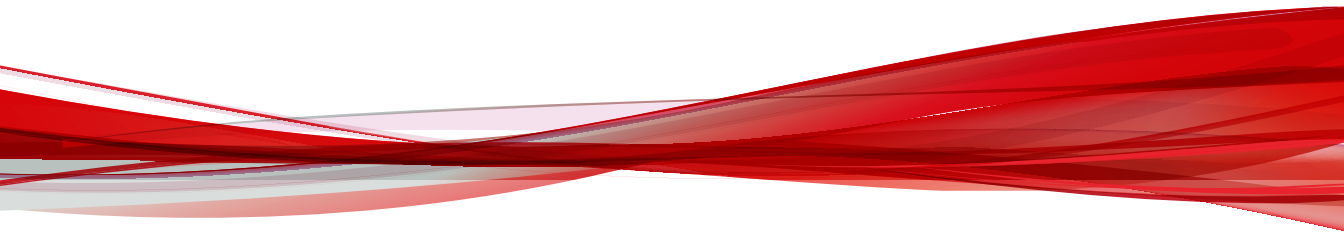
Die folgende Tabelle enthält offizielle Begriffe, die in der gesamten Trend Micro Apex Central Dokumentation verwendet werden:

Begriffe	Beschreibung
Administrator (oder Trend Micro Apex Central Administrator)	Die Person, die den Trend Micro Apex Central Server verwaltet.
Security Agent	Das auf einem Endpunkt installierte verwaltete Produktprogramm
Komponenten	Suchen und entdecken Sicherheitsrisiken und führen Aktionen gegen sie durch.

Begriffe	Beschreibung
Trend Micro Apex Central-Konsole, Webkonsole oder Management-Konsole	Die webbasierte Benutzeroberfläche für den Zugriff auf einen Trend Micro Apex Central, dessen Konfiguration oder Verwaltung **Hinweis** Konsolen für integrierte verwaltete Produkte sind durch den Namen des verwalteten Produkts gekennzeichnet. Beispiel: die Apex One-Webkonsole.
Verwalteter Endpunkt	Der Endpunkt, auf dem das verwaltete Produkt Security Agent installiert ist
Verwaltetes Produkt	Ein Trend Micro-Produkt, das in Trend Micro Apex Central integriert ist
Verwalteter Server	Der Endpunkt, auf dem das verwaltete Produkt installiert ist
Server	Der Endpunkt, auf dem der Trend Micro Apex Central Server installiert ist
Sicherheitsrisiko	Der Oberbegriff für Viren/Malware, Spyware/Grayware und Internet-Bedrohungen
Dual-stack	Elemente, die sowohl über IPv4- als auch IPv6-Adressen verfügen
Reines IPv4	Ein Gerät, das nur über IPv4-Adressen verfügt
Reines IPv6	Ein Gerät, das nur über IPv6-Adressen verfügt

Teil I

Einführung



Kapitel 1

Das Dashboard

In diesem Abschnitt wird erläutert, wie die Dashboard-Registerkarten und -Widgets von Trend Micro Apex Central verwendet werden.

Es werden folgende Themen behandelt:

Info über das Dashboard

Das **Dashboard** wird angezeigt, wenn Sie die Trend Micro Apex Central-Webkonsole öffnen oder im Hauptmenü auf **Dashboard** klicken. Jedes Trend Micro Apex Central-Benutzerkonto verfügt über ein völlig unabhängiges Dashboard. Alle Änderungen des Dashboards, das zu einem bestimmten Benutzerkonto gehört, haben keine Auswirkungen auf die Dashboards anderer Benutzerkonten.

Das **Dashboard** enthält folgende Informationen:

- Registerkarten
- Widgets

Registerkarten und Widgets

Widgets sind die Kernkomponenten des **Dashboard**. Widgets bieten spezifische Informationen über verschiedene sicherheitsrelevante Ereignisse.

Die Informationen, die Widgets anzeigen, stammen von:

- Trend Micro Apex Central-Datenbank
- Registrierte verwaltete Produkte
- Trend Micro Smart Protection Network

Registerkarten stellen einen Container für Widgets zur Verfügung. Das **Dashboard** unterstützt bis zu 30 Registerkarten.

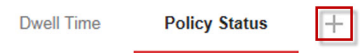
Mit Registerkarten arbeiten

Verwalten Sie Registerkarten, indem Sie das Layout hinzufügen, umbenennen oder ändern und automatisch zwischen Registerkartenansichten wechseln.

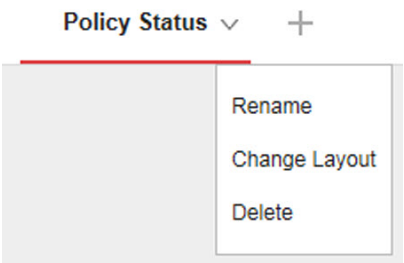
Prozedur

1. Navigieren Sie zum **Dashboard**.

2. So fügen Sie eine Registerkarte hinzu:
   a. Klicken Sie auf das Symbol zum Hinzufügen (+).



   b. Geben Sie einen Namen für die neue Registerkarte ein.
3. So benennen Sie eine Registerkarte um:
   a. Bewegen Sie den Mauszeiger über den Namen der Registerkarte und klicken Sie auf den Abwärtspfeil.

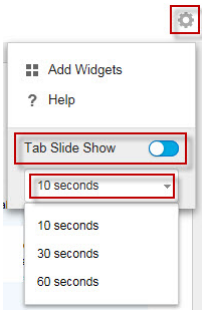


   b. Klicken Sie auf **Umbenennen** und geben Sie den neuen Registerkartennamen ein.
4. So ändern Sie das Layout der Widgets für eine Registerkarte:
   a. Bewegen Sie den Mauszeiger über den Namen der Registerkarte und klicken Sie auf den Abwärtspfeil.
   b. Klicken Sie auf **Layout ändern**.
   c. Wählen Sie das neue Layout im angezeigten Fenster aus.
   d. Klicken Sie auf **Save**.
5. So löschen Sie eine Registerkarte:
   a. Bewegen Sie den Mauszeiger über den Namen der Registerkarte und klicken Sie auf den Abwärtspfeil.

b. Klicken Sie auf **Löschen** und bestätigen Sie den Vorgang.

6. So geben Sie eine Bildschirmpräsentation der Registerkarten wieder:

   a. Klicken Sie rechts neben der Registerkartenanzeige auf die Schaltfläche **Einstellungen**.



   b. Aktivieren Sie das Steuerelement **Bildschirmpräsentation mit Registerkarte wiedergeben**.

   c. Wählen Sie den Zeitraum aus, der zwischen der Anzeige der Registerkarten vergehen soll.

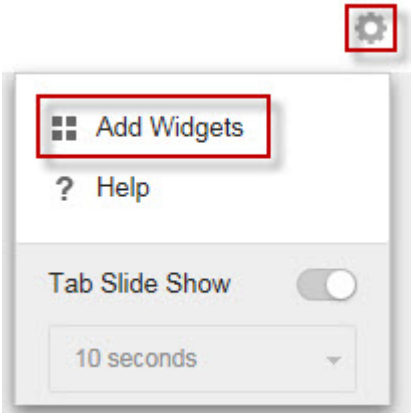
Arbeiten mit Widgets

Verwalten Sie Widgets durch Hinzufügen, Verschieben, ändern, Umbenennen und Löschen von Elementen. Sie können auch die Produkte ändern, die Daten für das Widget bereitstellen.

Prozedur

1. Navigieren Sie zum **Dashboard**.
2. Klicken Sie auf eine Registerkarte.
3. So fügen Sie ein Widget hinzu:

   a. Klicken Sie rechts neben der Registerkartenanzeige auf die Schaltfläche **Einstellungen**.



b. Klicken Sie auf **Widgets hinzufügen**.

c. Wählen Sie hinzuzufügende Widgets aus.

- Wählen Sie in der Dropdown-Liste oberhalb der Widgets eine Kategorie aus, um die Auswahl einzugrenzen.
- Verwenden Sie das Suchtextfeld im Fenster oben, um nach einem bestimmten Widget zu suchen.

d. Klicken Sie auf **Hinzufügen**.

4. Zum Verschieben eines Widgets an eine neue Position auf derselben Registerkarte ziehen Sie es an die neue Position und legen Sie es dort ab.

5. Sie können die Größe von Widgets in einer mehrspaltigen Registerkarte anpassen, indem Sie mit dem Cursor auf den rechten Rand des Widgets zeigen und den Cursor nach links oder rechts bewegen.

6. So benennen Sie ein Widget um:

a. Klicken Sie auf das Einstellungssymbol (>).

b. Geben Sie einen neuen Titel ein.

c. Klicken Sie auf **Save**.

7. So ändern Sie den Produktbereich des Widgets:

a. Klicken Sie auf das Einstellungssymbol (>).

b. Konfigurieren Sie die **Bereich**.

Widgets verwenden eine der folgenden Methoden zur Verwaltung des Umfangs:

- Wählen Sie den Umfang über das Listenfeld aus.
- Klicken Sie auf die Schaltfläche mit dem Doppelpfeil (>>), und wählen Sie die Produkte aus, für die Sie Daten für das Widget bereitstellen möchten.

c. Klicken Sie auf **Save**.

8. Um ein Widget zu löschen, klicken Sie auf das Löschsymbol (>).

Registerkarte Sicherheitsstatus

Die Registerkarte **Security Posture** bietet einen umfassenden Überblick über den Status des Netzwerkschutzes, indem Daten zu Konformitätsstufen, erkannten kritischen Bedrohungen und einer beendeten Erkennung in Ihrem Netzwerk konsolidiert werden. Mit Hilfe des Diagramms **Security Posture** können Sie über eine integrierte Active Directory-Struktur schnell Benutzer und Gruppen ermitteln, die hohen Risiken ausgesetzt sind.

Hinweis

Um die Beispieldiagrammdaten zu ändern und Standorte oder Berichtszeilen basierend auf Ihrem Unternehmensnetzwerk anzuzeigen, aktivieren Sie die Active Directory-Integration oder erstellen Sie benutzerdefinierte Standorte basierend auf IP-Adressen.

Standardmäßig ist die **Security Posture**-Registerkarte auf die **Diagramm**-Ansicht umgeschaltet ( ). Um die Diagrammknoten, kritischen Bedrohungen und Informationen zur Einhaltung des Viren-Patterns in einer Tabelle anzuzeigen, schalten Sie die **Tabelle**-Ansicht um ( ).

Klicken Sie auf das Einstellungssymbol (>), um die folgenden Informationen zu ändern, die auf der Registerkarte angezeigt werden.

- **Organisation**: Geben Sie den Anzeigenamen der Organisation ein.
- **Active Directory-Gruppierung**: Geben Sie an, ob die Knoten im Diagramm **Standorte** oder **Berichtszeilen** aus Ihrem Active Directory darstellen.
- **Gruppen anzeigen**: Wählen Sie die höchste Anzahl von Gruppen mit dem höchsten Risiko aus
- **Zeitraum**: Geben Sie den Zeitraum für die Anzeige der Daten im Diagramm an.

Konformitätsindikatoren

Dieser Abschnitt der Registerkarte **Security Posture** enthält Informationen über die Konformitätsstufe des Antivirus-Patterns oder die Konformitätsstufe der Funktion 'Prävention vor Datenverlust' Ihres Netzwerks.

Wenn sich die Konformitätsstufe Ihres Netzwerks ändert, ändert sich die Farbe des Konformitätsindikators, um die im Fenster **Active Directory- und Konformitätseinstellungen** konfigurierten Schwellenwerte widerzuspiegeln.

Die Standardansicht enthält Informationen zu dem Indikator **Antivirus-Pattern zur Einhaltung von Richtlinien**.

Hinweis

Durch das Ändern des Konformitätsindikators wird die im Diagramm **Security Posture** angezeigte Konformitätsstufe ebenfalls geändert.

Um die angezeigten Konformitätsinformationen zu ändern, klicken Sie auf den Namen des ausgewählten Konformitätsindikators neben dem Symbol mit dem Abwärtspfeil ( ) und wählen Sie einen der folgenden Indikatoren in der Dropdown-Liste aus.

Indikator	Beschreibung
Antivirus-Pattern zur Einhaltung von Richtlinien	Zeigt die folgenden Informationen an: • Den Prozentsatz der Security Agents, die zulässige Viren-Pattern- und Smart Scan Agent Pattern-Versionen nutzen • Die Gesamtzahl der Endpunkte mit veralteten Antivirus-Pattern in Ihrem Netzwerk Klicken Sie auf den Zähler für **Endpunkte mit veralteten Pattern**, um detaillierte Informationen über die betroffenen Endpunkte im Benutzer-/Endpunktverzeichnis anzuzeigen.
Einhaltung der Richtlinien für 'Prävention vor Datenverlust'	Zeigt die folgenden Informationen an: • Der Prozentsatz der Security Agents mit aktivierter Funktion 'Prävention vor Datenverlust' mit einer zulässigen Anzahl von erkannten Bedrohungen • Die Gesamtzahl aller Endpunkte mit Data Discovery-Bedrohungserkennungen Klicken Sie auf den Zähler für **Endpunkte mit unzulässigen Bedrohungserkennungen**, um detaillierte Informationen über die betroffenen Endpunkte im Benutzer-/Endpunktverzeichnis anzuzeigen.

Kritische Bedrohungen

Der Abschnitt **Kritische Bedrohungen** der Registerkarte **Security Posture** zeigt die Gesamtanzahl der eindeutigen kritischen Bedrohungen (nach Bedrohungsart) im Netzwerk, die Gesamtanzahl der betroffenen Benutzer und die Anzahl der betroffenen wichtigen Benutzer (durch den Stern gekennzeichnet).

Klicken Sie im Fenster **Benutzer-/Endpunktverzeichnis** auf die Anzahl der betroffenen Benutzer, um weitere Details anzuzeigen.

Zu den erkannten kritischen Bedrohungen zählen die folgenden Bedrohungstypen.

Bedrohungsart	Beschreibung
Ransomware	Malware, die den Zugriff von Benutzern auf ihr System so lange verhindert oder einschränkt, bis ein Lösegeld gezahlt wurde
Bekannte erweiterte anhaltende Bedrohung (Advanced Persistent Threat, APT)	Eindringversuche durch Angreifer, die aggressiv gewählte Ziele verfolgen und gefährden, häufig durchgeführt in Kampagnen – als eine Reihe fehlgeschlagener und erfolgreicher Versuche im Laufe der Zeit, um immer tiefer in ein Zielnetzwerk einzudringen – und nicht als isolierte Vorfälle
Social-Engineering-Angriff	Malware- oder Hacker-Angriffe, die eine in Dokumenten (z. B. einer PDF-Datei) gefundene Sicherheitsschwachstelle ausnutzen
Schwachstellenangriff	Malware- oder Hacker-Angriffe, die eine in der Regel in Programmen und Betriebssystemen gefundene Sicherheitslücke ausnutzen
Seitliche Verschiebung	Sucht nach Verzeichnissen, E-Mail- und Verwaltungsservern und anderen Ressourcen, um die interne Struktur eines Netzwerks abzubilden, Anmeldedaten für den Zugriff auf diese Systeme abzurufen und den Angreifern den Wechsel von System zu System zu ermöglichen
Unbekannte Bedrohungen	Verdächtige Objekte (IP-Adressen, Domänen, Datei-SHA-1-Hash-Werte, E-Mail-Nachrichten) mit der Risikostufe 'Hoch', die von Deep Discovery Inspector, Produkten für die Endpunktsicherheit oder anderen Produkten mit Virtual Analyzer erkannt wurden
C&C-Callback	Versuche mit einem C&C-Server (Command & Control-Server) zu kommunizieren, um Informationen zu übermitteln, Anweisungen zu erhalten und weitere Malware herunterzuladen

Behobene Ereignisse

In diesem Abschnitt der Registerkarte **Security Posture** wird die Gesamtanzahl der behobenen und nicht behobenen Ereignisse in Ihrem Netzwerk angezeigt.

Klicken Sie auf den Zähler für das Feld **Benutzer betroffen von __ ungelösten Ereignissen**, um detaillierte Informationen über die von nicht behobenen Ereignissen in Ihrem Netzwerk betroffenen Benutzer anzuzeigen.

Sicherheitsstatus-Diagramm

In dem Diagramm auf der Registerkarte **Security Posture** wird die Beziehung zwischen dem kritischen Bedrohungsverhältnis und der Konformitätsstufe Ihres Netzwerks angezeigt. Die X-Achse bezeichnet das Verhältnis zwischen den kritischen Bedrohungen und der Gesamtzahl der Endpunkte an einem Standort oder in einer Berichtszeile. Die y-Achse bezeichnet die Konformitätsstufen der Standorte oder der Berichtszeilen für den ausgewählten Konformitätsindikator. Mit Hilfe dieser Daten können Sie schnell Benutzer und Gruppen mit hohem Risiko in einer integrierten Active Directory-Struktur identifizieren.

Hinweis

Um die Beispieldiagrammdaten zu ändern und Standorte oder Berichtszeilen basierend auf Ihrem Unternehmensnetzwerk anzuzeigen, aktivieren Sie die Active Directory-Integration oder erstellen Sie benutzerdefinierte Standorte basierend auf IP-Adressen.

Bewegen Sie den Mauszeiger über einen Knoten, um Informationen zur Konformität und zu kritischen Bedrohungen für bestimmte Standorte oder Berichtszeilen anzuzeigen. Das Ende eines Knotens gibt die Richtung an, von der aus der Sicherheitsstatus im angegebenen Zeitraum geändert wurde.

- Klicken Sie auf das Einstellungssymbol (>), um die **Active Directory-Gruppierung** (**Standorte**, **Berichtszeilen**) zu ändern, die durch den Knoten dargestellt wird.
- Sie können auch Websites und Berichtszeilen mithilfe des Bildschirms **Active Directory- und Konformitätseinstellungen** anpassen.

Die Standardansicht enthält die Informationen zum ausgewählten Konformitätsindikator für alle Knoten im Netzwerk für die letzten 7 Tage.

- Wählen Sie einen anderen Konformitätsindikator aus, um die angezeigten Konformitätsinformationen zu ändern.
- Klicken Sie auf das Einstellungssymbol (>), um die **Zeitraum** für die angezeigten Daten zu ändern.

- Klicken Sie auf einen Knoten, um ausführliche Informationen über den ausgewählten Knoten im Zusammenfassungsbereich auf der rechten Seite anzuzeigen.

Einzelheiten Sicherheitslage Bereich

Im Detailbereich auf der Registerkarte **Security Posture** werden ausführlichere Informationen über die Konformitätsstufen, Funde kritischer Bedrohungen und die Gesamtzahl behobener/nicht behobener Ereignisse im Netzwerk angezeigt.

Die Standardansicht enthält die Informationen zum ausgewählten Konformitätsindikator für alle Knoten im Netzwerk für die letzten 7 Tage.

- Wählen Sie einen anderen Konformitätsindikator aus, um die angezeigten Konformitätsinformationen zu ändern.
- Klicken Sie auf einen Knoten im Diagramm, um nur die Informationen für den ausgewählten Knoten anzuzeigen.
- Klicken Sie auf das Einstellungssymbol (>), um die **Zeitraum** für die angezeigten Daten zu ändern.

Tabelle 1-1. Informationen zur Einhaltung von Richtlinien

Indikator	Beschreibung

Antivirus-Pattern zur Einhaltung von Richtlinien	Zeigt den Prozentsatz der Security Agents an, die zulässige Viren-Pattern- und Smart Scan Agent Pattern-Versionen nutzen
	
	Sie können auch die folgenden Details anzeigen:
	
	• **Verwaltete Agenten**: Die Anzahl der Endpunkte, auf denen Apex One oder Worry-Free Business Security Services Security Agents installiert sind
	  • **Mit konformen Viren-Pattern**: Die Anzahl der verwalteten Agents, die zulässige Viren-Pattern- und Smart Scan Agent Pattern-Versionen nutzen
	  • **Mit veralteten Viren-Patterns**: Die Anzahl der verwalteten Agents, die keine zulässigen Viren-Pattern- und Smart Scan Agent Pattern-Versionen nutzen
	  • **Offline für 7 Tage**: Die Anzahl der verwalteten Agents, die an 7 oder mehr Tagen nicht mit dem verwalteten Produktserver kommuniziert haben
	  • **Ausnahmen**: Die Anzahl der Benutzer oder Endpunkte, die aus den Konformitätsberechnungen ausgeschlossen werden
	• **Nicht verwaltete Endpunkte**: Die Anzahl der Endpunkte, auf denen keine Apex One- oder Worry-Free Business Security Services Security Agents installiert sind
	
	Erweitern Sie die Kategorien und klicken Sie auf einen Zähler, um zusätzliche Details zu den betroffenen Endpunkten anzuzeigen.

Indikator	Beschreibung

Einhaltung der Richtlinien für 'Prävention vor Datenverlust'	Zeigt den Prozentsatz der Apex One-Agents mit aktivierter Funktion 'Prävention vor Datenverlust' mit einer zulässigen Anzahl von erkannten Bedrohungen an
	
	Sie können auch die folgenden Details anzeigen:
	
	• **Verwaltete Agenten**: Die Anzahl der Endpunkte, auf denen Apex One oder Worry-Free Business Security Services Security Agents installiert sind
	  • **Mit akzeptablen Bedrohungserkennungen**: Die Anzahl der verwalteten Agents mit einer zulässigen Anzahl erkannter Bedrohungen
	  • **Mit inakzeptablen Bedrohungserkennungen**: Die Anzahl der verwalteten Agents, die die zulässige Anzahl der erkannten Bedrohungen überschritten haben
	  • **Offline für 7 Tage**: Die Anzahl der verwalteten Agents, die an 7 oder mehr Tagen nicht mit dem verwalteten Produktserver kommuniziert haben
	  • **Ausnahmen**: Die Anzahl der Benutzer oder Endpunkte, die aus den Konformitätsberechnungen ausgeschlossen werden
	• **Nicht verwaltete Endpunkte**: Die Anzahl der Endpunkte, auf denen keine Apex One- oder Worry-Free Business Security Services Security Agents installiert sind
	
	Erweitern Sie die Kategorien und klicken Sie auf einen Zähler, um zusätzliche Details zu den betroffenen Endpunkten anzuzeigen.

Tabelle 1-2. Kritische Bedrohungen

Abschnitt	Beschreibung
Kritische Bedrohungen	Zeigt die Gesamtzahl der eindeutigen kritischen Bedrohungen (nach Bedrohungsart) an, die in Ihrem Netzwerk erkannt wurden Listet alle Typen kritischer Bedrohungen auf, die Ihr Netzwerk beeinträchtigen Für Bedrohungstypen mit Funden: • Erweitern Sie den Bedrohungstyp, um eine Liste der Funde anzuzeigen. • Klicken Sie auf eine Erkennung, um weitere Details auf dem Bildschirm **Informationen zur Bedrohung** anzuzeigen.
Betroffene Benutzer	Zeigt die Gesamtanzahl der von kritischen Bedrohungen betroffenen Benutzer an • Erweitern Sie den Bereich, um die betroffenen Benutzer anzuzeigen. • Klicken Sie auf einen betroffenen Benutzer, um weitere Details im Informationsfenster **Benutzer** anzuzeigen.
Betroffene Endpunkte	Zeigt die Gesamtanzahl der von kritischen Bedrohungen betroffenen Endpunkte an • Erweitern Sie den Bereich, um die betroffenen Endpunkte anzuzeigen. • Klicken Sie auf einen betroffenen Endpunkt, um weitere Details im Informationsfenster **Endpunkt** anzuzeigen.

Tabelle 1-3. Ereignisse insgesamt

Daten	Beschreibung
Ereignisse insgesamt	Zeigt die Gesamtzahl der erkannten Ereignisse an
Behobene Ereignisse	Zeigt die Anzahl der behobenen Ereignisse im Netzwerk an
Nicht behobene Ereignisse	Zeigt die Anzahl der nicht behobenen Ereignisse im Netzwerk an, für die Aktionen erforderlich sind

Daten	Beschreibung
Betroffene Benutzer	Zeigt die Anzahl der Benutzer an, die von nicht behobenen Ereignissen im Netzwerk betroffen sind Klicken Sie auf den Zähler, um Details zu den betroffenen Benutzern anzuzeigen.

Registerkarte „Zusammenfassung“

Die Registerkarte **Zusammenfassung** enthält einen vordefinierten Satz an Widgets, die einen Überblick über den Sicherheitsstatus Ihres Netzwerks bieten.

Hinweis

Sie können die auf der Registerkarte **Zusammenfassung** angezeigten Widgets hinzufügen, löschen oder ändern.

Verfügbare Widgets:

- Kritische Bedrohungen
- Benutzer mit Bedrohungen
- Endpunkte mit Bedrohungen
- Verbindungsstatus des Produkts
- Produktkomponentenstatus
- Ransomware-Prävention

Kritische Bedrohungen – Widget

Dieses Widget zeigt die Gesamtanzahl der einzigartigen kritischen Bedrohungsarten an, die in Ihrem Netzwerk erkannt wurden, sowie die Anzahl der betroffenen Benutzer und Bedrohungserkennungen für jede Bedrohungsart.

Klicken Sie auf das Einstellungssymbol (>), um den Standardwert für **Anzeigen** zu ändern.

- Auf der Registerkarte **Übersicht** oder einer benutzerdefinierten Registerkarte ist standardmäßig die Ansicht **Betroffene Benutzer** ausgewählt.
- Auf der Registerkarte **Bedrohungsuntersuchung** ist standardmäßig die Ansicht **Bedrohungserkennungen** ausgewählt.

Hinweis

- Der Widget enthält Typen kritischer Bedrohungen sortiert nach Schweregrad.
- Einzelne Benutzer können von mehreren kritischen Bedrohungstypen betroffen sein.

Verwenden Sie die Dropdown-Liste **Bereich**, um den Zeitraum für die angezeigten Daten auszuwählen.

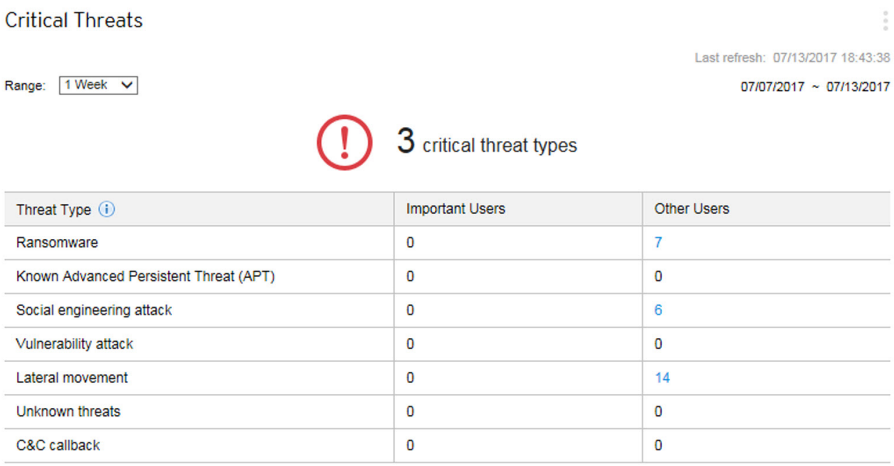


ABBILDUNG 1-1. Ansicht der betroffenen Benutzer

Die **Betroffene Benutzer**-Ansicht zeigt die Anzahl der **Wichtige Benutzer** und **Andere Benutzer**, die von jeder Bedrohungsart betroffen sind.

- Klicken Sie auf die Anzahl in der Spalte **Wichtige Benutzer** oder **Andere Benutzer** und dann auf den betroffenen Benutzer, den Sie anzeigen möchten.
- Sie können wichtige Benutzer oder Endpunkte auf dem **Benutzer-/ Endpunktverzeichnis**-Bildschirm definieren.

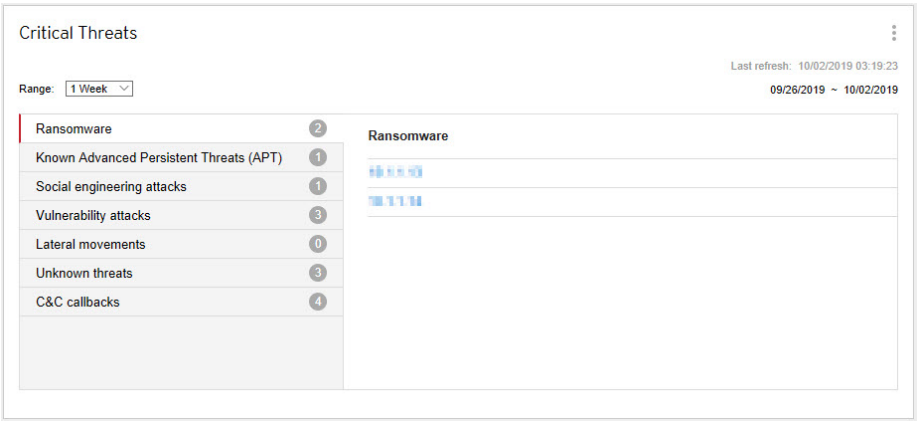


ABBILDUNG 1-2. Ansicht der Bedrohungserkennungen

Die **Bedrohungserkennungen**-Ansicht zeigt die Anzahl der Erkennungen für jede kritische Bedrohungsart an.

- Klicken Sie auf eine kritische Bedrohungsart, um die spezifischen Bedrohungserkennungen anzuzeigen.
- Klicken Sie auf den Hyperlink für eine spezifische Bedrohungserkennung, um Details über die betroffenen Benutzer anzuzeigen und automatisch eine Grundursachenanalyse zu starten, um festzustellen, ob die Bedrohung andere Endpunkte in Ihrem Netzwerk betroffen hat.

Zu den erkannten kritischen Bedrohungen zählen die folgenden Bedrohungstypen.

Bedrohungsart	Beschreibung
Ransomware	Malware, die den Zugriff von Benutzern auf ihr System so lange verhindert oder einschränkt, bis ein Lösegeld gezahlt wurde
Bekannte erweiterte anhaltende Bedrohungen (Advanced Persistent Threats, APT)	Eindringversuche durch Angreifer, die aggressiv gewählte Ziele verfolgen und gefährden, häufig durchgeführt in Kampagnen – als eine Reihe fehlgeschlagener und erfolgreicher Versuche im Laufe der Zeit, um immer tiefer in ein Zielnetzwerk einzudringen – und nicht als isolierte Vorfälle
Social-Engineering-Angriffe	Malware- oder Hacker-Angriffe, die eine in Dokumenten (z. B. einer PDF-Datei) gefundene Sicherheitsschwachstelle ausnutzen
Sicherheitslückenangriffe	Malware- oder Hacker-Angriffe, die eine in der Regel in Programmen und Betriebssystemen gefundene Sicherheitslücke ausnutzen
Laterale Bewegungen	Sucht nach Verzeichnissen, E-Mail- und Verwaltungsservern und anderen Ressourcen, um die interne Struktur eines Netzwerks abzubilden, Anmeldedaten für den Zugriff auf diese Systeme abzurufen und den Angreifern den Wechsel von System zu System zu ermöglichen
Unbekannte Bedrohungen	Verdächtige Objekte (IP-Adressen, Domänen, Datei-SHA-1-Hash-Werte, E-Mail-Nachrichten) mit der Risikostufe 'Hoch', die von Deep Discovery Inspector, Produkten für die Endpunktsicherheit oder anderen Produkten mit Virtual Analyzer erkannt wurden
C&C-Callbacks	Versuche mit einem C&C-Server (Command & Control-Server) zu kommunizieren, um Informationen zu übermitteln, Anweisungen zu erhalten und weitere Malware herunterzuladen

Benutzer mit Bedrohungen – Widget

Dieses Widget zeigt Informationen über die Benutzer mit erkannten Sicherheitsbedrohungen an.

Verwenden Sie die Dropdown-Liste **Bereich**, um den Zeitraum für die angezeigten Daten auszuwählen.

Klicken Sie auf die Registerkarten **Wichtige Benutzer** oder **Andere Benutzer**, um zwischen den verschiedenen Ansichten zu wechseln.

In der Tabelle sind die betroffenen Benutzer zuerst nach dem Schweregrad des Typs der kritischen Bedrohung und dann nach der Anzahl der Bedrohungserkennungen für den Benutzer aufgelistet.

- Klicken Sie auf die Zahl in der Spalte **Bedrohungen** für den Benutzer, den Sie anzeigen möchten.

Die **Kritischste Bedrohung**-Spalte zeigt die folgenden Bedrohungsarten an.

Bedrohungsart	Beschreibung
C&C-Callback	Versuche mit einem C&C-Server (Command & Control-Server) zu kommunizieren, um Informationen zu übermitteln, Anweisungen zu erhalten und weitere Malware herunterzuladen
Bekannte erweiterte anhaltende Bedrohung (Advanced Persistent Threat, APT)	Eindringversuche durch Angreifer, die aggressiv gewählte Ziele verfolgen und gefährden, häufig durchgeführt in Kampagnen – als eine Reihe fehlgeschlagener und erfolgreicher Versuche im Laufe der Zeit, um immer tiefer in ein Zielnetzwerk einzudringen – und nicht als isolierte Vorfälle
Seitliche Verschiebung	Sucht nach Verzeichnissen, E-Mail- und Verwaltungsservern und anderen Ressourcen, um die interne Struktur eines Netzwerks abzubilden, Anmeldedaten für den Zugriff auf diese Systeme abzurufen und den Angreifern den Wechsel von System zu System zu ermöglichen
Ransomware	Malware, die den Zugriff von Benutzern auf ihr System so lange verhindert oder einschränkt, bis ein Lösegeld gezahlt wurde
Social-Engineering-Angriff	Malware- oder Hacker-Angriffe, die eine in Dokumenten (z. B. einer PDF-Datei) gefundene Sicherheitsschwachstelle ausnutzen
Unbekannte Bedrohungen	Verdächtige Objekte (IP-Adressen, Domänen, Datei-SHA-1-Hash-Werte, E-Mail-Nachrichten) mit der Risikostufe 'Hoch', die von Deep Discovery Inspector, Produkten für die Endpunktsicherheit oder anderen Produkten mit Virtual Analyzer erkannt wurden
Schwachstellenangriff	Malware- oder Hacker-Angriffe, die eine in der Regel in Programmen und Betriebssystemen gefundene Sicherheitslücke ausnutzen

Endpunkte mit Bedrohungen – Widget

Dieses Widget zeigt Informationen über die Endpunkte mit erkannten Sicherheitsbedrohungen an.

Verwenden Sie die Dropdown-Liste **Bereich**, um den Zeitraum für die angezeigten Daten auszuwählen.

Klicken Sie auf die Registerkarten **Wichtige Benutzer** oder **Andere Benutzer**, um zwischen den verschiedenen Ansichten zu wechseln.

In der Tabelle sind die betroffenen Benutzer zuerst nach dem Schweregrad des Typs der kritischen Bedrohung und dann nach der Anzahl der Bedrohungserkennungen für den Benutzer aufgelistet.

- Klicken Sie auf die Zahl in der Spalte **Bedrohungen** für den Benutzer, den Sie anzeigen möchten.

Die **Kritischste Bedrohung**-Spalte zeigt die folgenden Bedrohungsarten an.

Bedrohungsart	Beschreibung
C&C-Callback	Versuche mit einem C&C-Server (Command & Control-Server) zu kommunizieren, um Informationen zu übermitteln, Anweisungen zu erhalten und weitere Malware herunterzuladen
Bekannte erweiterte anhaltende Bedrohung (Advanced Persistent Threat, APT)	Eindringversuche durch Angreifer, die aggressiv gewählte Ziele verfolgen und gefährden, häufig durchgeführt in Kampagnen – als eine Reihe fehlgeschlagener und erfolgreicher Versuche im Laufe der Zeit, um immer tiefer in ein Zielnetzwerk einzudringen – und nicht als isolierte Vorfälle
Seitliche Verschiebung	Sucht nach Verzeichnissen, E-Mail- und Verwaltungsservern und anderen Ressourcen, um die interne Struktur eines Netzwerks abzubilden, Anmeldedaten für den Zugriff auf diese Systeme abzurufen und den Angreifern den Wechsel von System zu System zu ermöglichen
Ransomware	Malware, die den Zugriff von Benutzern auf ihr System so lange verhindert oder einschränkt, bis ein Lösegeld gezahlt wurde
Social-Engineering-Angriff	Malware- oder Hacker-Angriffe, die eine in Dokumenten (z. B. einer PDF-Datei) gefundene Sicherheitsschwachstelle ausnutzen

Bedrohungsart	Beschreibung
Unbekannte Bedrohungen	Verdächtige Objekte (IP-Adressen, Domänen, Datei-SHA-1-Hash-Werte, E-Mail-Nachrichten) mit der Risikostufe 'Hoch', die von Deep Discovery Inspector, Produkten für die Endpunktsicherheit oder anderen Produkten mit Virtual Analyzer erkannt wurden
Schwachstellenangriff	Malware- oder Hacker-Angriffe, die eine in der Regel in Programmen und Betriebssystemen gefundene Sicherheitslücke ausnutzen

Apex Central – häufigste Bedrohungen – Widget

Dieses Widget zeigt Informationen über die bösartigen Dateien und URLs an, die für einen bestimmten Zeitraum erkannt wurden.

Sie können die Daten in einem Balkendiagramm oder einer Tabelle anzeigen, indem Sie auf die Anzeigesymbole ( ) klicken.

In der Dropdown-Liste über dem Diagramm/der Tabelle können Sie den Typ der Bedrohung auswählen, der angezeigt werden soll.

- **Bösartige Dateien**: Sortiert die in Ihrem Netzwerk erkannten bösartigen Dateien nach der Anzahl der Funde
- **Bösartige URLs**: Sortiert die in Ihrem Netzwerk erkannten bösartigen URLs nach der Anzahl der Funde

Klicken Sie auf einen Balken, den Namen der Bedrohung oder die Nummer des Funds, um das Fenster **Protokollabfrage** zu öffnen. In diesem Fenster werden Informationen über die betroffenen Endpunkte, die Details zu Bedrohungen und die Anzahl der Funde angezeigt.

Die Standardansicht zeigt die 10 häufigsten Bedrohungen für alle verwalteten Produkte an, für die der angemeldete Benutzer über Zugriffsrechte verfügt.

- Klicken Sie auf das Einstellungssymbol ( ), um den Widget-Titel, den Produktumfang oder die Anzahl der angezeigten Bedrohungen zu bearbeiten.

Produktkomponentenstatus – Widget

Dieses Widget zeigt Komponentenversionen und den Konformitätsstatus von verwalteten Produkten oder Endpunkten im Netzwerk an. Verwenden Sie dieses Widget, um verwaltete Produkte oder Endpunkte mit veralteten Komponenten zu ermitteln.

Die Standardansicht zeigt die neuesten Versionen der von Trend Micro Apex Central verwalteten Komponenten und den Konformitätsstatus der verwalteten Produkte an. In den Abschnitten **Pattern** und **Engine** sind sortierte Komponenten aufgelistet, wobei die höchste Rate von Nichtkonformität an erster Stelle steht. Sie können auf die Spalte **Bewerten** klicken, um die Sortierreihenfolge zu ändern.

Klicken Sie auf Komponenten in den Spalten **Pattern** oder **Engine**, um ein Tortendiagramm anzuzeigen, in dem die Anzahl der verwalteten Produkte oder Endpunkte angezeigt wird, die jede Komponentenversion verwenden.

Klicken Sie auf die Zähler in den Spalten **Veraltet/alle**, um Informationen über die Komponentenversionen auf veralteten verwalteten Produkten, allen verwalteten Produkten, veralteten Endpunkten oder allen Endpunkten anzuzeigen.

Klicken Sie auf das Einstellungssymbol (>), um die folgenden Optionen zu konfigurieren:

Hinweis

Das Symbol 'Einstellungen' ( ) wird für die Widgets auf der Registerkarte **Übersicht** nicht angezeigt.

- Um den Produktumfang des Widgets zu ändern, klicken Sie auf die Schaltfläche mit dem Doppelpfeil ( ) im Feld **Bereich** und wählen Sie die Produkte aus, die Daten beitragen.
- Um die Komponenten zu bearbeiten, die im Widget angezeigt werden, aktivieren oder deaktivieren Sie Komponenten in den Feldern **Pattern** oder **Engine**.

- Um Konformitätsinformationen für verwaltete Produkte, Endpunkte oder beides anzuzeigen, geben Sie die **Quelle** an.
- Um anzugeben, ob Daten von allen Komponenten angezeigt werden sollen, die von verwalteten Produkten gemeldet wurden, oder ob nur Daten von Komponenten angezeigt werden sollen, die durch Trend Micro Apex Central verwaltet wurden, wählen Sie die **Anzeigen** aus.

Daten	Beschreibung
Pattern	Zeigt den Namen der Pattern-Datei, der Vorlage oder der Anti-Spam-Regel an
Engine	Zeigt den Namen der Scan-Engine an
Neueste Version	Zeigt die folgenden Informationen an: • Die neueste Version der von Trend Micro Apex Central heruntergeladenen Komponente • Die neueste Version der Komponente, die zum Download bereitsteht (gemeldet von verwalteten Produkten)
Veraltet/alle	Zeigt die folgenden Informationen an: • **Nicht aktuell**: Die Anzahl der verwalteten Produkte oder Endpunkte mit veralteten Komponenten Klicken Sie auf den ersten Zähler in der Spalte **Veraltet/alle**, um Informationen zu den Komponentenversionen auf den veralteten verwalteten Produkten oder Endpunkten anzuzeigen. • **Alle**: Die Gesamtzahl der verwalteten Produkte oder Endpunkte, die die Komponente verwenden Klicken Sie auf den zweiten Zähler in der Spalte **Veraltet/alle**, um Informationen über die Komponentenversionen auf allen verwalteten Produkten oder Endpunkten anzuzeigen. **Hinweis** Diese Spalte zeigt an, wann **Beide** für **Quelle** ausgewählt ist.

Daten	Beschreibung
Rate	Zeigt den Prozentsatz der verwalteten Produkte oder Endpunkte mit veralteten Komponenten an **Hinweis** Diese Spalte zeigt an, wann **Beide** für **Quelle** ausgewählt ist.

Verbindungsstatus des Produkts – Widget

Dieses Widget zeigt den Verbindungsstatus aller verwalteten Produkte an, die beim Trend Micro Apex Central-Server registriert sind.

In der Standardansicht sind der Verbindungsstatus und der Name des verwalteten Servers jedes verwalteten Produkts aufgelistet, für das das angemeldete Benutzerkonto über Zugriffsrechte verfügt.

- Um den Produktumfang zu ändern, klicken Sie auf das Einstellungssymbol (>) und wählen Sie ein neues **Bereich** aus.
- Um eine Zusammenfassung der Gesamtzahl der verwalteten Produkte für jeden Verbindungsstatus anzuzeigen, klicken Sie auf das Einstellungssymbol (>) und wechseln Sie **Anzeigen** zu **Übersicht**.

Klicken Sie auf **Details anzeigen**, um detaillierte Informationen auf dem Bildschirm **Protokollabfrage** anzuzeigen.

Status	Beschreibung
Aktiv	Zeigt an, dass der Produktdienst ausgeführt wird und die Kommunikation mit dem Trend Micro Apex Central erfolgreich hergestellt wurde
Inaktiv	Zeigt an, dass der Produktdienst nicht ausgeführt wird oder die Kommunikation mit dem Trend Micro Apex Central-Server nicht einrichten kann

Status	Beschreibung
Ungewöhnlich	Zeigt an, dass der Produktdienst innerhalb des vom Benutzer definierten Zeitüberschreitungsintervalls für die Agent-Kommunikation nicht mit dem Trend Micro Apex Central-Server kommuniziert hat

Ransomware-Prävention – Widget

Dieses Widget bietet eine übersicht über alle Ransomware-Angriffsversuche während eines bestimmten Zeitraums.

In der Standardansicht wird eine Zusammenfassung aller Ransomware-Funde angezeigt. Darüber hinaus werden alle Versuche auf Basis des Infektionskanals kategorisiert.

- Klicken Sie auf die Anzahl der Ransomware-Funde, um weitere Informationen anzuzeigen.

Kanal	Beschreibung
Meldungen	In E-Mail-Nachrichten oder -Anhängen gefundene Ransomware
Websites	Von den Web-Reputation-Diensten gefundene Ransomware
Netzwerkverkehr	Von verdächtigen Apex One-Verbindungen und Deep Discovery Inspector gefundene Ransomware
Cloud-Synchronisierung	Ransomware, die von Cloud App Security im Cloud-Speicher oder auf Office 365-Servern (Exchange Online, SharePoint Online und OneDrive) oder von Apex One in lokalen Ordnern auf Apex One-Agents gefunden wurde, die sich mit dem Cloud-Speicher synchronisieren
Dateien	Von den File-Reputation-Diensten gefundene Ransomware
Verhaltensweisen	Von der Apex One-Verhaltensüberwachung gefundene Ransomware

Registerkarte 'Prävention vor Datenverlust'

Die Registerkarte **Prävention vor Datenverlust** enthält Widgets, die Informationen über DLP-Vorfälle, Vorlagenübereinstimmungen oder Vorfallquellen anzeigen.

Die vordefinierten Widgets umfassen:

- DLP-Vorfälle nach Schweregrad und Status
- DLP-Vorfallstrends nach Benutzer
- DLP-Vorfälle nach Benutzer
- DLP-Vorfälle nach Kanal
- DLP-Vorlagenübereinstimmungen
- Häufigste Quellen für DLP-Vorfälle
- DLP-Richtlinienverstoß

DLP-Vorfallstrends nach Benutzer – Widget

Dieses Widget überprüft die Anzahl der DLP-Vorfallstrends basierend auf verwalteten Benutzern. Daten können nach Schweregrad gefiltert werden, oder es kann nur die Gesamtzahl der Vorfälle angezeigt werden, die von einem bestimmten Benutzer für einen bestimmten Zeitraum ausgelöst wurde. Standardmäßig zeigt das Widget alle Daten für alle verwalteten Produkte an, die gemäß den Kontoberechtigungen eines Benutzers zulässig sind.

Verwenden Sie die Dropdown-Liste **Bereich**, um den Zeitraum für die angezeigten Daten auszuwählen.

Klicken Sie auf die Abschnitte der Grafik, um das Fenster **Informationen zum Vorfall** zu öffnen und den Überblick über die Vorfälle zu überprüfen.

Klicken Sie auf das Symbol mit den Widget-Einstellungen, um auf weitere Einstellungen zuzugreifen.

Einstellung	Beschreibung
Titel	Geben Sie einen neuen und aussagekräftigen Titel für das Widget in das Feld ein.
Bereich	Geben Sie den Zeitraum an, in dem die DLP-Vorfälle ausgelöst wurden.

Einstellung	Beschreibung
Bereich	Geben Sie den vom Widget angezeigten Datenbereich an. • Direkt verwaltete Benutzer • Alle verwalteten Benutzer: Die Daten werden von direkt verwalteten Benutzern und von Personen, die direkt verwalteten Benutzern unterstehen, erfasst.
Schweregrad	Geben Sie die Schweregrade zum Filtern der Daten an.
Anzuzeigende Benutzer	Geben Sie die Anzahl der anzuzeigenden verwalteten Benutzer an.

Klicken Sie auf **Speichern**, um Änderungen zu übernehmen und die Widget-Daten zu aktualisieren.

DLP-Vorfälle nach Schweregrad und Status – Widget

Dieses Widget überprüft die Anzahl der DLP-Vorfälle basierend auf dem Schweregrad und dem Vorfallstatus. Daten können nach Schweregrad gefiltert werden. Außerdem kann die Gesamtzahl der neuen Vorfälle und der Vorfälle mit dem Schweregrad 'Hoch' angezeigt werden. Standardmäßig zeigt das Widget alle Daten für alle verwalteten Produkte an, die gemäß den Kontoberechtigungen eines Benutzers zulässig sind.

Verwenden Sie die Dropdown-Liste **Bereich**, um den Zeitraum für die angezeigten Daten auszuwählen.

Klicken Sie auf die Zahlen in den Spalten, um das Fenster **Informationen zum Vorfall** zu öffnen und den Überblick über die Vorfälle zu überprüfen.

Um einen bestimmten Vorfall zu suchen, geben Sie eine ID in das Feld **Vorfall-ID** ein und klicken Sie auf **Suchen**.

Tipp

Jedem Vorfall wird eine ID-Nummer zugewiesen. ID-Nummern werden angezeigt, indem Sie auf einen Tabellenlink klicken, in den Ereignisbenachrichtigungen unter **Details zu Vorfällen aktualisiert** oder in den Protokollabfrageergebnissen unter **Prävention vor Datenverlust**.

Klicken Sie auf das Symbol mit den Widget-Einstellungen, um auf weitere Einstellungen zuzugreifen.

Einstellung	Beschreibung
Titel	Geben Sie einen neuen und aussagekräftigen Titel für das Widget in das Feld ein.
Bereich	Geben Sie den Zeitraum an, in dem die DLP-Vorfälle ausgelöst wurden.
Bereich	Geben Sie den vom Widget angezeigten Datenbereich an. • Direkt verwaltete Benutzer • Alle verwalteten Benutzer: Die Daten werden von direkt verwalteten Benutzern und von Personen, die direkt verwalteten Benutzern unterstehen, erfasst
Schweregrad	Geben Sie die Schweregrade zum Filtern der Daten an.

Klicken Sie auf **Speichern**, um Änderungen zu übernehmen und die Widget-Daten zu aktualisieren.

DLP-Vorfälle nach Benutzer – Widget

Dieses Widget überprüft die Anzahl der DLP-Vorfälle basierend auf dem Schweregrad und den verwalteten Benutzern. Daten können nach Schweregrad gefiltert werden. Außerdem kann die Gesamtzahl der neuen Vorfälle und der Vorfälle mit dem Schweregrad 'Hoch' angezeigt werden, die von bestimmten Benutzern ausgelöst werden. Standardmäßig zeigt das Widget alle Daten für alle verwalteten Produkte an, die gemäß den Kontoberechtigungen eines Benutzers zulässig sind. Das Widget zeigt maximal 50 Benutzer an.

Verwenden Sie die Dropdown-Liste **Bereich**, um den Zeitraum für die angezeigten Daten auszuwählen.

Klicken Sie auf die Zahlen in den Spalten, um das Fenster **Informationen zum Vorfall** zu öffnen und den Überblick über die Vorfälle zu überprüfen.

Um nach einem bestimmten Benutzer zu suchen, geben Sie ein paar Zeichen in das Feld **Benutzer** ein und klicken Sie auf **Suchen**. Wenn Sie beispielsweise ke eingeben, werden alle Benutzernamen angezeigt, die die

Buchstabenfolge `ke` enthalten. Beispiel: „Ken“ und „Brooke“. Sie können auch einen Domänen- und einen Benutzernamen eingeben. Beispiel: `domain1\chris`.

Hinweis

Benutzernamen dürfen die folgenden Zeichen nicht enthalten: " [ ] : ; | = + * ? / \ < &> ,

Domänennamen dürfen die folgenden Zeichen nicht enthalten: \ * + = | : ; " ? < &> ,

Klicken Sie auf das Symbol mit den Widget-Einstellungen, um auf weitere Einstellungen zuzugreifen.

Einstellung	Beschreibung
Titel	Geben Sie einen neuen und aussagekräftigen Titel für das Widget in das Feld ein.
Bereich	Geben Sie den Zeitraum an, in dem die DLP-Vorfälle ausgelöst wurden.
Bereich	Geben Sie den vom Widget angezeigten Datenbereich an. • Direkt verwaltete Benutzer • Alle verwalteten Benutzer: Die Daten werden von direkt verwalteten Benutzern und von Personen, die direkt verwalteten Benutzern unterstehen, erfasst.
Schweregrad	Geben Sie die Schweregrade zum Filtern der Daten an.
Anzuzeigende Benutzer	Geben Sie die Anzahl der anzuzeigenden verwalteten Benutzer an.

Klicken Sie auf **Speichern**, um Änderungen zu übernehmen und die Widget-Daten zu aktualisieren.

DLP-Vorfälle nach Kanal – Widget

Dieses Widget zeigt die Gesamtzahl der DLP-Vorfälle an. Daten können nach dem Typ der Kanäle, in denen der Vorfall ausgelöst wurde, gefiltert werden.

Verwenden Sie die Dropdown-Liste **Bereich**, um den Zeitraum für die angezeigten Daten auszuwählen.

Verwenden Sie die Dropdown-Liste **Kanal**, um nach dem Typ der Kanäle zu filtern, in denen der Vorfall ausgelöst wurde.

Dieses Widget zeigt die Anzahl der DLP-Vorfälle und das Verhältnis zwischen den Kanälen und der Gesamtzahl der Vorfälle an. Dieses Widget zeigt folgende Daten an:

Daten	Beschreibung
P2P	Zeigt alle Peer-to-Peer-DLP-Vorfälle nach den verwalteten Produkten an, die der Datenbereich umfasst
IM	Zeigt alle Instant-Messaging-DLP-Vorfälle nach den verwalteten Produkten an, die der Datenbereich umfasst
Webmail	Zeigt alle Webmail-DLP-Vorfälle nach den verwalteten Produkten an, die der Datenbereich umfasst
E-Mail	Zeigt alle E-Mail-DLP-Vorfälle nach den verwalteten Produkten an, die der Datenbereich umfasst
Web-App	Zeigt alle DLP-Vorfälle für Webanwendungen nach den verwalteten Produkten an, die der Datenbereich umfasst
Andere	Zeigt die verbleibenden DLP-Vorfälle nach den verwalteten Produkten an, die der Datenbereich umfasst

Durch Klicken auf die Links in der Spalte **Kanal** oder auf die Abschnitte der Grafik wird ein Fenster mit näheren Informationen geöffnet.

Daten	Beschreibung
Kanal	Der Typ der Kanäle, in denen die DLP-Vorfälle ausgelöst wurden
Vorfälle	Die Anzahl der ausgelösten DLP-Vorfälle
Prozentsatz (%)	Der prozentuale Anteil der DLP-Vorfälle an der Gesamtzahl der Vorfälle

Um die Informationen zu ändern, die das Widget anzeigt, klicken Sie auf > . Geben Sie im daraufhin angezeigten Dialogfeld den **Bereich** an, indem

Sie auf >> klicken und die übergeordneten Server auswählen, die das Widget als Quelle nutzt.

DLP-Vorlagenübereinstimmungen – Widget

Dieses Widget zeigt den Typ der DLP-Vorfälle in Ihrem Netzwerk an. Daten können nach Vorlage gefiltert werden.

Verwenden Sie die Dropdown-Liste **Bereich**, um den Zeitraum für die angezeigten Daten auszuwählen.

Durch Klicken auf die Links in der Spalte **Vorlage** oder auf die Abschnitte der Grafik wird ein Fenster mit näheren Informationen geöffnet.

Daten	Beschreibung
Vorlage	Von DLP-Vorfällen ausgelöste Vorlage
Vorfälle	Anzahl der DLP-Vorfälle
Prozentsatz (%)	Der prozentuale Anteil der DLP-Vorfälle an der Gesamtzahl der Vorfälle

Um die Informationen zu ändern, die das Widget anzeigt, klicken Sie auf > . Geben Sie im daraufhin angezeigten Dialogfeld den **Bereich** an, indem Sie auf >> klicken und die übergeordneten Server auswählen, die das Widget als Quelle nutzt.

Häufigste Quellen für DLP-Vorfälle – Widget

Dieses Widget zeigt die Gesamtzahl der häufigsten Quellen für DLP-Vorfälle im Netzwerk an. Zu diesen Daten gehören Benutzer, E-Mail-Adressen, Hostnamen und IP-Adressen, die nach Vorfallsquelle gefiltert werden können.

Verwenden Sie die Dropdown-Liste **Bereich**, um den Zeitraum für die angezeigten Daten auszuwählen.

Verwenden Sie die Dropdown-Liste **Anzeigen**, um die anzuzeigenden Daten auszuwählen.

DLP-Richtlinienverstoß – Widget

Dieses Widget zeigt den DLP-Richtlinienverstoß an. Verwenden Sie dieses Widget, um die Gesamtzahl der DLP-Vorfälle zu überprüfen. Daten werden standardmäßig nach der Anzahl der Vorfälle sortiert. Um die Daten nach Name der Richtlinie zu sortieren, klicken Sie auf den Titel der Spalte **Richtlinie**.

Verwenden Sie die Dropdown-Liste **Bereich**, um den Zeitraum für die angezeigten Daten auszuwählen.

Durch Klicken auf die Links in der Spalte **Vorfälle** wird ein Fenster mit detaillierten Informationen geöffnet.

Daten	Beschreibung
Richtlinie	Der Name der Richtlinie, bei der die DLP-Vorfälle ausgelöst wurden
Vorfälle	Die Anzahl der ausgelösten DLP-Vorfälle

Registerkarte 'Konformität'

Die Registerkarte **Konformität** enthält Widgets, die Informationen zur Konformität von Komponenten oder Verbindungen für verwaltete Produkte oder Endpunkte anzeigen.

Es gibt die folgenden vordefinierten Widgets:

- Einhaltung von Richtlinien für Produktanwendung
- Produktkomponentenstatus
- Verbindungsstatus des Produkts
- Verbindungsstatus des Agents

Einhaltung von Richtlinien für Produktanwendung – Widget

In diesem Widget werden Produktversion, Sprache, Build und Aktualisierungsstatus für verwaltete Produkte angezeigt. So können Administratoren schnell erkennen, welche Anwendungen des verwalteten Produkts auf dem neuesten Stand sind und welche aktualisiert werden müssen.

Sie können die Daten in einem Balkendiagramm oder einer Tabelle anzeigen, indem Sie auf die Anzeigesymbole ( ) klicken.

Klicken Sie auf die Anzahl in den Spalten **Auf dem neuesten Stand** und **Nicht aktuell**, um ein Fenster mit ausführlichen Informationen zu öffnen. Trend Micro Apex Central führt eine Protokollabfrage durch, um ausführliche Informationen bereitzustellen.

Daten	Beschreibung
Produkt	Das verwaltete Produkt wurde bei Trend Micro Apex Central registriert
Version	Version des verwalteten Produkts
Sprache	Sprachversion des verwalteten Produkts
Build	Build-Nummer des verwalteten Produkts
Auf dem neuesten Stand	Anzahl der Produkte, die als aktualisiert gelten Bearbeiten Sie das Widget, um die niedrigste Produktversion anzugeben, die noch als „Auf dem neuesten Stand“ gelten soll. Klicken Sie auf die Anzahl, um weitere Informationen zum Produkt anzuzeigen.
Nicht aktuell	Anzahl der „nicht aktuellen“ Produkte Klicken Sie auf die Anzahl, um weitere Informationen zum Produkt anzuzeigen.
Aktuelle Rate (%)	Prozentsatz der Produkte, die „auf dem neuesten Stand“ sind

Standardmäßig zeigt das Widget alle Daten für alle verwalteten Produkte an, die gemäß den Kontoberechtigungen eines Benutzers zulässig sind.

Geben Sie ein Balkendiagramm oder eine Tabelle zur Anzeige der Daten an. Standardmäßig werden die Daten in einem Balkendiagramm angezeigt.

Klicken Sie auf **Bearbeiten**, um auf die folgenden Optionen zuzugreifen:

- Klicken Sie auf **Bereich** > **Durchsuchen** zur Angabe der Produkte, die Daten für das Widget bereitstellen.

Im Datenbereich werden die Produkte angegeben, die vom Widget zur Anzeige von Daten verwendet werden. Dies kann drastische Auswirkungen auf die Verwendbarkeit der Daten haben, die im Widget angezeigt werden.

- Geben Sie in der Dropdown-Liste **Bereich auf dem neuesten Stand** die Nummern der Produktversionen vor dem aktuellen Build an, die noch als „auf dem neuesten Stand“ gelten sollen.

Klicken Sie auf **Speichern**, um die Änderungen zu übernehmen und das Widget zu beenden.

Produktkomponentenstatus – Widget

Dieses Widget zeigt Komponentenversionen und den Konformitätsstatus von verwalteten Produkten oder Endpunkten im Netzwerk an. Verwenden Sie dieses Widget, um verwaltete Produkte oder Endpunkte mit veralteten Komponenten zu ermitteln.

Die Standardansicht zeigt die neuesten Versionen der von Trend Micro Apex Central verwalteten Komponenten und den Konformitätsstatus der verwalteten Produkte an. In den Abschnitten **Pattern** und **Engine** sind sortierte Komponenten aufgelistet, wobei die höchste Rate von Nichtkonformität an erster Stelle steht. Sie können auf die Spalte **Bewerten** klicken, um die Sortierreihenfolge zu ändern.

Klicken Sie auf Komponenten in den Spalten **Pattern** oder **Engine**, um ein Tortendiagramm anzuzeigen, in dem die Anzahl der verwalteten Produkte oder Endpunkte angezeigt wird, die jede Komponentenversion verwenden.

Klicken Sie auf die Zähler in den Spalten **Veraltet/alle**, um Informationen über die Komponentenversionen auf veralteten verwalteten Produkten, allen verwalteten Produkten, veralteten Endpunkten oder allen Endpunkten anzuzeigen.

Klicken Sie auf das Einstellungssymbol (>), um die folgenden Optionen zu konfigurieren:

Hinweis

Das Symbol 'Einstellungen' ( ) wird für die Widgets auf der Registerkarte **Übersicht** nicht angezeigt.

- Um den Produktumfang des Widgets zu ändern, klicken Sie auf die Schaltfläche mit dem Doppelpfeil (>>) im Feld **Bereich** und wählen Sie die Produkte aus, die Daten beitragen.
- Um die Komponenten zu bearbeiten, die im Widget angezeigt werden, aktivieren oder deaktivieren Sie Komponenten in den Feldern **Pattern** oder **Engine**.
- Um Konformitätsinformationen für verwaltete Produkte, Endpunkte oder beides anzuzeigen, geben Sie die **Quelle** an.
- Um anzugeben, ob Daten von allen Komponenten angezeigt werden sollen, die von verwalteten Produkten gemeldet wurden, oder ob nur Daten von Komponenten angezeigt werden sollen, die durch Trend Micro Apex Central verwaltet wurden, wählen Sie die **Anzeigen** aus.

Daten	Beschreibung
Pattern	Zeigt den Namen der Pattern-Datei, der Vorlage oder der Anti-Spam-Regel an
Engine	Zeigt den Namen der Scan-Engine an
Neueste Version	Zeigt die folgenden Informationen an: • Die neueste Version der von Trend Micro Apex Central heruntergeladenen Komponente • Die neueste Version der Komponente, die zum Download bereitsteht (gemeldet von verwalteten Produkten)

Daten	Beschreibung
Veraltet/alle	Zeigt die folgenden Informationen an: • **Nicht aktuell**: Die Anzahl der verwalteten Produkte oder Endpunkte mit veralteten Komponenten Klicken Sie auf den ersten Zähler in der Spalte **Veraltet/alle**, um Informationen zu den Komponentenversionen auf den veralteten verwalteten Produkten oder Endpunkten anzuzeigen. • **Alle**: Die Gesamtzahl der verwalteten Produkte oder Endpunkte, die die Komponente verwenden Klicken Sie auf den zweiten Zähler in der Spalte **Veraltet/alle**, um Informationen über die Komponentenversionen auf allen verwalteten Produkten oder Endpunkten anzuzeigen. **Hinweis** Diese Spalte zeigt an, wann **Beide** für **Quelle** ausgewählt ist.
Rate	Zeigt den Prozentsatz der verwalteten Produkte oder Endpunkte mit veralteten Komponenten an **Hinweis** Diese Spalte zeigt an, wann **Beide** für **Quelle** ausgewählt ist.

Verbindungsstatus des Produkts – Widget

Dieses Widget zeigt den Verbindungsstatus aller verwalteten Produkte an, die beim Trend Micro Apex Central-Server registriert sind.

In der Standardansicht sind der Verbindungsstatus und der Name des verwalteten Servers jedes verwalteten Produkts aufgelistet, für das das angemeldete Benutzerkonto über Zugriffsrechte verfügt.

- Um den Produktumfang zu ändern, klicken Sie auf das Einstellungssymbol (>) und wählen Sie ein neues **Bereich** aus.

- Um eine Zusammenfassung der Gesamtzahl der verwalteten Produkte für jeden Verbindungsstatus anzuzeigen, klicken Sie auf das Einstellungssymbol (>) und wechseln Sie **Anzeigen** zu **Übersicht**.

Klicken Sie auf **Details anzeigen**, um detaillierte Informationen auf dem Bildschirm **Protokollabfrage** anzuzeigen.

Status	Beschreibung
Aktiv	Zeigt an, dass der Produktdienst ausgeführt wird und die Kommunikation mit dem Trend Micro Apex Central erfolgreich hergestellt wurde
Inaktiv	Zeigt an, dass der Produktdienst nicht ausgeführt wird oder die Kommunikation mit dem Trend Micro Apex Central-Server nicht einrichten kann
Ungewöhnlich	Zeigt an, dass der Produktdienst innerhalb des vom Benutzer definierten Zeitüberschreitungsintervalls für die Agent-Kommunikation nicht mit dem Trend Micro Apex Central-Server kommuniziert hat

Verbindungsstatus des Agents – Widget

Dieses Widget zeigt den Verbindungsstatus der Agents mit ihren übergeordneten Servern an. Agents für die folgenden verwalteten Produkte werden angezeigt:

- Endpoint Sensor
- Endpoint Encryption
- Mobile Security
- Mobile Security (für Mac)
- Apex One
- Vulnerability Protection
- Worry-Free Business Security Services

Standardmäßig zeigt das Widget alle Daten für alle verwalteten Produkte an, die gemäß den Kontoberechtigungen eines Benutzers zulässig sind.

Klicken Sie auf die Werte in den Spalten **Online**, **Offline** oder **Gesamt**, um Weitere Informationen anzuzeigen. Trend Micro Apex Central führt eine Protokollabfrage durch, um die Informationen zur Verfügung zu stellen.

Daten	Beschreibung
Server	Übergeordnete Server
Online	Mit ihren übergeordneten Servern verbundene Agents
Offline	Von ihren übergeordneten Servern getrennte Agents
Gesamt	Gesamtzahl der Endpunkte

Um die Informationen zu ändern, die das Widget anzeigt, klicken Sie auf ⋮ > . Geben Sie im daraufhin angezeigten Dialogfeld den **Bereich** an, indem Sie auf » klicken und die übergeordneten Server auswählen, die das Widget als Quelle nutzt.

Bedrohungsstatistik-Registerkarte

Die Registerkarte **Bedrohungsstatistik** enthält Widgets, die aggregierte Funde von Sicherheitsbedrohungen anzeigen.

Die vordefinierten Widgets umfassen:

- Apex Central Top-Bedrohungen
- Apex Central – Bedrohungsstatistiken
- Bedrohungserkennungsergebnisse
- Erkannte Richtlinienverstöße
- C&C-Callback-Ereignisse

Apex Central – häufigste Bedrohungen – Widget

Dieses Widget zeigt Informationen über die bösartigen Dateien und URLs an, die für einen bestimmten Zeitraum erkannt wurden.

Sie können die Daten in einem Balkendiagramm oder einer Tabelle anzeigen, indem Sie auf die Anzeigesymbole ( ) klicken.

In der Dropdown-Liste über dem Diagramm/der Tabelle können Sie den Typ der Bedrohung auswählen, der angezeigt werden soll.

- **Bösartige Dateien**: Sortiert die in Ihrem Netzwerk erkannten bösartigen Dateien nach der Anzahl der Funde
- **Bösartige URLs**: Sortiert die in Ihrem Netzwerk erkannten bösartigen URLs nach der Anzahl der Funde

Klicken Sie auf einen Balken, den Namen der Bedrohung oder die Nummer des Funds, um das Fenster **Protokollabfrage** zu öffnen. In diesem Fenster werden Informationen über die betroffenen Endpunkte, die Details zu Bedrohungen und die Anzahl der Funde angezeigt.

Die Standardansicht zeigt die 10 häufigsten Bedrohungen für alle verwalteten Produkte an, für die der angemeldete Benutzer über Zugriffsrechte verfügt.

- Klicken Sie auf das Einstellungssymbol (>), um den Widget-Titel, den Produktumfang oder die Anzahl der angezeigten Bedrohungen zu bearbeiten.

Apex Central Bedrohungsstatistiken – Widget

Dieses Widget zeigt die Gesamtzahl der erkannten Sicherheitsbedrohungen in Ihrem Netzwerk an. Daten können nach Typ der Sicherheitsbedrohung oder nach dem Ort in Ihrem Netzwerk, an dem die Bedrohung erkannt wurde, gefiltert werden.

- Produktkategorie

Daten	Beschreibung
Dateiserver	Sicherheitsbedrohungen auf Dateiservern, die von allen verwalteten Produkten erkannt werden, die der Datenbereich umfasst
Netzwerk	Sicherheitsbedrohungen in Ihrem Netzwerk, die von allen verwalteten Produkten erkannt werden, die der Datenbereich spezifiziert
Unbekannt	Unbekannte Sicherheitsbedrohungen

Daten	Beschreibung
E-Mail	Sicherheitsbedrohungen auf E-Mail-Servern, die von allen verwalteten Produkten erkannt werden, die der Datenbereich umfasst
Desktop	Sicherheitsbedrohungen auf Desktops, die von allen verwalteten Produkten erkannt werden, die der Datenbereich umfasst
Gateway	Sicherheitsbedrohungen am Gateway, die von allen verwalteten Produkten erkannt werden, die der Datenbereich spezifiziert
Apex Central-Server	Sicherheitsbedrohungen auf Apex Central-Servern, die von allen verwalteten Produkten erkannt werden, die der Datenbereich umfasst

- Verstoßtyp

Daten	Beschreibung
Verhaltensüberwachung	Verstoß der Verhaltensüberwachung, der von allen verwalteten Produkten erkannt wird, die der Datenbereich umfasst
Inhaltsbezogener Verstoß	Inhaltssicherheitsverstöße (Spam, gesperrte Schlüsselwörter und Ausdrücke), die von allen verwalteten Produkten erkannt werden, die der Datenbereich umfasst
Gerätesteuerung	Verstoß gegen die Gerätesteuerung, der von allen verwalteten Produkten erkannt wird, die der Datenbereich umfasst
Firewall-Verstoß	Firewall-Verstoß durch alle verwalteten Produkte, die der Datenbereich umfasst
Prüfung der Netzwerkinhalte	Netzwerkinhaltsinspektionsverstoß, der von allen verwalteten Produkten erkannt wird, die der Datenbereich umfasst
Vorausschauendes Maschinenlernen	Vorausschauendes Maschinenlernen-Erkennung durch alle verwalteten Produkte, die der Datenbereich umfasst
Spyware/Grayware	Spyware/Grayware, die von allen verwalteten Produkten erkannt werden, die der Datenbereich umfasst
Verdächtige Dateien	Verdächtige Dateierkennung durch alle verwalteten Produkte, die der Datenbereich umfasst

Daten	Beschreibung
Virus/Malware	Viren/Malware, die von allen verwalteten Produkten erkannt werden, die der Datenbereich umfasst
Websicherheit	Websicherheitsverstöße (bösartige URLs, gesperrte URLs), die von allen verwalteten Produkten erkannt werden, die der Datenbereich umfasst

Hinweis

Das Widget kann zu einem Zeitpunkt jeweils nur Daten für eine Art von Information anzeigen.

Klicken Sie auf die Links in der Spalte **Funde**, um ein Fenster zu öffnen, in dem detaillierte Informationen angezeigt werden. Apex Central führt eine Protokollabfrage durch, um ausführliche Informationen anzugeben.

Daten	Beschreibung
Typ	Typ der Sicherheitsbedrohung oder des verwalteten Produkts, in dem die Bedrohung gefunden wurde
Funde	Anzahl der erkannten Sicherheitsbedrohungen
Prozentsatz (%)	Prozentsatz der Gesamtzahl der erkannten Sicherheitsbedrohungen

Geben Sie den Datumsbereich für die Daten an, die im Widget angezeigt werden:

- Heute
- Letzte 7 Tage
- Letzte 14 Tage
- Letzte 30 Tage

Geben Sie an, wie die Daten im Widget angezeigt werden:

- Tortendiagramm
- Balkendiagramm

- Tabellarisch
- Liniendiagramm

Standardmäßig zeigt das Widget alle Daten für alle verwalteten Produkte an, die gemäß den Kontoberechtigungen eines Benutzers zulässig sind.

Um die Informationen zu ändern, die das Widget anzeigt, klicken Sie auf > . Geben Sie im daraufhin angezeigten Dialogfeld den **Bereich** an, indem Sie auf >> klicken und die übergeordneten Server auswählen, die das Widget als Quelle nutzt.

Bedrohungserkennungsergebnisse – Widget

Dieses Widget zeigt die Anzahl der erkannten Bedrohungen und das Verhältnis der Bedrohungen zur Gesamtzahl der Funde an. Das Widget kann zu einem Zeitpunkt jeweils nur Daten für eine Art von Information anzeigen. Durch Klicken auf Links in der Spalte **Funde** wird ein Fenster mit ausführlichen Informationen geöffnet. Apex Central führt eine Protokollabfrage durch, um ausführliche Informationen anzugeben.

Daten	Beschreibung
Ergebnisse	Die Aktion oder das Ergebnis der Aktion, die vom verwalteten Produkt durchgeführt wurde **Hinweis** Diese Spalte wird für den Bedrohungstyp **Websicherheit** nicht angezeigt
Richtlinie/Regel	Der Typ der Richtlinie/Regel unter dem Bedrohungstyp **Websicherheit**. **Hinweis** Diese Spalte wird für andere aufgeführte Bedrohungstypen nicht angezeigt.
Funde	Die Anzahl der erkannten Sicherheitsbedrohungen

Daten	Beschreibung
Prozentsatz (%)	Der Prozentsatz aller Erkennungen, die Sicherheitsbedrohungen darstellen

Dieses Widget zeigt Bedrohungsfunde für die folgenden Bedrohungsarten an:

Tabelle 1-4. Bedrohungsarten

Bedrohungsart	Beschreibung
Virus/Malware	Zeigt die Aktion an, die von einem beliebigen, vom Datenbereich angegebenen verwalteten Produkt für alle Dateien durchgeführt wurde. Beispiel: Bereinigt, Zugriff verweigert usw.
Spyware/Grayware	Zeigt die Aktion an, die von einem beliebigen, vom Datenbereich angegebenen verwalteten Produkt für alle Dateien durchgeführt wurde. Beispiel: erfolgreich, weitere Aktion erforderlich usw.
Inhaltssicherheit	Zeigt die Aktion an, die von einem beliebigen, vom Datenbereich angegebenen verwalteten Produkt für alle E-Mail-Nachrichten durchgeführt wurde. Beispiel: gelöscht, Anhänge entfernt usw.
Websicherheit	Zeigt alle Websicherheitsverstöße an, die mit Hilfe der Richtlinien von allen vom Datenbereich angegebenen verwalteten Produkten gesperrt wurden. Beispiel: Sperren von Dateien, Dateinamen usw.
Netzwerkviren	Zeigt die Aktion an, die von einem beliebigen vom Datenbereich angegebenen verwalteten Produkt für alle Netzwerkviren durchgeführt wurde

Klicken Sie auf das Einstellungssymbol (>), um den Widget-Titel, den Produktumfang oder die Art der angezeigten Bedrohungen zu bearbeiten.

Erkannte Richtlinienverstöße – Widget

Dieses Widget zeigt erkannte Richtlinienverstöße für Network VirusWall Enforcer-Geräte an. Durch Klicken auf Links in der Spalte **Funde** wird ein Fenster mit ausführlichen Informationen geöffnet. Apex Central führt eine Protokollabfrage durch, um ausführliche Informationen bereitzustellen.

Daten	Beschreibung
Typ	Listet **Dienstverstöße** als Sicherheitsbedrohungstyp auf
Aktualisiert	Zuletzt aktualisiert
Funde	Anzahl der Dienstverstöße, die von Network VirusWall Enforcer-Geräten erkannt werden

Klicken Sie auf das Einstellungssymbol (>), um den Widget-Titel oder den Produktumfang zu bearbeiten.

Hinweis

Dieses Widget zeigt ausschließlich Funde erkannter Richtlinienverstöße für Network VirusWall Enforcer an.

Klicken Sie auf **Speichern**, um die Änderungen zu übernehmen und das Widget zu beenden.

C&C-Callback-Ereignisse – Widget

Dieses Widget zeigt die Anzahl der C&C-Callback-Versuche basierend auf den infizierten Hosts oder den Callback-Adressen an. Das Widget kann zu einem Zeitpunkt jeweils nur Daten für eine Art von Information anzeigen. Durch Klicken auf die Zahlen in beliebigen Tabellenzellen wird das Fenster **C&C-Callback-Ereignisse** geöffnet, das die folgenden Übersichtsdaten für Callbacks enthält:

Daten	Beschreibung
Infizierter Host	Betroffene Host- oder E-Mail-Adresse
Callback-Adresse	URL, IP-Adresse oder E-Mail-Adresse, an die ein infizierter Host versucht, einen Callback durchzuführen
C&C-Serverstandort	Bereich und Land, in dem sich der C&C-Server befindet
Callback-Versuche	Anzahl der Kontakte zwischen Callback-Adressen und infizierten Hosts

Daten	Beschreibung
Letzte Callback-Adresse/Infizierter Host	URL, IP-Adresse oder E-Mail-Adresse, für die der letzte Callback-Versuch protokolliert wurde
Callback-Adressen/ Infizierte Hosts (mit in den Spalten angezeigten Zahlen)	Anzahl der infizierten Hosts oder Callback-Adressen, die mit den Callback-Versuchen verknüpft sind
Protokolliert von	Name des verwalteten Produkts, das das Ereignis protokolliert hat

Klicken Sie auf das Einstellungssymbol (>), um Folgendes zu bearbeiten:

- **Titel**: Ändern Sie den Titel des **C&C-Callback-Ereignisse**-Widgets.
- **Bereich**: Klicken Sie auf >> und wählen Sie die übergeordneten Server aus, die das Widget als Quelle nutzt.
- **C&C-Listenquelle**: Wählen Sie **Global Intelligence**, **Virtual Analyzer** oder **Benutzerdefiniert** als C&C-Listenquellen aus.
- **Anzuzeigende Elemente**: Wählen Sie die Anzahl der Elemente aus, die im Widget angezeigt werden sollen.

Klicken Sie auf **Speichern**, um die Änderungen zu übernehmen und das Widget zu beenden.

Kapitel 2

Richtlinienverwaltung

Dieser Abschnitt enthält Informationen zur Durchführung von Richtlinienverwaltung für verwaltete Produkte und Endpunkte.

Wichtig

Jedes verwaltete Produkt bietet unterschiedliche Richtlinieneinstellungen, die Sie konfigurieren und auf Richtlinienziele anwenden können. Eine vollständige Liste der unterstützten verwalteten Produkte und der jeweiligen Richtlinieneinstellungen finden Sie im *Apex Central Widget- und Richtlinienverwaltungsleitfaden*.

Sie können eine PDF-Version des Handbuchs mithilfe des folgenden Links herunterladen:

https://docs.trendmicro.com/de-de/enterprise/apex-central.aspx

Sie können das Handbuch auch online mithilfe des folgenden Links anzeigen:

https://docs.trendmicro.com/de-de/enterprise/apex-central-widget-and-policy-management-guide/introduction.aspx

---

Es werden folgende Themen behandelt:

- *Richtlinienverwaltung auf Seite 2-3*

- *Richtlinienstatus auf Seite 2-31*

Richtlinienverwaltung

Mit Hilfe der Richtlinienverwaltung können Administratoren über eine einzelne Management-Konsole Produkteinstellungen auf verwalteten Produkten und Endpunkten durchsetzen. Administratoren erstellen eine Richtlinie, indem Sie die Ziele auswählen und eine Liste mit Produkteinstellungen konfigurieren.

Zum Durchführen von Richtlinienverwaltung auf einem neu verwalteten Produkt oder Endpunkt verschieben Sie das verwaltete Produkt aus dem Ordner **Neue Entität** in einen anderen Ordner in der Produktverzeichnisstruktur.

Neue Richtlinie erstellen

Wichtig

Jedes verwaltete Produkt bietet unterschiedliche Richtlinieneinstellungen, die Sie konfigurieren und auf Richtlinienziele anwenden können. Eine vollständige Liste der unterstützten verwalteten Produkte und der jeweiligen Richtlinieneinstellungen finden Sie im *Apex Central Widget- und Richtlinienverwaltungsleitfaden*.

Sie können eine PDF-Version des Handbuchs mithilfe des folgenden Links herunterladen:

https://docs.trendmicro.com/de-de/enterprise/apex-central.aspx

Sie können das Handbuch auch online mithilfe des folgenden Links anzeigen:

https://docs.trendmicro.com/de-de/enterprise/apex-central-widget-and-policy-management-guide/introduction.aspx

Prozedur

1. Gehe zu **Richtlinien** > **Richtlinienverwaltung**.

   Das Fenster **Richtlinienverwaltung** wird angezeigt.

2. Wählen Sie den Typ der Produkteinstellungen aus der Produktliste aus.

   Das Fenster wird aktualisiert, um die für das ausgewählte verwaltete Produkt erstellten Richtlinien anzuzeigen.

   Weitere Informationen zum Konfigurieren von Richtlinieneinstellungen für bestimmte verwaltete Produkte finden Sie im *Trend Micro Apex Central Widget- und Richtlinienverwaltungshandbuch*.

3. Klicken Sie auf **Erstellen**.

   Das Fenster **Richtlinie erstellen** wird angezeigt.

4. Geben Sie einen Name der Richtlinie ein.

5. Geben Sie Ziele an.

   Trend Micro Apex Central stellt verschiedene Methoden zum Auswählen von Zielen zur Verfügung, die sich auf die Funktionsweise einer Richtlinie auswirken.

   Hinweis

   Um ein verwaltetes Produkt oder einen verwalteten Endpunkt als Ziel einzubeziehen, stellen Sie sicher, dass die Produktversion des verwalteten Produkts oder Endpunkts die Richtlinienverwaltung in Trend Micro Apex Central unterstützt. Das Fenster **Einstellungen der Richtlinienvorlage** (**Richtlinien** > **Richtlinienressourcen** > **Einstellungen der Richtlinienvorlage**) enthält Informationen über unterstützte Produktversionen.

   In der Liste der Richtlinien sind die Richtlinienziele in folgender Reihenfolge angeordnet:

   - **Ziele angeben**: Verwenden Sie diese Option, um bestimmte Endpunkte oder verwaltete Produkte auszuwählen.

     Weitere Informationen finden Sie unter *Richtlinienziele angeben auf Seite 2-11*.

- **Filtern nach Kriterien**: Verwenden Sie diese Option, um Endpunkte automatisch basierend auf den Filterkriterien zuzuweisen.

  Weitere Informationen finden Sie unter *Filtern nach Kriterien auf Seite 2-7*.

- **Bezeichnungen auswählen**: Verwenden Sie diese Option, um Endpunkte basierend auf Labels zuzuweisen.

  Weitere Informationen finden Sie unter *Bezeichnungen auf Seite 2-13*.

- **Keine (nur Entwurf)**: Verwenden Sie diese Option, um die Richtlinie als Entwurf zu speichern, ohne Ziele auszuwählen.

Weitere Informationen zur Richtlinienliste finden Sie unter *Grundlegendes zur Richtlinienliste auf Seite 2-26*.

6. Klicken Sie auf eine verwaltete Produktfunktion, um sie einzublenden und ihre Einstellungen zu konfigurieren. Wiederholen Sie diesen Schritt, um alle Funktionen konfigurieren.

   - Jede Funktion enthält einen Link zu einem Hilfethema, das die Funktion und deren Verwendung erläutert.
   - Für bestimmte Produkteinstellungen muss Trend Micro Apex Central bestimmte Einstellungsoptionen von den verwalteten Produkten abrufen. Wenn Administratoren mehrere Ziele für eine Richtlinie auswählen, kann Trend Micro Apex Central nur die Einstellungsoptionen vom ersten ausgewählten Ziel abrufen. Um eine erfolgreiche Richtlinienverteilung sicherzustellen, vergewissern Sie sich, dass die Produkteinstellungen auf allen Zielen synchronisiert sind.
   - Wenn Sie eine Richtlinie für **Apex One Security Agent** erstellen, die als übergeordnete Richtlinie für eine zukünftige untergeordnete Richtlinie fungieren soll, konfigurieren Sie Einstellungen, die in der untergeordneten Richtlinie übernommen, angepasst oder erweitert werden können.
     - Eine Liste der Security Agent-Einstellungen, die übernommen, angepasst oder erweitert werden können, finden Sie unter

Mit Einstellungen für übergeordnete Richtlinien arbeiten auf Seite 2-13.

- Weitere Informationen zum Erstellen einer untergeordneten Richtlinie finden Sie unter *Richtlinieneinstellungen übernehmen auf Seite 2-18*.

7. Klicken Sie auf **Verteilen** oder **Speichern**.

   Wenn Sie auf **Verteilen** geklickt haben, startet Trend Micro Apex Central die Verteilung. Die verteilte Richtlinie wird in der Liste im Fenster **Richtlinienverwaltung** angezeigt. Es dauert normalerweise ein paar Minuten, bis Trend Micro Apex Central die Richtlinie auf die Ziele verteilt.

   Klicken Sie im Fenster **Richtlinienverwaltung** auf **Aktualisieren**, um die Statusinformationen in der Richtlinienliste zu aktualisieren. Wenn der Status der Verteilung nach einem längeren Zeitraum immer noch 'Ausstehend' ist, liegen möglicherweise Probleme im Zusammenhang mit den Zielen vor. Überprüfen Sie, ob eine Verbindung zwischen Trend Micro Apex Central und den Zielen vorhanden ist. Überprüfen Sie auch, ob die Ziele ordnungsgemäß arbeiten.

   Sobald Trend Micro Apex Central eine Richtlinie auf die Ziele verteilt, überschreiben die in der Richtlinie definierten Einstellungen die vorhandenen Einstellungen in den Zielen. Trend Micro Apex Central erzwingt die Richtlinieneinstellungen in den Zielen alle 24 Stunden. Obwohl lokale Administratoren Änderungen an den Einstellungen über die Konsole des verwalteten Produkts vornehmen können, werden die Änderungen jedes Mal überschrieben, wenn Trend Micro Apex Central die Richtlinieneinstellungen erzwingt.

   - Trend Micro Apex Central erzwingt die Richtlinieneinstellungen auf den Zielen alle 24 Stunden. Da die Richtliniendurchsetzung nur alle 24 Stunden erfolgt, stimmen die Produkteinstellungen in den Zielen möglicherweise nicht mit den Richtlinieneinstellungen überein, wenn lokale Administratoren während des Durchsetzungszeitraums Änderungen über die Konsole des verwalteten Produkts vornehmen.

- Auf IMSVA-Servern verteilte Richtlinieneinstellungen haben Vorrang vor den bestehenden Einstellungen auf den Zielservern, statt diese zu überschreiben. IMSVA-Server speichern diese Richtlinieneinstellungen ganz oben in der Liste.
- Wenn ein Apex One Security Agent mit einer Trend Micro Apex Central-Richtlinie in eine andere Apex One-Domäne verschoben wurde, werden die Agent-Einstellungen vorübergehend in die von dieser Apex One-Domäne definierten Einstellungen geändert. Sobald Trend Micro Apex Central die Richtlinie erneut erzwingt, entsprechen die Agent-Einstellungen den Richtlinieneinstellungen.

Filtern nach Kriterien

Mit dieser Option können Sie Endpunkte automatisch basierend auf den Filterkriterien auswählen.

Diese Option:

- Steht nur in den folgenden verwalteten Produkten zur Verfügung:
  - Apex One (Mac)
  - Apex One-Prävention vor Datenverlust
  - Apex One Security Agent
  - Mobile Security for Enterprise
  - Trend Micro Endpoint Application Control
- Verwendet einen Filter, um der Richtlinie automatisch aktuelle und zukünftige Ziele zuzuweisen
- Ist nützlich für die Verteilung von Standardeinstellungen auf einer Gruppe von Zielen

Administratoren können die Priorität der gefilterten Richtlinien in der Richtlinienliste ändern. Wenn ein Administrator die Richtlinienliste neu sortiert, weist Trend Micro Apex Central die Ziele anderen gefilterten Richtlinien basierend auf den Zielkriterien und den Benutzerrollen für jeden Ersteller einer Richtlinie zu.

Trend Micro Apex Central kann einer neuen gefilterten Richtlinie nur Endpunkte ohne Richtlinien zuweisen. Um einen Endpunkt, der bereits einer gefilterten Richtlinie zugewiesen ist, neu zuzuordnen, verschieben Sie eine andere gefilterte Richtlinie mit den passenden Kriterien in der Prioritätenliste nach oben.

Siehe *Endpunkte gefilterten Richtlinien zuweisen auf Seite 2-9*, um weitere Informationen darüber zu erhalten, wie Trend Micro Apex Central Ziele auf gefilterte Richtlinien zuweisen.

Prozedur

1. Navigieren Sie im Fenster **Richtlinie erstellen** zum Abschnitt **Ziele**, wählen Sie **Filtern nach Kriterien** aus und klicken Sie dann auf **Filter festlegen**.

   Das Fenster **Filtern nach Kriterien** wird angezeigt.

2. Wählen Sie die folgenden Optionen aus und legen Sie die Kriterien fest.

Kriterien	Beschreibung
Schlüsselwörter abgleichen in	Definieren Sie Schlüsselwörter basierend auf dem Hostnamen oder dem Trend Micro Apex Central-Anzeigenamen. **Hinweis** Trend Micro Apex Central führt den Teilabgleich für die Suche nach einzelnen Schlüsselwörtern durch. Sie können nach mehreren durch Kommas getrennten Schlüsselwörtern suchen. Trend Micro Apex Central bietet jedoch nur vollständige Zeichenfolgenübereinstimmungen für jedes angegebene Schlüsselwort.

KRITERIEN	BESCHREIBUNG
IP-Adressen	Definieren Sie einen Bereich von IP-Adressen und klicken Sie auf **Hinzufügen**. **Hinweis** • Die Richtlinienverwaltung unterstützt nur IPv4-Adressen. • Wenn ein neues verwaltetes Produkt oder ein Endpunkt bei Trend Micro Apex Central registriert wird, dauert es etwa eine Stunde, bis das verwaltete Produkt oder der Endpunkt für die Suche nach IP-Adresse verfügbar ist.
Betriebssysteme	Wählen Sie ein oder mehrere Betriebssysteme in der Dropdown-Liste aus.
Verzeichnisse	Wählen Sie eines der folgenden Verzeichnisse aus und legen Sie die Kriterien fest. • **Produktverzeichnis**: Wählen Sie Ordner in der Produktverzeichnisstruktur aus • **Active Directory**: Wählen Sie Organisationseinheiten in einer integrierten Active Directory-Struktur aus • **Apex One Domänenhierarchie**: Geben Sie mindestens ein Domänenhierarchie-Schlüsselwort von Apex One ein

3. Klicken Sie auf **Save**.

   Das Fenster **Richtlinie erstellen** wird neu geladen.

Endpunkte gefilterten Richtlinien zuweisen

Wenn ein neuer Endpunkt bei Trend Micro Apex Central registriert wird, durchläuft er die gefilterten Richtlinien in der Liste in absteigender Reihenfolge. Trend Micro Apex Central weist den neuen Endpunkt einer gefilterten Richtlinie zu, wenn die folgenden beiden Bedingungen erfüllt sind:

- Der neue Endpunkt erfüllt die Zielkriterien in der Richtlinie
- Der Verfasser der Richtlinie verfügt über die Berechtigung, den neuen Endpunkt zu verwalten

Die gleiche Aktion gilt für einen Endpunkt, der bereits einer Richtlinie zugewiesen ist. Der Ersteller der Richtlinie löscht die Richtlinie jedoch zu einem späteren Zeitpunkt.

Hinweis

Für Endpunkte, die soeben bei Trend Micro Apex Central registriert wurden, und für diejenigen, die soeben von gelöschten Richtlinien freigegeben wurden, gibt es eine dreiminütige Übergangsfrist, während der keine Endpunktzuordnung erfolgt. Diese Endpunkte sind während dieses Zeitraums vorübergehend ohne Richtlinien.

Wenn ein Endpunkt die Zielkriterien in gefilterten Richtlinien nicht erfüllt, wird der Endpunkt keinen Richtlinien zugeordnet. Trend Micro Apex Central weist diese Endpunkte erneut zu, wenn die folgenden Aktionen stattfinden:

- Neue gefilterte Richtlinie erstellen
- Gefilterte Richtlinie bearbeiten
- Gefilterte Richtlinien neu anordnen
- Täglicher Zeitplan für die Zuordnung von Endpunkten

  Trend Micro Apex Central verwendet einen täglichen Zeitplan für die Zuordnung von Endpunkten, um sicherzustellen, dass Endpunkte den richtigen Richtlinien zugewiesen werden. Diese Aktion findet täglich um 15:15 Uhr statt. Wenn sich Endpunkteigenschaften ändern, wie beispielsweise das Betriebssystem oder die IP-Adresse, müssen sie mit Hilfe des täglichen Zeitplans den richtigen Richtlinien erneut zugewiesen werden.

Hinweis

- Falls die Endpunkte offline sind, wenn die tägliche Endpunktzuordnung gemäß dem Zeitplan erfolgt, bleibt der Richtlinienstatus für diese Endpunkte so lange 'Ausstehend', bis sie wieder online geschaltet werden.
- Wenn die Apex One-Domäne des Endpunkts geändert wird, setzt Trend Micro Apex Central die aktualisierte Richtlinie nach 10 Minuten um.

Wenn die oben angegebenen Aktionen durchgeführt werden, ordnet Trend Micro Apex Central Endpunkte basierend auf folgenden Bedingungen zu:

TABELLE 2-1. Endpunktzuordnung für gefilterte Richtlinien

	Neue Endpunkte oder Endpunkte aus gelöschten Richtlinien	Endpunkte ohne Richtlinien	Endpunkte mit Richtlinien
Neue Richtlinie erstellen		●	
Richtlinie bearbeiten	●	●	●
Gefilterte Richtlinien neu anordnen	●	●	●
Täglicher Zeitplan für die Zuordnung von Endpunkten	●	●	●

Richtlinienziele angeben

Verwenden Sie diese Option, um bestimmte Endpunkte oder verwaltete Produkte auszuwählen.

Diese Option:

- Verwendet die Funktionen zum Durchsuchen und Suchen, um bestimmte Ziele zu finden und sie manuell einer Richtlinie zuzuweisen
- Ist hilfreich, wenn Administratoren bestimmte Einstellungen nur auf bestimmte Ziele verteilen möchten

- Bleibt an statischer Position ganz oben in der Richtlinienliste und hat eine höhere Priorität als alle gefilterten Richtlinien.

Prozedur

1. Navigieren Sie im Fenster **Richtlinie erstellen** zum Abschnitt **Ziele**, wählen Sie **Ziel(e) festlegen** aus und klicken Sie dann auf **Auswählen**.

   Das Fenster **Ziele festlegen** wird angezeigt.

2. Verwenden Sie **Suchen** oder **Durchsuchen**, um die Ziele zu lokalisieren.

   - **Suchen**: Verwenden Sie die folgenden Suchkriterien, um Endpunkte oder verwaltete Produkte zu finden. Die Suchergebnisse zeigen die Endpunkte oder die verwalteten Produkte an, die allen ausgewählten Kriterien entsprechen.
     - **Schlüsselwörter abgleichen in**: Definieren Sie Schlüsselwörter basierend auf dem Hostnamen oder dem Trend Micro Apex Central-Anzeigenamen.
     - **IP-Adressen**: Definieren Sie einen Bereich von IP-Adressen und klicken Sie auf **Hinzufügen**.

       Hinweis

       - Die Richtlinienverwaltung unterstützt nur IPv4-Adressen.
       - Wenn ein neues verwaltetes Produkt oder ein Endpunkt bei Trend Micro Apex Central registriert wird, dauert es etwa eine Stunde, bis das verwaltete Produkt oder der Endpunkt für die Suche nach IP-Adresse verfügbar ist.

     - **Betriebssysteme**: Wählen Sie ein oder mehrere Betriebssysteme in der Dropdown-Liste aus.
   - **Durchsuchen**: Durchsuchen Sie das Produktverzeichnis oder die Active Directory, um Endpunkte oder verwaltete Produkte zu finden, die der Richtlinie zugewiesen werden sollen.

3. Wählen Sie die Endpunkte oder die verwalteten Produkte aus und klicken Sie auf **Ausgewählte Ziele hinzufügen**.

4. Warten Sie, bis sich die Zahlen in **Aktionsliste anzeigen** und **Ergebnisse anzeigen** ändern.
5. Klicken Sie auf **OK**.

   Das Fenster **Richtlinie erstellen** wird neu geladen.

Bezeichnungen

Labels sind eine Variation des bestehenden Tagging-Systems, die auch eine Filterfunktion bieten. Sie können Labels erstellen und manuell Endpunkten zuweisen, als ob Sie Tags/Filter verwenden würden. Sie können auch Auto-Label-Regeln erstellen, um Labels automatisch Endpunkten zuzuweisen, die bestimmten Kriterien entsprechen. Nachdem Sie ein Label oder eine Auto-Label-Regel erstellt haben, können Sie Labels für Richtlinien, Protokollabfragen oder Berichte verwenden.

Mit Einstellungen für übergeordnete Richtlinien arbeiten

Trend Micro Apex Central-Administratoren, die eine übergeordnete Richtlinie für ein **Apex One Agent** erstellen, können bestimmte Richtlinieneinstellungen konfigurieren, die vererbt, angepasst oder erweitert werden können.

Hinweis

Diese Optionen stehen für andere verwaltete Produkte nicht zur Verfügung.

- **Von übergeordneter Richtlinie übernehmen**
  - Ein Administrator für untergeordnete Richtlinien kann die Einstellung nicht ändern. Ein Apex One-Administrator kann die Einstellung manuell über die Konsole des Apex One-Servers ändern. Die Einstellung wird jedoch überschrieben, wenn Trend Micro Apex Central Richtlinien auf dem Apex One-Server bereitstellt.

    Ein Trend Micro Apex Central-Administrator kann beispielsweise eine untergeordnete Richtlinie erstellen, die den Ausschluss von PDF-Dateien aus der manuellen Suche erzwingt.

- Änderungen an der Einstellung in der übergeordneten Richtlinie werden immer in der untergeordneten Richtlinie durchgesetzt.
- Wenn die Berechtigung in der übergeordneten Richtlinie von „Von übergeordneter Richtlinie übernehmen“ in „Sind anpassbar“ oder „Erweitern von übergeordneter Richtlinie“ geändert wird, kann der Administrator für untergeordnete Richtlinien die aktuelle Einstellung anpassen oder erweitern. Änderungen an der Einstellung in der übergeordneten Richtlinie werden nicht mehr durchgesetzt.

- **Sind anpassbar**
  - Eine untergeordnete Richtlinie kann von der in der übergeordneten Richtlinie konfigurierten Einstellung abweichen.

    Beispiel: Wenn die zeitgesteuerte Suche in der übergeordneten Richtlinie wöchentlich ausgeführt wird, die Einstellung aber anpassbar ist, kann der Administrator für untergeordnete Richtlinien den Zeitplan in „Täglich“ ändern.
  - Änderungen an der Einstellung in der übergeordneten Richtlinie werden niemals in der untergeordneten Richtlinie durchgesetzt.
  - Wenn die Berechtigung in der übergeordneten Richtlinie von „Sind anpassbar“ in „Von übergeordneter Richtlinie übernehmen“ geändert wird, überschreibt die aktuelle Einstellung in der übergeordneten Richtlinie die Einstellung in der untergeordneten Richtlinie. Änderungen an der Einstellung in der übergeordneten Richtlinie werden immer durchgesetzt.

- **Erweitern von übergeordneter Richtlinie**
  - Ein Administrator für untergeordnete Richtlinien kann Ergänzungen zu den in der übergeordneten Richtlinie konfigurierten Elementen vornehmen.

    Beispiel: Wenn die übergeordnete Richtlinie 20 Dateinamen aus der manuellen Suche ausschließt, kann der Administrator 10 weitere sichere und vertrauenswürdige Dateien zur untergeordneten Richtlinie hinzufügen.

- Elemente, die aus der übergeordneten Richtlinie entfernt oder dieser hinzugefügt werden, werden auch aus der untergeordneten Richtlinie entfernt oder dieser hinzugefügt. Ein entferntes Element kann erneut zur untergeordneten Richtlinie hinzugefügt werden.
- Wenn die Berechtigung in der übergeordneten Richtlinie von „Erweitern von übergeordneter Richtlinie“ in „Von übergeordneter Richtlinie übernehmen“ geändert wird, werden Elemente in der untergeordneten Richtlinie ohne Entsprechung in der übergeordneten Richtlinie entfernt. Änderungen an den Elementen in der übergeordneten Richtlinie werden immer durchgesetzt.

In der folgenden Tabelle werden die Einstellungen für übergeordnete Richtlinien aufgelistet, die vererbt, angepasst oder erweitert werden können.

Einstellung und Pfad	Verfügbare Optionen		
	Von übergeordneter Richtlinie übernehmen	Sind anpassbar	Erweitern von übergeordneter Richtlinie
Zeitplan für die Suche **Einstellungen für die zeitgesteuerte Suche** > Registerkarte **Ziel** > Bereich **Zeitplan**	●	●	
Zu durchsuchende Dateierweiterungen **Manuelle Suche / Echtzeitsuche / Jetzt durchsuchen / Einstellungen für die zeitgesteuerte Suche** > Registerkarte **Ziel** > Abschnitt **Zu durchsuchende Dateien** > Option **Dateien mit den folgenden Erweiterungen**	●		●

Einstellung und Pfad	Verfügbare Optionen		
	Von übergeordneter Richtlinie übernehmen	Sind anpassbar	Erweitern von übergeordneter Richtlinie
Suchausschlussliste (Verzeichnisse, Dateien und Dateierweiterungen, die von der Suche ausgeschlossen werden) **Manuelle Suche / Echtzeitsuche / Jetzt durchsuchen / Einstellungen für die zeitgesteuerte Suche** > Registerkarte **Suchausschluss**	●		● **Hinweis** Bei Auswahl von **Erweitern von übergeordneter Richtlinie** aus einer Suchausschlussliste wird in der entsprechenden Liste der Bereich **Einschränkungen für untergeordnete Richtlinien** angezeigt, in dem Ersteller übergeordneter Richtlinien Elemente angeben können, die untergeordnete Richtlinien nicht aus Suchläufen ausschließen können.
Zulässige Programme **Verhaltensüberwachung**>**Ausnahmen** Registerkarte	●		●

Einstellung und Pfad	Verfügbare Optionen		
	Von übergeordneter Richtlinie übernehmen	Sind anpassbar	Erweitern von übergeordneter Richtlinie
Gesperrte Programme **Verhaltensüberwachung>Ausnahmen** Registerkarte	●		●
Ausnahmen **Vorausschauendes Maschinenlernen**	●		●
Liste der vertrauenswürdigen Programme **Liste der vertrauenswürdigen Programme**	●		●

Richtlinieneinstellungen kopieren

Administratoren können die Einstellungen aus einer vorhandenen Richtlinie kopieren, eine neue Richtlinie mit den gleichen Einstellungen erstellen und die Einstellungen an verschiedene Endpunkte oder verwaltete Produkte verteilen.

Hinweis

Es ist nicht möglich, die Einstellungen einer untergeordneten **Apex One Agent**-Richtlinie zu kopieren. Um zu ermitteln, ob die **Apex One Agent**-Richtlinie eine unter- oder eine übergeordnete Richtlinie ist, überprüfen Sie die Spalte **Übergeordnete Richtlinie**. Ein Wert, auf den geklickt werden kann, zeigt an, ob es sich um eine untergeordnete Richtlinie handelt. Andernfalls wird N/V angezeigt.

Prozedur

1. Navigieren Sie zu **Richtlinien** > **Richtlinienverwaltung**.

   Das Fenster **Richtlinienverwaltung** wird angezeigt.

2. Wählen Sie den Typ der Produkteinstellungen aus der Produktliste aus.

   Das Fenster wird aktualisiert, um die für das ausgewählte verwaltete Produkt erstellten Richtlinien anzuzeigen.

3. Wählen Sie eine Richtlinie aus der Liste aus.

4. Klicken Sie auf **Einstellungen kopieren**.

   Das Fenster **Richtlinie kopieren und erstellen** wird angezeigt.

5. Geben Sie im Feld **Name der Richtlinie** einen Namen für die Richtlinie ein.

6. Weisen Sie der Richtlinie **Ziele** zu.

7. (Optional) Ändern Sie die Einstellungen nach Bedarf.

8. Klicken Sie auf **Deploy**.

Hinweis

- Nachdem Sie auf **Verteilen** geklickt haben, warten Sie zwei Minuten, bis Trend Micro Apex Central die Richtlinie an die Ziele verteilt. Klicken Sie im Fenster **Richtlinienverwaltung** auf **Aktualisieren**, um die Statusinformationen in der Richtlinienliste zu aktualisieren.
- Trend Micro Apex Central erzwingt die Richtlinieneinstellungen auf den Zielen alle 24 Stunden.

Richtlinieneinstellungen übernehmen

Erstellen Sie eine neue untergeordnete Richtlinie, indem Sie die Einstellungen einer vorhandenen übergeordneten Richtlinie übernehmen. Eine untergeordnete Richtlinie konnte nicht kopiert werden, und die Einstellungen können nicht übernommen werden.

Diese Aufgabe erfordert eine übergeordnete Richtlinie für den Apex One-Agent. Eine übergeordnete Richtlinie für den Apex One-Agent hat den Wert **N/V**, der unter der Spalte **Übergeordnete Richtlinie** angezeigt wird.

Prozedur

1. Navigieren Sie zu **Richtlinien** > **Richtlinienverwaltung**.

   Das Fenster **Richtlinienverwaltung** wird angezeigt.

2. Wählen Sie in der Produktliste **Apex One Agent** aus.

   Das Fenster wird aktualisiert, um die für das ausgewählte verwaltete Produkt erstellten Richtlinien anzuzeigen.

3. Wählen Sie eine übergeordnete Richtlinie aus, die nicht über lokal verwaltete Einstellungen verfügt.

4. Klicken Sie auf **Einstellungen übernehmen**.

   Das Fenster **Richtlinie vererben und erstellen** wird angezeigt.

5. Geben Sie im Feld **Name der Richtlinie** einen Namen für die Richtlinie ein.

6. Weisen Sie der Richtlinie **Ziele** zu.

7. (Optional) Überprüfen Sie die Einstellungen, die angepasst oder erweitert werden können, und nehmen Sie dann die erforderlichen Änderungen vor. Eine Liste der zu überprüfenden Einstellungen finden Sie unter *Mit Einstellungen für übergeordnete Richtlinien arbeiten auf Seite 2-13*.

   Hinweis

   Eine Einstellung kann nicht angepasst oder erweitert werden, wenn die für die übergeordnete Richtlinie ausgewählte Option **Von übergeordneter Richtlinie übernehmen** ist.

   Beispiel:

- Wenn die Einstellung 'Zeitgesteuerte Suche' anpassbar ist, können Sie den Zeitplan von 'Wöchentlich' in 'Täglich' ändern.
- Wenn die Ausschlussliste für die Echtzeitsuche erweitert werden kann, können Sie zusätzliche Dateinamen eingeben, die Sie als sicher und vertrauenswürdig erachten. Nachdem die untergeordnete Richtlinie erstellt wurde, werden diese Dateinamen der Ausschlussliste für die Suche hinzugefügt.

8. Klicken Sie auf **Deploy**.

Hinweis

- Nachdem Sie auf **Verteilen** geklickt haben, warten Sie zwei Minuten, bis Trend Micro Apex Central die Richtlinie an die Ziele verteilt. Klicken Sie im Fenster **Richtlinienverwaltung** auf **Aktualisieren**, um die Statusinformationen in der Richtlinienliste zu aktualisieren.
- Trend Micro Apex Central erzwingt die Richtlinieneinstellungen auf den Zielen alle 24 Stunden.

Richtlinien ändern

Administratoren können Richtlinienziele und Einstellungen nach Bedarf ändern. Der Besitzer des Stammkonto kann jede Richtlinie in der Liste ändern, während andere Kontobesitzer nur die Richtlinien ändern können, die sie erstellt haben. Nachdem eine Richtlinie geändert wurde, verteilt Trend Micro Apex Central die Richtlinie auf den Zielen.

Wichtig

Jedes verwaltete Produkt bietet unterschiedliche Richtlinieneinstellungen, die Sie konfigurieren und auf Richtlinienziele anwenden können. Eine vollständige Liste der unterstützten verwalteten Produkte und der jeweiligen Richtlinieneinstellungen finden Sie im *Apex Central Widget- und Richtlinienverwaltungsleitfaden*.

Sie können eine PDF-Version des Handbuchs herunterladen oder das Handbuch online mithilfe des folgenden Links anzeigen:

https://docs.trendmicro.com/de-de/enterprise/apex-central.aspx

Wenn Sie die Ziele und Einstellungen für bestimmte Funktionen geändert haben, werden bei einer übergeordneten Richtlinie für den Apex One-Agent die Änderungen auf alle untergeordneten Richtlinien angewendet und auf die entsprechenden Ziele verteilt. Einige Einstellungen einer übergeordneten Richtlinie unterstützen **Berechtigungen**, die für untergeordnete Richtlinien zulässige Änderungen steuern. Änderungen an diesen übergeordneten Richtlinienberechtigungen werden auch auf untergeordnete Richtlinien angewendet und auf Ziele verteilt. Eine Liste der Einstellungen, die Berechtigungen unterstützen, finden Sie unter *Mit Einstellungen für übergeordnete Richtlinien arbeiten auf Seite 2-13*.

Beispiel:

- Wenn Sie die Berechtigung 'Zeitplan durchsuchen' für den Suchzeitplan von 'Von übergeordneter Richtlinie übernehmen' in 'Sind anpassbar' geändert haben, können Administratoren mit dem Anpassen des vorhandenen Zeitplans für ihre untergeordneten Richtlinien beginnen.
- Wenn Sie die Berechtigung 'Manuelle Suche (Dateierweiterungen)' von 'Von übergeordneter Richtlinie erweitern' in 'Von übergeordneter Richtlinie übernehmen' geändert haben, werden alle Dateierweiterungen, die Administratoren zu untergeordneten Richtlinien hinzugefügt haben, entfernt. Außerdem können Administratoren keine Dateierweiterungen mehr hinzufügen.

Prozedur

1. Navigieren Sie zu **Richtlinien** > **Richtlinienverwaltung**.

   Das Fenster **Richtlinienverwaltung** wird angezeigt.

2. Wählen Sie den Typ der Produkteinstellungen aus der Produktliste aus.

   Das Fenster wird aktualisiert, um die für das ausgewählte verwaltete Produkt erstellten Richtlinien anzuzeigen.

3. Klicken Sie auf den Namen einer Richtlinie in der Spalte **Richtlinie**.

   Das Fenster **Richtlinie bearbeiten** wird angezeigt.

4. Ändern Sie die Richtlinie.

   Hinweis

   Das Ändern der Filterkriterien in einer gefilterten Richtlinie kann sich auf die Zielzuordnung auswirken. Trend Micro Apex Central weist einige Ziele möglicherweise anderen gefilterten Richtlinien neu zu oder fügt der aktuellen Richtlinie zusätzliche Ziele hinzu.

5. Klicken Sie auf **Deploy**.

   Es kann einige Zeit dauern, bis Trend Micro Apex Central die Richtlinie auf die Ziele verteilt. Klicken Sie im Fenster **Richtlinienverwaltung** auf **Aktualisieren**, um die Statusinformationen in der Richtlinienliste zu aktualisieren. Wenn der Status der Verteilung nach einem längeren Zeitraum immer noch 'Ausstehend' ist, liegen möglicherweise Probleme im Zusammenhang mit den Zielen vor. Überprüfen Sie, ob eine Verbindung zwischen Trend Micro Apex Central und den Zielen vorhanden ist. Überprüfen Sie auch, ob die Ziele ordnungsgemäß arbeiten.

   Trend Micro Apex Central erzwingt die Richtlinieneinstellungen auf den Zielen alle 24 Stunden.

Richtlinien importieren und exportieren

Exportieren Sie Richtlinien für Sicherungen oder um einen anderen Trend Micro Apex Central-Server derselben Version zu importieren.

Hinweis

- Trend Micro Apex Central exportiert Richtlinieneinstellungen, aber keine Richtlinienziele.
- Eine übergeordnete Richtlinie bleibt auch nach dem Export oder Import eine übergeordnete Richtlinie.
- Eine untergeordnete Richtlinie wird nach dem Export zu einer übergeordneten Richtlinie. Somit ist sie nach dem Import auch eine übergeordnete Richtlinie.
- Trend Micro Apex Central kann eine Richtlinie nicht importieren, wenn ihr Name mit dem einer vorhandenen untergeordneten Richtlinie identisch ist. Falls die vorhandene Richtlinie keine untergeordnete Richtlinie ist, wird sie von Trend Micro Apex Central nach dem Import überschrieben.
- Weitere Informationen finden Sie in folgenden Themen:
  - *Neue Richtlinie erstellen auf Seite 2-3*
  - *Richtlinieneinstellungen übernehmen auf Seite 2-18*

Prozedur

1. Navigieren Sie zu **Richtlinien** > **Richtlinienverwaltung**.

   Das Fenster **Richtlinienverwaltung** wird angezeigt.

2. Wählen Sie den Typ der Produkteinstellungen aus der Produktliste aus.

   Das Fenster wird aktualisiert, um die für das ausgewählte verwaltete Produkt erstellten Richtlinien anzuzeigen.

3. Wählen Sie zum Exportieren eine oder mehrere Richtlinien aus, klicken Sie auf **Einstellungen exportieren** und speichern Sie dann die sich ergebende Richtliniendatei.

   - Wenn Sie eine einzelne Richtlinie exportiert haben, hat die sich ergebende Datei die Erweiterung `*.cmpolicy`.
   - Falls Sie mehrere Richtlinien importiert haben, ist die sich ergebende Datei eine komprimierte Datei (`*.zip`), die die einzelnen `.cmpolicy`-Dateien enthält.

4. Klicken Sie zum Importieren auf **Einstellungen importieren** und suchen und laden Sie dann die Richtliniendatei.

   - Sie können eine vollständige `*.zip`-Datei oder einzelne `*.cmpolicy`-Dateien nacheinander importieren.
   - Wenn die Richtlinie in der Richtlinienliste bereits vorhanden ist, wird eine Bestätigungsabfrage angezeigt, in der Sie gefragt werden, ob Sie die vorhandene Richtlinie überschreiben möchten.

     Klicken Sie zum Fortfahren auf **OK**.

   Das Fenster wird aktualisiert und enthält dann die importierte Richtlinie oben in der Liste.

   Weitere Informationen zum Neuanordnen der Richtlinienliste finden Sie unter *Richtlinienliste neu ordnen auf Seite 2-30*.

Richtlinie löschen

Administratoren können eine Richtlinie aus der Liste entfernen. Trend Micro Apex Central weist die mit der gelöschten Richtlinie verknüpften Ziele neu zu, wenn die Ziele den Filterkriterien einer anderen Richtlinie entsprechen. Diejenigen ohne Übereinstimmung werden zu Endpunkten ohne Richtlinien. Sie behalten die von der gelöschten Richtlinie definierten Einstellungen bei, es sei denn der Administrator eines verwalteten Produkts ändert die Einstellungen.

Trend Micro Apex Central gestattet nur Richtlinienerstellern das Löschen ihrer eigenen Richtlinien. Das Stammkonto kann jedoch jede Richtlinie in der Liste löschen.

Es ist nicht möglich, eine übergeordnete Apex One-Agent-Richtlinie mit Einstellungen, die von einer vorhandenen untergeordneten Richtlinie *übernommen* wurden, zu löschen.

Prozedur

1. Navigieren Sie zu **Richtlinien** > **Richtlinienverwaltung**.

   Das Fenster **Richtlinienverwaltung** wird angezeigt.

2. Wählen Sie den Typ der Produkteinstellungen aus der Produktliste aus.

   Das Fenster wird aktualisiert, um die für das ausgewählte verwaltete Produkt erstellten Richtlinien anzuzeigen.

3. Wählen Sie die zu löschende Richtlinie aus.

4. Klicken Sie auf **Löschen**.

   Ein Bestätigungsfenster wird angezeigt.

5. Klicken Sie auf **OK**.

Richtlinienbesitzer ändern

Der standardmäßige Besitzer einer Richtlinie ist das Benutzerkonto, das die Richtlinie erstellt hat. Im Fenster **Richtlinienverwaltung** können Sie den Besitzer einer Richtlinie in ein beliebiges Trend Micro Apex Central-Benutzerkonto ändern. Sie können den Besitzer der Richtlinie auch in eine Active Directory-Gruppe ändern. Dadurch werden alle Active Directory-Benutzer in der Gruppe als Besitzer der Richtlinie festgelegt.

Wichtig

Wenn Sie den Besitzer einer Richtlinie in ein Benutzerkonto ändern, das keine Zugriffsrechte für die angegebenen Ziele hat, kann der neue Besitzer die Richtlinieneinstellungen ändern, aber die Richtliniendaten nicht anzeigen.

Prozedur

1. Navigieren Sie zu **Richtlinien** > **Richtlinienverwaltung**.

   Das Fenster **Richtlinienverwaltung** wird angezeigt.

2. Wählen Sie eine oder mehrere Richtlinien aus, deren Besitzer geändert werden soll.

3. Klicken Sie auf **Besitzer ändern**.

   Das Fenster **Richtlinienbesitzer ändern** wird angezeigt.

4. Wählen Sie ein Benutzerkonto aus der Dropdown-Liste aus.

5. Klicken Sie auf **Speichern**, um den Besitzer zu ändern.

   Trend Micro Apex Central sendet eine E-Mail-Benachrichtigung an alle Benutzerkonten, die der Rolle „Administrator“ zugewiesen sind.

Grundlegendes zur Richtlinienliste

In der Richtlinienliste werden die Informationen und der Status der Richtlinien angezeigt, die von allen Benutzern erstellt wurden. Wenn ein neuer Endpunkt bei Trend Micro Apex Central registriert wird, durchläuft er die gefilterten Richtlinien in der Liste in absteigender Reihenfolge. Trend Micro Apex Central weist den neuen Endpunkt einer gefilterten Richtlinie zu, wenn die folgenden beiden Bedingungen erfüllt sind:

- Der neue Endpunkt stimmt mit dem Zielkriterium der Richtlinie überein
- Der Verfasser der Richtlinie verfügt über die Berechtigung, den neuen Endpunkt zu verwalten

In der folgenden Tabelle werden die Listenspalten mit Richtlinien beschrieben, die im Fenster **Richtlinienverwaltung** angezeigt werden. Klicken Sie auf eine Spalte, um die Daten zu sortieren.

TABELLE 2-2. Richtlinienliste

SPALTE	BESCHREIBUNG
Priorität	Zeigt die Priorität der Richtlinien an • In Trend Micro Apex Central werden Richtlinien von der höchsten bis zur niedrigsten Priorität angezeigt. • Wenn Administratoren eine gefilterte Richtlinie erstellen, speichert Trend Micro Apex Central die neue Richtlinie mit der niedrigsten Priorität. • Eine angegebene Richtlinie hat Vorrang vor gefilterten Richtlinien und wird weiterhin oben in der Liste angezeigt. Administratoren können angegebene Richtlinien nicht neu sortieren. • Trend Micro Apex Central platziert Entwurfsrichtlinien unten in der Liste.
Richtlinie	Zeigt den Namen der Richtlinie an
Richtlinienversion	Diese Spalte wird nur dann angezeigt, wenn es sich bei dem ausgewählten Produkt um **Apex One Security Agent** handelt. Zeigt die neueste bereitgestellte Richtlinienversion an **Hinweis** Einige Ziele haben möglicherweise nicht die neueste Richtlinienversion implementiert. Um die aktuelle Richtlinie auf bestimmten Zielen anzuzeigen, klicken Sie auf die Zahl in der **Verteilt**-Spalte.
Übergeordnete Richtlinie	Diese Spalte wird nur dann angezeigt, wenn es sich bei dem ausgewählten Produkt um **Apex One Security Agent** handelt. Für eine untergeordnete Richtlinie (d. h., die entsprechenden Einstellungen stammen aus einer übergeordneten Richtlinie) wird in dieser Spalte der Name der übergeordneten Richtlinie angezeigt. Andernfalls wird "n. v." angezeigt.

Spalte	Beschreibung
Abweichungen	Diese Spalte wird nur dann angezeigt, wenn es sich bei dem ausgewählten Produkt um **Apex One Security Agent** handelt. Für eine untergeordnete Richtlinie wird in dieser Spalte die Anzahl der Einstellungen angezeigt, die für die Richtlinie geändert wurden und deshalb nicht mit den Einstellungen der übergeordneten Richtlinie übereinstimmen. Wenn die Einstellungen zwischen der Richtlinie und seiner übergeordneten Richtlinie übereinstimmen, wird 0 (Null) angezeigt. Handelt es sich bei der Richtlinie nicht um eine untergeordnete Richtlinie wird "n. v." angezeigt.
Besitzer	Zeigt den Benutzer an, dem die Richtlinie aktuell zugewiesen ist **Hinweis** Standardmäßig ist der Besitzer der Benutzer, der die Richtlinie erstellt hat. • Wenn Sie den Besitzer einer Richtlinie in ein Benutzerkonto ändern, das keine Zugriffsrechte für die angegebenen Ziele hat, kann der neue Besitzer die Richtlinieneinstellungen ändern, aber die Richtliniendaten nicht anzeigen. • Sie können auch mehrere Eigentümer zuweisen, indem Sie die Richtlinie einer Active Directory-Gruppe zuordnen. Weitere Informationen finden Sie unter *Richtlinienbesitzer ändern auf Seite 2-25*.
Letzter Editor	Zeigt den Benutzer an, der die Richtlinie zuletzt bearbeitet hat
Zuletzt bearbeitet	Diese Spalte wird nur dann angezeigt, wenn es sich bei dem ausgewählten Produkt um **Apex One Security Agent** handelt. Zeigt an, wann die Richtlinie zuletzt bearbeitet wurde

Spalte	Beschreibung
Ziele	Zeigt an, wie Administratoren Ziele für die Richtlinie auswählen. • **Angegeben**: Verwendet die Funktion zum Durchsuchen oder Suchen, um bestimmte Ziele für die Richtlinie auszuwählen. Angegebene Richtlinien bleiben statisch ganz oben in der Richtlinienliste und haben eine höhere Priorität als jede gefilterte Richtlinie. • **Gefiltert**: Verwendet einen Filter, um der Richtlinie automatisch aktuelle und zukünftige Endpunkte zuzuweisen. Administratoren können die Priorität der gefilterten Richtlinien neu anordnen. Zeigen Sie mit dem Mauszeiger auf ein Element, um die Filterkriterien anzuzeigen und gegebenenfalls Anpassungen vorzunehmen. • **Bezeichnung**: Verwendet Endpunkt-Labels, um Endpunkte der Richtlinie zuzuweisen. • **Keine**: Der Ersteller der Richtlinie hat die Richtlinie als Entwurf gespeichert, ohne Ziele auszuwählen.
Verteilt	Zeigt die Anzahl der Ziele an, auf die die Richtlinieneinstellungen angewendet wurden oder die über nicht aktivierte Produktdienste verfügen Klicken Sie auf die Zahl, um den Status der Richtlinie anzuzeigen.
Ausstehend	Zeigt die Anzahl der Ziele an, auf die die Richtlinien nicht angewendet wurden Klicken Sie auf die Zahl, um den Status der Richtlinie anzuzeigen.
Offline	Zeigt die Anzahl der Ziele an, die über Offline-Agents verfügen Klicken Sie auf die Zahl, um den Status der Richtlinie anzuzeigen.
Mit Problemen	Zeigt die Anzahl der Ziele an, auf die die Richtlinieneinstellungen aus folgenden Gründen nicht angewendet wurden: nicht unterstützte Richtlinienbereitstellung, keine Richtlinienkonfiguration, Systemfehler, Fehler bei der Kommunikation des Endpunkts mit dem Produktserver, nicht unterstützte Endpunkte, lokal geänderte Einstellungen, deaktivierte Produktdienste oder teilweise Bereitstellung Klicken Sie auf die Zahl, um den Status der Richtlinie anzuzeigen.

Hinweis

Bei den Zahlen in den Spalten **Bereitgestellt** und **Ausstehend** handelt es sich ausschließlich um die verwalteten Produkte oder Endpunkte, die von einem Administrator verwaltet werden dürfen.

Richtlinienliste neu ordnen

Administratoren können die Schaltfläche **Neu anordnen** verwenden, um die Reihenfolge der gefilterten Richtlinien zu ändern. Die Neuanordnung der Richtlinienliste kann sich auf die Zielverteilung auswirken. Trend Micro Apex Central weist verschiedenen gefilterten Richtlinien unter Umständen erneut bestimmte Ziele zu.

Hinweis

- Bestimmte Richtlinien bleiben statisch und haben immer Vorrang vor gefilterten Richtlinien.
- Diese Funktion steht nur für die Verwaltung von Apex One-Einstellungen zur Verfügung.

Prozedur

1. Navigieren Sie zu **Richtlinien** > **Richtlinienverwaltung**.

   Das Fenster **Richtlinienverwaltung** wird angezeigt.

2. Wählen Sie den Typ der Produkteinstellungen aus der Produktliste aus.

   Das Fenster wird aktualisiert, um die für das ausgewählte verwaltete Produkt erstellten Richtlinien anzuzeigen.

3. Klicken Sie auf **Neu ordnen**.

   Das Fenster **Richtlinien neu anordnen** wird geöffnet.

4. Ändern Sie die Reihenfolge in der Spalte **Priorität**.

5. Klicken Sie auf **Save**.

Hinweis

Warten Sie nach dem Klicken auf **Speichern** zwei Minuten, bis Trend Micro Apex Central die Ziele neu zugewiesen hat. Klicken Sie im Fenster **Richtlinienverwaltung** auf **Aktualisieren**, um die Statusinformationen in der Richtlinienliste zu aktualisieren.

Richtlinienstatus

Mit Hilfe des Richtlinienstatus können Administratoren überprüfen, ob Trend Micro Apex Central eine Richtlinie erfolgreich auf den entsprechenden Zielen bereitgestellt hat.

Verwenden Sie zur Überprüfung des Verteilungsstatus einer Richtlinie eine der folgenden Methoden:

- Klicken Sie im Fenster **Richtlinienverwaltung** auf eine Zahl in der Richtlinienliste. Das Fenster **Protokollabfrage** wird angezeigt.
- Klicken Sie im Dashboard auf eine Zahl im Widget **Richtlinienstatus**. Das Fenster **Protokollabfrage** wird angezeigt.
- Durchführen einer Protokollabfrage

Die folgende Tabelle enthält die Beschreibungen und Vorschläge zu jedem Richtlinienstatus:

Tabelle 2-3. Richtlinienstatus

Richtlinienstatus	Beschreibung	Vorschläge
Ausstehend	Trend Micro Apex Central verarbeitet die Richtlinie.	Warten Sie ein paar Minuten und überprüfen Sie den Status erneut.
Ohne Richtlinie	Trend Micro Apex Central hat diesem Endpunkt oder diesem verwalteten Produkt keine Richtlinie zugewiesen.	Weisen Sie dem Endpunkt oder verwalteten Produkt eine Richtlinie zu.

Richtlinienstatus	Beschreibung	Vorschläge
Verteilt	Trend Micro Apex Central hat die Richtlinie erfolgreich bereitgestellt.	N/A
Endpunkt kann keine Verbindung zum Server herstellen	• Der Endpunkt hat die Richtlinieneinstellungen nicht erhalten. • Der Server ist zur Zeit ausgelastet.	• Überprüfen Sie den Verbindungsstatus des Endpunkts • Verbinden Sie den Endpunkt mit dem Unternehmensnetzwerk • Warten Sie auf den aktualisierten Richtlinienstatus
Ungeeignete Produkteinstellungen	Das verwaltete Produkt kann bestimmte Richtlinieneinstellungen nicht verarbeiten.	• Überprüfen Sie die Richtlinieneinstellungen • Aktualisieren Sie auf die neueste Version der Richtlinienvorlage • Überprüfen Sie die Einstellungen im verwalteten Produkt • Überprüfen Sie die IP-Adresse des verwalteten Produkts im Fenster **Verwaltete Server** Wenn die IP-Adresse ungültig ist, heben Sie die Registrierung des verwalteten Produkts bei Trend Micro Apex Central auf und registrieren Sie das verwaltete Produkt dann erneut. • Informationen zum verwalteten Produkt finden Sie im *Administratorhandbuch*

Richtliniensta tus	Beschreibung	Vorschläge
Nicht unterstützter Endpunkt	Der Endpunkt bietet keine Unterstützung für bestimmte Funktionen, die in den Richtlinieneinstellungen angegeben sind.	Aktualisieren Sie den Agent auf eine unterstützte Version.
Einstellungen wurden lokal geändert	Bestimmte Einstellungen auf dem Endpunkt oder verwalteten Produkt stimmen nicht mit den in der Richtlinie festgelegten Einstellungen überein, da der Administrator des verwalteten Produkts einige Änderungen über die Konsole des verwalteten Produkts vorgenommen hat.	Überprüfen Sie die Einstellungen in der Konsole des verwalteten Produkts.
Nicht aktivierte Lizenzen	Für das verwaltete Produkt sind die Lizenzen für bestimmte in den Richtlinieneinstellungen festgelegte Dienste nicht aktiviert.	Aktivieren Sie die Lizenzen für die zugehörigen Dienste über den **Lizenz-Management**-Bildschirm in der Trend Micro Apex Central-Konsole
Deaktivierte Produktdienste	Für das verwaltete Produkt sind bestimmte, in den Richtlinieneinstellungen festgelegte Dienste nicht aktiviert.	Aktivieren Sie die zugehörigen Dienste für das verwaltete Produkt.
Teilweise verteilt	Trend Micro Apex Central hat einen Teil der Richtlinieneinstellungen durchgesetzt.	Warten Sie ein paar Minuten und überprüfen Sie den Status erneut.
Verwaltet von [Name des Trend Micro Apex Central-Servers]	Ein anderer Trend Micro Apex Central verwaltet derzeit das verwaltete Produkt.	Entfernen Sie das verwaltete Produkt aus der Liste der verwalteten Server und fügen Sie das verwaltete Produkt erneut zur Liste hinzu.
Ungültiger Benutzername oder ungültiges Kennwort	Der Benutzername oder das Kennwort für die Authentifizierung ist ungültig.	Überprüfen Sie den Benutzernamen oder das Kennwort.

Richtliniestatus	Beschreibung	Vorschläge
Ungültige Produktserver- oder Authentifizierungsinformationen	Der Servername oder die Authentifizierungsdaten sind ungültig.	Überprüfen Sie den Servernamen und die Authentifizierungsdaten.
Automatische Anmeldung an Produkt nicht möglich	Trend Micro Apex Central kann die Single Sign-On-Funktion nicht verwenden, um auf das verwaltete Produkt zuzugreifen.	• Überprüfen Sie die Single Sign-On-Funktion im Produktverzeichnis • Überprüfen Sie den Verbindungsstatus des MCP-Agents • Ändern Sie den Serververbindungstyp von **Automatisch** in **Manuell** in der Liste **Verwaltete Server**.
Fehler bei der Konfiguration des Webservers	Im Webdienst ist ein Fehler aufgetreten.	Überprüfen Sie die IIS-Konfiguration.
Produktkommunikationsfehler	Zugriff auf die Produktkonsole nicht möglich.	• Überprüfen Sie, ob Sie auf die Webkonsole des verwalteten Produkts zugreifen können. • Überprüfen Sie die Einstellungen des verwalteten Produkts.
Zum Produkt kann keine Verbindung hergestellt werden	Trend Micro Apex Central kann keine Verbindung zum verwalteten Produkt herstellen.	• Überprüfen Sie den Verbindungsstatus des verwalteten Produkts. • Überprüfen Sie die Netzwerkverbindung
Nicht unterstützte Produktversion	Die Version des verwalteten Produkts wird nicht unterstützt.	Aktualisieren Sie das verwaltete Produkt auf eine unterstützte Version.

Richtlinienstatus	Beschreibung	Vorschläge
Netzwerkkonfigurationsfehler	Ein Netzwerkverbindungsfehler ist aufgetreten.	Überprüfen Sie die Netzwerkverbindung.
Systemfehler. Fehler-ID: [Nummer der Fehler-ID].	Ein Systemfehler ist aufgetreten.	Wenden Sie sich an Ihren Support-Mitarbeiter bei Trend Micro.

Kapitel 3

Richtlinienressourcen

Dieser Abschnitt enthält Informationen zu Richtlinienressourcen für integrierte Produkte/Dienstleistungen.

Wichtig

Jedes verwaltete Produkt bietet unterschiedliche Richtlinieneinstellungen, die Sie konfigurieren und auf Richtlinienziele anwenden können. Eine vollständige Liste der unterstützten verwalteten Produkte und der jeweiligen Richtlinieneinstellungen finden Sie im *Apex Central Widget- und Richtlinienverwaltungsleitfaden*.

Sie können eine PDF-Version des Handbuchs herunterladen oder das Handbuch online mithilfe des folgenden Links anzeigen:

https://docs.trendmicro.com/de-de/enterprise/apex-central.aspx

Es werden folgende Themen behandelt:

- *Application Control-Kriterien auf Seite 3-2*
- *Prävention vor Datenverlust auf Seite 3-16*
- *Regeln zum Eindringschutz auf Seite 3-38*
- *Zulässige Geräte – Gerätesteuerung auf Seite 3-42*

Application Control-Kriterien

Konfigurieren Sie die Application Control-Kriterien, die Sie dann den Security Agent-Richtlinienregeln zuweisen können. Sie können „Zulassen“ und „Sperren“-Kriterien erstellen, um die Anwendungen zu begrenzen, die Benutzer auf geschützten Endpunkten ausführen oder installieren können. Sie können auch Bewertungskriterien erstellen, um die auf Endpunkten ausgeführten Anwendungen zu überwachen und die Kriterien basierend auf den Nutzungsergebnissen zu verfeinern.

Wichtig

Sie müssen die Application Control-Kriterien konfigurieren, bevor Sie eine Application Control-Richtlinie auf Security Agents bereitstellen.

Jedes verwaltete Produkt bietet unterschiedliche Richtlinieneinstellungen, die Sie konfigurieren und auf Richtlinienziele anwenden können. Eine vollständige Liste der unterstützten verwalteten Produkte und der jeweiligen Richtlinieneinstellungen finden Sie im *Apex Central Widget- und Richtlinienverwaltungsleitfaden*.

Sie können eine PDF-Version des Handbuchs herunterladen oder das Handbuch online mithilfe des folgenden Links anzeigen:

https://docs.trendmicro.com/de-de/enterprise/apex-central.aspx

In der folgenden Tabelle sind die Aufgaben aufgeführt, die im Fenster **Application Control-Kriterien** verfügbar sind.

Aufgabe	Beschreibung
Kriterien hinzufügen	Klicken Sie auf die Dropdown-Schaltfläche **Kriterien hinzufügen** und wählen Sie folgende Optionen aus: • **Zulassen**: Klicken, um die Kriterien „Zulassen“ oder „Lockdown“ festzulegen Weitere Informationen finden Sie unter *Definieren von Kriterien für erlaubte Anwendungen auf Seite 3-4*. • **Sperren**: Klicken, um die Kriterien „Sperren“ oder „Bewertung“ festzulegen Weitere Informationen finden Sie unter *Kriterien für gesperrte Anwendungen definieren auf Seite 3-7*. • **Kopieren**: Wählen Sie ein bestehendes Kriterium aus und klicken Sie auf **Kopieren**, um neue Kriterien basierend auf den vorhandenen Einstellungen zu definieren • **Importieren**: Klicken Sie, um ein ZIP-Paket auszuwählen, das aus einer kompatiblen Application Control-Quelle exportiert wurde **Hinweis** Wenn das importierte Paket Kriteriennamen enthält, die mit bereits vorhandenen Kriterien übereinstimmen, haben Sie die Möglichkeit, die vorhandenen Kriterien zu **Überschreiben** oder den Import der Kriterien mit doppelten Namen zu **Überspringen**.
Exportkriterien	Aktivieren Sie das Kontrollkästchen links neben den vorhandenen Kriterien und klicken Sie auf **Exportieren**, um die ausgewählten Kriterien in einem ZIP-Paket (`<timestamp>_iACRuleExport.zip`) zu speichern

Aufgabe	Beschreibung
Löschkriterien	Aktivieren Sie das Kontrollkästchen links neben den vorhandenen Kriterien und klicken Sie auf **Löschen**, um die ausgewählten Kriterien aus der Liste zu entfernen **Warnung!** Wenn Sie Kriterien ausgewählt haben, die von bestehenden Apex One Security Agent-Richtlinien verwendet werden, müssen Sie bestätigen, dass Sie die Kriterien aus allen betroffenen Security Agent-Richtlinien löschen und entfernen möchten. Diese Aktion kann nicht rückgängig gemacht werden.
Kriterien ändern	Klicken Sie auf ein **Kriterienname**, um die Kriterieneinstellungen zu ändern **Hinweis** Betroffene Endpunkte erhalten geänderte Kriterieneinstellungen, sobald die Security Agents das nächste Mal eine Verbindung zum Server herstellen.
Richtlinienzuordnungen anzeigen	Klicken Sie auf den Wert in der **Zielrichtlinien**-Spalte, um eine Liste aller Apex One Security Agent-Richtlinien anzuzeigen, die die Kriterien umsetzen. **Tipp** Klicken Sie auf einen Richtliniennamen, um einen neuen Browser-Tab zu öffnen, in dem Sie die Richtlinieneinstellungen anzeigen oder ändern können.

Definieren von Kriterien für erlaubte Anwendungen

Application Control bietet die Möglichkeit, Kriterien zu definieren, die die Ausführung bestimmter Anwendungen speziell zulassen. Sie können Zulassungskriterien definieren, um sicherzustellen, dass Application Control

niemals eine bestimmte Anwendung blockiert, oder Sie können eine vollständige Liste von Anwendungen erstellen, die auf Endpunkten ausgeführt werden dürfen, und dann eine **Lockdown**-Richtlinie für die Endpunkte bereitstellen. Im **Lockdown**-Modus können Benutzer nur Anwendungen ausführen, darauf zugreifen oder installieren, die Sie in die Zulassungskriterien aufgenommen haben.

Weitere Informationen zu Lockdown-Richtlinien finden Sie unter *Application Control-Richtlinieneinstellungen*.

Prozedur

1. Navigieren Sie zu **Richtlinien** > **Richtlinienressourcen** > **Application Control-Kriterien**.

   Das Fenster **Application Control-Kriterien** wird angezeigt.

2. Klicken Sie auf **Kriterien hinzufügen** und wählen Sie dann **Zulassen** aus.

   Das Fenster **Einstellungen für Zulassungskriterien** wird angezeigt.

3. Geben Sie einen eindeutigen **Name** für die Kriterien ein.

4. Wählen Sie die Stufe von **Vertrauensberechtigung** für die Anwendungen aus.

Berechtigung	Beschreibung	Beispielverwendung
Anwendung kann keine externen Prozesse ausführen	Anwendungen können nicht auf externe Prozesse zugreifen oder andere Anwendungen starten	Verwenden Sie dies, wenn Sie eigenständige Anwendungen auf Endpunkten ausführen möchten, aber den Zugriff auf andere Prozesse verhindern möchten Zum Beispiel ermöglicht diese Einstellung, dass Microsoft Word ausgeführt wird, verhindert jedoch die Ausführung eingebetteter OLE-Objekte.

Berechtigung	Beschreibung	Beispielverwendung
Anwendung kann andere Prozesse ausführen	Anwendungen können externe Prozesse und Anwendungen starten, auf die Benutzer nicht direkt zugreifen können	Verwenden Sie dies, wenn Sie Anwendungen auf Endpunkten ausführen möchten und dennoch den Zugriff auf erforderliche untergeordnete Prozesse oder Add-ons zulassen möchten. Zum Beispiel ermöglicht diese Einstellung, dass Internet Explorer ausgeführt wird und auch, dass Internet Explorer alle installierten Plug-ins ausführt.
Vererbbare Ausführungsrechte (nicht empfohlen)	Anwendungen können externe Prozesse und Anwendungen installieren und starten, und die untergeordneten Anwendungen können ebenfalls externe Prozesse und Anwendungen installieren und starten	Verwenden Sie dies, wenn Sie Installationspaketen erlauben möchten, auf dem Endpunkt ausgeführt zu werden **Vererbbare Ausführungsrechte (nicht empfohlen)** ermöglicht es dem Installationspaket, alle Installationsaufgaben auszuführen, und erlaubt der installierten Anwendung, alle erforderlichen Prozesse auszuführen.

5. Wählen Sie das **Übereinstimmungsmethode** zur Identifizierung von Anwendungen aus und konfigurieren Sie die erforderlichen Einstellungen.

Methode	Beschreibung
Anwendungsverbreitungsliste	Ermöglicht es Ihnen, die Kriterien auf Anwendungen anzuwenden, die von Trend Micro getestet und mit einer Sicherheitsbewertung versehen wurden Weitere Informationen finden Sie unter *Anwendungsverbreitungsliste auf Seite 3-9*.

Methode	Beschreibung
Dateipfade	Lässt zu, dass Sie die Kriterien auf jede Anwendung anwenden, die am angegebenen Speicherort installiert ist Weitere Informationen finden Sie unter *Dateipfade auf Seite 3-10*.
Zertifikate	Ermöglicht es Ihnen, die Kriterien auf Anwendungen basierend auf der Gültigkeit des Zertifikats und den Zertifikatsattributen anzuwenden Weitere Informationen finden Sie unter *Zertifikate auf Seite 3-14*.
Hash-Werte	Lässt zu, dass Sie die Kriterien auf Anwendungen anwenden, die auf SHA-1- oder SHA-256-Hash-Werten basieren Weitere Informationen finden Sie unter *Hash-Werte auf Seite 3-15*.
Gray Software-Liste	Ermöglicht es Ihnen, Anwendungen in die Kriterien aufzunehmen, die Trend Micro getestet und als potenziell schädlich befunden hat Die Gray Software-Liste ist eine Untermenge der Anwendungsreputationsliste und enthält Anwendungen, die bösartig sein können, wenn sie nicht ordnungsgemäß verwendet werden. Trend Micro empfiehlt, Anwendungen in der Gray Software-Liste zu blockieren oder zu überwachen, um die Sicherheit Ihres Netzwerks zu gewährleisten.

6. Klicken Sie auf **Save**.

Kriterien für gesperrte Anwendungen definieren

Application Control bietet die Möglichkeit, Kriterien festzulegen, die bestimmte Anwendungen gezielt am Ausführen hindern. Sie können Sperrkriterien definieren, um sicherzustellen, dass Application Control bestimmte Anwendungen immer sperrt, oder Sie können „Bewertung“-Kriterien erstellen, um die Anwendungen zu überwachen, auf die Benutzer zugreifen.

Prozedur

1. Navigieren Sie zu **Richtlinien** > **Richtlinienressourcen** > **Application Control-Kriterien**.

   Das Fenster **Application Control-Kriterien** wird angezeigt.

2. Klicken Sie auf **Kriterien hinzufügen** und wählen Sie dann **Sperren** aus.

   Das Fenster **Einstellungen für Sperrkriterien** wird angezeigt.

3. Geben Sie einen eindeutigen **Name** für die Kriterien ein.

4. Um eine Überwachungsregel zu erstellen, wählen Sie **Bewertungsmodus aktivieren**.

Hinweis

Application Control – Protokolle protokolliert alle Anwendungen, die den Bewertungskriterien entsprechen, ergreift jedoch keine weiteren Maßnahmen. Application Control ermöglicht es den Anwendungen, normal ausgeführt zu werden.

5. Wählen Sie das **Übereinstimmungsmethode** zur Identifizierung von Anwendungen aus und konfigurieren Sie die erforderlichen Einstellungen.

Methode	Beschreibung
Anwendungsverbreitungsliste	Ermöglicht es Ihnen, die Kriterien auf Anwendungen anzuwenden, die von Trend Micro getestet und mit einer Sicherheitsbewertung versehen wurden Weitere Informationen finden Sie unter *Anwendungsverbreitungsliste auf Seite 3-9*.
Dateipfade	Lässt zu, dass Sie die Kriterien auf jede Anwendung anwenden, die am angegebenen Speicherort installiert ist Weitere Informationen finden Sie unter *Dateipfade auf Seite 3-10*.
Zertifikate	Ermöglicht es Ihnen, die Kriterien auf Anwendungen basierend auf der Gültigkeit des Zertifikats und den Zertifikatsattributen anzuwenden Weitere Informationen finden Sie unter *Zertifikate auf Seite 3-14*.
Hash-Werte	Lässt zu, dass Sie die Kriterien auf Anwendungen anwenden, die auf SHA-1- oder SHA-256-Hash-Werten basieren Weitere Informationen finden Sie unter *Hash-Werte auf Seite 3-15*.

Methode	Beschreibung
Gray Software-Liste	Ermöglicht es Ihnen, Anwendungen in die Kriterien aufzunehmen, die Trend Micro getestet und als potenziell schädlich befunden hat Die Gray Software-Liste ist eine Untermenge der Anwendungsreputationsliste und enthält Anwendungen, die bösartig sein können, wenn sie nicht ordnungsgemäß verwendet werden. Trend Micro empfiehlt, Anwendungen in der Gray Software-Liste zu blockieren oder zu überwachen, um die Sicherheit Ihres Netzwerks zu gewährleisten.

6. Klicken Sie auf **Save**.

Anwendung Übereinstimmungsmethoden

Application Control bietet mehrere Methoden zur Identifizierung von Anwendungen, die in die Zulassungs- und Sperrkriterien aufgenommen werden sollen.

Hinweis

Application Control stellt auch die Gray Software-Liste bereit, die Sie nicht ändern können.

Die Gray Software-Liste ist eine Untermenge der Anwendungsreputationsliste und enthält Anwendungen, die bösartig sein können, wenn sie nicht ordnungsgemäß verwendet werden. Trend Micro empfiehlt, Anwendungen in der Gray Software-Liste zu blockieren oder zu überwachen, um die Sicherheit Ihres Netzwerks zu gewährleisten.

Anwendungsverbreitungsliste

Die Anwendungsreputationsliste ist eine umfassende Liste von Anwendungen, die von Trend Micro getestet wurden. Die Liste umfasst die beliebtesten Betriebssystemdateien und -binärdateien sowie Anwendungen für Desktops, Server und Mobilgeräte. Trend Micro stellt regelmäßig Aktualisierungen der Liste bereit.

Wichtig

Stellen Sie sicher, dass Sie regelmäßige Updates für das Pattern für Certified Safe Software aktiviert haben, um stets die neuesten Anwendungsinformationen zu erhalten.

Sie können nach Anwendungen suchen, indem Sie den Namen von **Anbieter** oder **Anwendungen** eingeben. Wählen Sie Anwendungen anhand der bereitgestellten Daten aus.

Daten	Beschreibung
Anwendung	Der Name der Anwendung **Tipp** Um detaillierte Informationen zu jeder Anwendungsversion anzuzeigen, erweitern Sie die Anwendungs-Reputations-Liste.
KI-Score	Ein umfassender Sicherheitswert basierend auf der Beliebtheit und dem Ruf einer Anwendung
Globale Nutzung	Die weltweite Verbreitung der Anwendung **Tipp** Klicken Sie auf die Prävalenz, um eine regionale Aufschlüsselung der Anwendungsnutzung anzuzeigen.

Dateipfade

Sie können Application Control so konfigurieren, dass bestimmte Verzeichnispfade gezielt anhand des absoluten Pfads, des Speichertyps und Perl-kompatibler regulärer Ausdrücke (PCRE) angesprochen werden.

Wählen Sie, ob nach einem bestimmten Pfad oder einem Speichertyp abgeglichen werden soll, und geben Sie den Typ der Übereinstimmungszeichenfolge an (**Zeichenfolge** oder **Regulärer Ausdruck (PCRE)**). Geben Sie die Dateipfade ein, die auf die Kriterien zutreffen.

Hinweis

- Application Control unterstützt die Verwendung des Sternchens (*) als Platzhalter, wenn ein **Zeichenfolge**-Typ-Match angegeben wird. Das Sternchen kann ein oder mehrere Zeichen in einem Unterverzeichnis des angegebenen Zeichenfolgenstandorts darstellen.
- Application Control unterstützt nicht die Verwendung von Umgebungsvariablen beim Angeben von Dateipfaden für **Zeichenfolge** oder **Regulärer Ausdruck (PCRE)**-Typ-Übereinstimmungen.
- Sie können keine Platzhalterzeichen verwenden, um den gesamten Inhalt des ausgewählten Speicherorts anzuzeigen.
- Sie können bis zu 100 Dateipfade angeben.

TABELLE 3-1. Unterstützte Speicherorte

SPEICHERORT	UMGEBUNGSVARIABLE	BESCHREIBUNG
Spezifischer Pfad	Nicht zutreffend	Gilt nur für Anwendungen im genau angegebenen Pfad **Hinweis** Application Control überprüft den Gerätetyp nicht, wenn dieser Standorttyp verwendet wird.
Jeder integrierte Speicher	$FixedDrives	Gilt nur für Anwendungen im angegebenen Pfad, die auf einem internen Speichergerät (interne Festplatte) gespeichert sind
Jeder lokale Speicher	$LocalDrives	Gilt nur für Anwendungen im angegebenen Pfad, die auf einem nicht entfernbaren lokalen Speichergerät (interne oder externe Festplatte) gespeichert sind
Beliebiger Wechselspeicher	$Removable Drives	Gilt nur für Anwendungen im angegebenen Pfad, die auf einem Wechsellaufwerk (USB-Laufwerk, CD/DVD) gespeichert sind

Speicherort	Umgebungsvariable	Beschreibung
Netzwerkpfad	$RemoteDrives	Gilt nur für Anwendungen im angegebenen Pfad, die auf einer gemeinsamen Netzwerkressource gespeichert sind
Programme-Ordner	$ProgramFiles	Gilt nur für Anwendungen im angegebenen Pfad, die in den Programmdateien-Ordnern gespeichert sind (Standardordner `C:\Program Files` und `C:\Program Files (x86)`)
Systemlautstärke	$SystemDrive	Gilt nur für Anwendungen im angegebenen Pfad, die auf dem standardmäßigen Windows-Systemlaufwerk gespeichert sind

Beispielverwendung des Dateipfads

Ziel	Zulassungsregel	Sperrregel	Ergebnisse
Überwachen Sie den `Downloads`-Ordner aller Benutzer	-	1. **Bewertungsmodus aktivieren** 2. **Jeder lokale Speicher** 3. **Zeichenfolge** 4. `C:\Users\*\Downloads\*`	Protokolliert alle Zugriffsversuche auf Anwendungen im `Downloads`-Ordner aller Benutzer. Monitore: • `C:\Users\john_doe\Downloads\start.exe` • `C:\Users\Administrator\Downloads\start.exe`

Ziel	Zulassungsregel	Sperrregel	Ergebnisse
Sperren Sie alle Anwendungen, die sich in einem beliebigen Ordner unter dem `MyApps`-Unterordner des `Program Files`-Verzeichnisses befinden	-	1. **Programmdateien-Ordner** 2. **Zeichenfolge** 3. `\MyApps*`	Sperren: • `C:\Program Files(x86)\MyApps\start.exe` • `C:\Program Files\MyApps\start.exe` • `C:\Program Files(x86)\MyApps\bin\start.exe` Erlaubt: • `C:\Program Files(x86)\start.exe`
Erlaube alle Anwendungen, die sich in einem beliebigen Ordner unter dem `MyApps`-Unterordner des `Program Files`-Verzeichnisses befinden, aber sperre alle anderen Anwendungen/ Ordner	1. **Programmdateien-Ordner** 2. **Zeichenfolge** 3. `\MyApps*`	1. **Jeder lokale Speicher** 2. **Zeichenfolge** 3. `C:\Program Files\*` AND 1. **Jeder lokale Speicher** 2. **Zeichenfolge** 3. `C:\Program Files (x86)\*`	Sperren: • `C:\Program Files(x86)\start.exe` Erlaubt: • `C:\Program Files(x86)\MyApps\start.exe` • `C:\Program Files\MyApps\start.exe` • `C:\Program Files(x86)\MyApps\bin\start.exe`

Ziel	Zulassungsregel	Sperrregel	Ergebnisse
Nur Anwendungen im Unterordner `MyApps` des Verzeichnisses `Program Files` sperren, aber alle anderen Anwendungen/ Ordner zulassen	1. Erlaube die Unterordner des Verzeichnisses `MyApps` a. **Programmdateien-Ordner** b. **Zeichenfolge** c. `\MyApps\*\*`	1. **Programmdateien-Ordner** 2. **Zeichenfolge** 3. `\MyApps\*`	Sperren: • `C:\Program Files(x86)\MyApps\start.exe` • `C:\Program Files\MyApps\start.exe` Erlaubt: • `C:\Program Files(x86)\start.exe` • `C:\Program Files(x86)\MyApps\bin\start.exe`
Sperren Sie einen bestimmten Anwendungsdateinamen in jedem Ordner	-	1. **Spezifischer Pfad** 2. **Regulärer Ausdruck (PCRE)** 3. `.*\\(?i)test(?-i)\..*`	Sperren: • `C:\MyApps\test.exe` • `C:\Users\guet\AppData\Local\Temp\test.exe` • `C:\Program Files(x86)\MyApps\test.exe`

Zertifikate

Sie können Application Control so konfigurieren, dass es speziell auf Anwendungen abzielt, basierend auf dem „Vertrauen“-Niveau eines Zertifikats und die bestimmte Zertifikatsattribute enthalten.

Wählen Sie den Typ des Zertifikats „Vertrauen“ aus und geben Sie dann die erforderlichen Zertifikatsinformationen „Aussteller“ oder „Betreff“ an.

Hinweis

Application Control unterstützt die Verwendung des Sternchens (*) als Platzhalter bei der Angabe von Zertifikat-Attributen, obwohl Sie den Platzhalter in Verbindung mit anderen Zeichen verwenden müssen, um den Umfang einzuschränken. Zum Beispiel können Sie das Platzhalterzeichen nicht allein in einem Feld verwenden.

Die verschiedenen „Vertrauen“-Typen werden in der folgenden Tabelle beschrieben.

Typ	Beschreibung
Vertrauenswürdig (gültig)	Sie müssen das Zertifikat in die Liste der vertrauenswürdigen Zertifikate aufgenommen haben und das Zertifikat darf nicht abgelaufen sein
Vertraut (abgelaufen)	Sie müssen das Zertifikat zur Liste der vertrauenswürdigen Zertifikate hinzugefügt haben, aber das Zertifikat ist bereits abgelaufen
Nicht vertrauenswürdig	Das Zertifikat ist unbekannt oder Sie haben das Zertifikat nicht zur Liste der vertrauenswürdigen Zertifikate hinzugefügt

Hinweis

Die „Vertrauen“-Kombinationen für Zulassen- und Sperren-Kriterien unterscheiden sich.

Hash-Werte

Sie können Application Control so konfigurieren, dass Anwendungen mithilfe von SHA-1- oder SHA-256-Hashwertformaten abgeglichen werden. Sie können wählen, ob Sie Hashwerte manuell angeben oder eine Liste generierter Werte importieren möchten.

Wählen Sie Ihr **Eingabemethode** und folgen Sie den auf dem Bildschirm angezeigten Anweisungen.

Eingabemethode	Beschreibung
Manuell	Ermöglicht es Ihnen, bis zu 100 Hash-Werte (und Beschreibungen) manuell anzugeben
Importieren	Ermöglicht das Importieren eines ZIP-Pakets, das eine korrekt formatierte Hash-Wert-Liste im CSV-Format enthält Sie können wählen, ob Sie das **Hash-Generator-Tool** verwenden oder die CSV-Datei manuell mit dem **CSV-Beispielformat** erstellen. **Warnung!** Sie können nur eine Datei in jeden Kriterienkatalog importieren. Wenn Sie versuchen, eine neue Hash-Wert-Liste in die Kriterien zu importieren, überschreibt Application Control die vorhandenen Werte vollständig. • **Hash-Generator-Tool**: Laden Sie das Tool herunter und führen Sie es auf einem Zielendpunkt aus, auf dem Sie alle notwendigen Anwendungen installiert haben. Das Tool erstellt automatisch ein gültiges ZIP-Paket, das die Hash-Werte aller auf dem Endpunkt gefundenen Anwendungen enthält. • **CSV-Beispielformat**: Laden Sie die Beispieldatei herunter und folgen Sie den Anweisungen, um die Hash-Wert-Liste korrekt auszufüllen. Sobald Sie die Liste vervollständigt haben, komprimieren Sie die Datei im ZIP-Format, bevor Sie sie in das Kriterien-Set importieren. **Wichtig** Die Hashwertliste darf keine Mischung aus SHA-1- und SHA-256-Formaten enthalten. Sie müssen separate Hashwertdateien und separate Application Control-Kriterien für jeden Hashwertformattyp erstellen.

Prävention vor Datenverlust

'Prävention vor Datenverlust' (Data Loss Prevention, DLP) schützt die als digitale Assets bezeichneten vertraulichen und sensiblen Daten

eines Unternehmens vor versehentlicher Offenlegung und vorsätzlichem Diebstahl. Mit DLP können Sie:

- Die zu schützenden digitalen Assets erkennen
- Richtlinien erstellen, die die Übertragung von digitalen Assets über gemeinsam genutzte Kanäle wie E-Mail und externe Geräte einschränken oder verhindern
- Die Einhaltung bewährter Datenschutzstandards durchsetzen

DLP wertet Daten anhand einer Reihe von Regeln aus, die in Richtlinien definiert sind. Richtlinien legen die Daten fest, die vor einer unbefugten Übertragung geschützt werden müssen, und bestimmen die Aktion, die DLP durchführt, wenn eine Übertragung erkannt wird.

Wichtig

Jedes verwaltete Produkt bietet unterschiedliche Richtlinieneinstellungen, die Sie konfigurieren und auf Richtlinienziele anwenden können. Eine vollständige Liste der unterstützten verwalteten Produkte und der jeweiligen Richtlinieneinstellungen finden Sie im *Apex Central Widget- und Richtlinienverwaltungsleitfaden*.

Sie können eine PDF-Version des Handbuchs herunterladen oder das Handbuch online mithilfe des folgenden Links anzeigen:

https://docs.trendmicro.com/de-de/enterprise/apex-central.aspx

Datenbezeichnertypen

Digitale Assets sind Dateien und Daten, die ein Unternehmen vor unbefugter übertragung schützen muss. Administratoren können digitale Assets mit den folgenden Datenbezeichnern definieren:

- **Ausdrücke**: Daten, die eine bestimmte Struktur haben.

  Weitere Informationen finden Sie unter *Ausdrücke auf Seite 3-18*.

- **File attributes**: Dateieigenschaften wie Dateityp und Dateigröße.

  Weitere Informationen finden Sie unter *Dateiattribute auf Seite 3-23*.

- **Keyword lists**: Eine Liste von speziellen Wörtern oder Ausdrücken.

  Weitere Informationen finden Sie unter *Schlüsselwörter auf Seite 3-26*.

Hinweis

Administratoren können einen Datenbezeichner nicht löschen, der in einer DLP-Vorlage verwendet wird. Löschen Sie die Vorlage, bevor Sie den Datenbezeichner löschen.

Ausdrücke

Ein Ausdruck ist Daten mit einer bestimmten Struktur. Zum Beispiel bestehen Kreditkartennummern normalerweise aus 16 Ziffern im Format "nnnn-nnnn-nnnn-nnnn", weshalb sie sich für die ausdrucksbasierte Erkennung gut eignen.

Administratoren können vordefinierte und benutzerdefinierte Ausdrücke verwenden.

Weitere Informationen finden Sie unter *Vordefinierte Ausdrücke auf Seite 3-18* und *Benutzerdefinierte Ausdrücke auf Seite 3-19*.

Vordefinierte Ausdrücke

Im Lieferumfang der Prävention vor Datenverlust ist eine Reihe vordefinierter Ausdrücke enthalten. Diese Ausdrücke können weder geändert noch gelöscht werden.

Die Prävention vor Datenverlust überprüft diese Ausdrücke und verwendet hierfür den Pattern-Abgleich und mathematische Gleichungen. Nachdem die Prävention vor Datenverlust möglicherweise sensible Daten mit einem Ausdruck abgeglichen hat, werden für die Daten unter Umständen zusätzliche Überprüfungen durchgeführt.

Eine vollständige Liste aller vordefinierten Ausdrücke finden Sie in der *Datenschutzliste* unter:

https://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Einstellungen für vordefinierte Ausdrücke anzeigen

Hinweis

Vordefinierte Ausdrücke können weder geändert noch gelöscht werden.

Prozedur

1. Navigieren Sie zu **Richtlinien** > **Richtlinienressourcen** > **DLP-Datenbezeichner**.
2. Klicken Sie auf die Registerkarte **Ausdruck**.
3. Klicken Sie auf den Namen des Ausdrucks.
4. Es öffnet sich ein Fenster mit den Einstellungen.

Benutzerdefinierte Ausdrücke

Erstellen Sie benutzerdefinierte Ausdrücke, wenn keiner der vordefinierten Ausdrücke die Anforderungen des Unternehmens erfüllt.

Ausdrücke sind ein mächtiges Werkzeug zum Abgleichen von Zeichenketten. Machen Sie sich mit der Syntax von Ausdrücken vertraut, bevor Sie selbst Ausdrücke erstellen. Fehlerhaft formulierte Ausdrücke können die Leistung stark beeinträchtigen.

Hinweise zum Erstellen von Ausdrücken:

- Orientieren Sie sich zum Erstellen gültiger Ausdrücke an den vordefinierten Ausdrücken. Wenn Sie zum Beispiel einen Ausdruck erstellen, in dem ein Datum enthalten ist, können Sie sich auf die Ausdrücke mit dem Präfix "Datum" beziehen.
- Beachten Sie, dass die Prävention vor Datenverlust die in der PCRE-Bibliothek (Perl-kompatible reguläre Ausdrücke) definierten Ausdrucksformate verwendet. Weitere Informationen zu PCRE finden Sie auf der folgenden Website:

  http://www.pcre.org/

- Beginnen Sie mit einfachen Ausdrücken. Verändern Sie die Ausdrücke, wenn sie Fehlarme verursachen, oder machen Sie eine Feinabstimmung, um die Erkennungsrate zu verbessern.

Administratoren stehen beim Erstellen von Ausdrücken eine Reihe von Kriterien zur Verfügung. Ein Ausdruck muss die gewählten Kriterien erfüllen, damit die Prävention vor Datenverlust ihn für eine DLP-Richtlinie akzeptiert. Weitere Informationen zu den einzelnen Kriterienoptionen finden Sie unter *Kriterien für benutzerdefinierten Ausdruck auf Seite 3-20*.

Kriterien für benutzerdefinierten Ausdruck

Sehen Sie sich die verfügbaren Optionen zum Erstellen benutzerdefinierter Ausdrücke an.

TABELLE 3-2. Kriterienoptionen für benutzerdefinierte Ausdrücke

KRITERIEN	REGEL	BEISPIEL
Keiner	Keiner	Alle - Namen gemäß den Angaben des Statistischen Bundesamtes der Vereinigten Staaten • Ausdruck:[^\w]([A-Z][a-z]{1,12}(\s?,\s?|[\s]|\s([A-Z])\.\s)[A-Z][a-z]{1,12})[^\w]
Bestimmte Zeichen	In einem Ausdruck müssen die von Ihnen vorgegebenen Zeichen enthalten sein. Außerdem muss die Zeichenanzahl in einem Ausdruck innerhalb der vorgegebenen Mindest- und Höchstgrenzen liegen.	US - ABA-Routing-Nummer • Ausdruck:[^\d]([0123678]\d{8})[^\d] • Zeichen: 0123456789 • Mindestanzahl von Zeichen: 9 • Höchstanzahl von Zeichen: 9

Kriterien	Regel	Beispiel
Erweiterung	Als Suffix wird das letzte Segment in einem Ausdruck bezeichnet. In einem Suffix müssen die Zeichen enthalten sein, die Sie angegeben haben, und es muss aus einer bestimmten Anzahl von Zeichen bestehen. Außerdem muss die Zeichenanzahl in einem Ausdruck innerhalb der vorgegebenen Mindest- und Höchstgrenzen liegen.	Alle - Privatadresse • Ausdruck:\D(\d+\s[a-z.]+\s([a-z]+\s){0,2} (lane|ln|street|st|avenue|ave|road|rd|place|pl|drive|dr|circle| cr|court|ct|boulevard|blvd)\.? [0-9a-z,#\s\.]{0,30}[\s|,][a-z]{2}\ s\d{5}(-\d{4})?)[^\d-] • Suffix-Zeichen: 0123456789- • Anzahl von Zeichen: 5 • Mindestzeichenanzahl im Ausdruck: 25 • Höchstzeichenanzahl im Ausdruck: 80
Trennzeichen aus einem Zeichen	Ein Ausdruck muss aus zwei Segmenten bestehen, die mit einem Zeichen getrennt sind. Das Zeichen muss eine Länge von 1 Byte haben. Außerdem muss die Zeichenanzahl links vom Trennzeichen innerhalb der vorgegebenen Mindest- und Höchstgrenzen liegen. Die Zeichenanzahl rechts vom Trennzeichen darf die Höchstgrenze nicht überschreiten.	Alle - E-Mail-Adresse • Ausdruck:[^\w.]([\w\.]{1,20}@[a-z0-9]{2,20}[\.][a-z]{2,5}[a-z\.]{0,10})[^\w.] • Trennzeichen: @ • Mindestzeichenanzahl links: 3 • Höchstzeichenanzahl links: 15 • Höchstzeichenanzahl rechts: 30

Benutzerdefinierte Ausdrücke erstellen

Prozedur

1. Navigieren Sie zu **Richtlinien** > **Richtlinienressourcen** > **DLP-Datenbezeichner**.
2. Klicken Sie auf die Registerkarte **Ausdruck**.

3. Klicken Sie auf **Hinzufügen**.

   Ein neues Fenster wird geöffnet.

4. Geben Sie einen Namen für den Ausdruck ein. Der Name darf nicht länger als 100 Byte sein und folgende Zeichen dürfen nicht enthalten sein:

   - > < * ^ | & ? \ /

5. Geben Sie eine Beschreibung mit maximal 256 Byte ein.

6. Geben Sie die Daten ein, die angezeigt werden sollen.

   Wenn Sie zum Beispiel einen Ausdruck für Seriennummern erstellen, geben Sie das Muster einer Seriennummer ein. Die Daten sind nur zur Dokumentation, sie erscheinen an keiner anderen Stelle im Produkt.

7. Wählen Sie eine der folgenden Kriterien, und konfigurieren Sie zusätzliche Einstellungen für die ausgewählten Kriterien (siehe *Kriterien für benutzerdefinierten Ausdruck auf Seite 3-20*):

   - Keiner
   - Bestimmte Zeichen
   - Erweiterung
   - Trennzeichen aus einem Zeichen

8. Testen Sie den Ausdruck mit tatsächlichen Daten.

   Wenn der Ausdruck zum Beispiel für eine Personalausweisnummer steht, geben Sie eine gültige Ausweisnummer in das Textfeld **Testdaten** ein und klicken auf **Testen**. Überprüfen Sie anschließend das Ergebnis.

9. Klicken Sie auf **Speichern**, wenn Sie mit dem Ergebnis zufrieden sind.

Hinweis

Speichern Sie die Einstellungen nur dann, wenn der Test erfolgreich war. Ein Ausdruck, der keine Daten entdeckt, verschwendet Systemressourcen und kann die Leistung beeinträchtigen.

Benutzerdefinierte Ausdrücke importieren

Verwenden Sie diese Option, wenn Sie über eine ordnungsgemäß formatierte `.dat`-Datei verfügen, in der die Ausdrücke gespeichert sind. Sie können die Datei erzeugen, indem Sie die Ausdrücke entweder über den Server, auf den Sie gerade zugreifen, oder über einen anderen Server exportieren.

Prozedur

1. Navigieren Sie zu **Richtlinien** > **Richtlinienressourcen** > **DLP-Datenbezeichner**.
2. Klicken Sie auf die Registerkarte **Ausdruck**.
3. Klicken Sie auf **Importieren**, und suchen Sie dann die `.dat`-Datei, in der die Ausdrücke enthalten sind.
4. Klicken Sie auf **Öffnen**.

   Sie erhalten eine Nachricht, wenn der Import erfolgreich war. Wenn ein Ausdruck importiert werden soll, der bereits vorhanden ist, wird er übersprungen.

Dateiattribute

Dateiattribute sind bestimmte Eigenschaften einer Datei. Sie können zwei Dateiattribute zur Definition von Datenbezeichnern verwenden: Dateityp und Dateigröße. Nehmen wir an, ein Software-Entwickler möchte, dass sein firmeneigenes Software-Installationsprogramm nur an die R&D-Abteilung weitergegeben wird, deren Mitglieder für die Entwicklung und das Testen der Software zuständig sind. In diesen Fall kann der Trend Micro Apex Central Administrator eine Richtlinie erstellen, mit der die Übertragung ausführbarer Dateien mit einer Größe von 10 bis 40 MB auf alle Abteilungen, mit Ausnahme von R&D, gesperrt wird.

Dateiattribute sind an sich schlechte Indikatoren für sensible Dateien. Wenn wir unser Beispiel von oben weiterführen, werden Software-Installationsprogramme anderer Hersteller höchstwahrscheinlich gesperrt. Trend Micro empfiehlt deshalb die Kombination von Dateiattributen mit

anderen DLP-Datenbezeichnern, um eine gezieltere Erkennung sensibler Dateien zu ermöglichen.

Eine vollständige Liste aller unterstützten Dateitypen finden Sie in der *Datenschutzliste* unter:

https://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Eine Dateiattributliste erstellen

Prozedur

1. Navigieren Sie zu **Richtlinien** > **Richtlinienressourcen** > **DLP-Datenbezeichner**.
2. Klicken Sie auf die Registerkarte **File Attribute**.
3. Klicken Sie auf **Hinzufügen**.

   Ein neues Fenster wird geöffnet.
4. Geben Sie einen Namen für die Dateiattributliste ein. Der Name darf nicht länger als 100 Byte sein und folgende Zeichen dürfen nicht enthalten sein:
   - > < * ^ | & ? \ /
5. Geben Sie eine Beschreibung mit maximal 256 Byte ein.
6. Wählen Sie die gewünschten ursprünglichen Dateitypen aus.
7. Wenn ein Dateityp, den Sie einschließen möchten, nicht in der Liste steht, wählen Sie **File extensions** aus, und geben Sie anschließend die Erweiterung des Dateityps ein. Die Prävention vor Datenverlust überprüft Dateien mit der angegebenen Erweiterung, prüft aber nicht deren tatsächliche Dateitypen. Richtlinien beim Festlegen von Dateierweiterungen:
   - Jede Erweiterung muss mit einem Sternchen (*) beginnen, gefolgt von einem Punkt (.) und dann der Erweiterung. Das Sternchen ist ein Platzhalter, der den tatsächlichen Namen einer Datei darstellt. Zum Beispiel passt `*.pol` zu `12345.pol` und `test.pol`.

- Sie können Platzhalter in Erweiterungen einschließen. Mit einem Fragezeichen (?) können Sie ein einzelnes Zeichen und mit einem Stern (*) zwei oder mehr Zeichen darstellen. Beispiele dafür finden Sie nachstehend:

  - `*.*m` entspricht den folgenden Dateien: `ABC.dem`, `ABC.prm`, `ABC.sdcm`

  - `*.m*r` entspricht den folgenden Dateien: `ABC.mgdr`, `ABC.mtp2r`, `ABC.mdmr`

  - `*.fm?` entspricht den folgenden Dateien: `ABC.fme`, `ABC.fml`, `ABC.fmp`

- Gehen Sie beim Hinzufügen eines Sterns am Ende einer Erweiterung besonders sorgfältig vor, da dieser Platzhalter mit Teilen eines Dateinamens oder einer nicht zugehörigen Erweiterung übereinstimmen kann. Beispiel: `*.do*` stimmt mit `abc.doctor_john.jpg` und `abc.donor12.pdf` überein.

- Verwenden Sie Strichpunkte (;), um mehrere Dateierweiterungen zu trennen. Sie müssen nach einem Strichpunkt kein Leerzeichen einfügen.

8. Geben Sie die minimale und maximale Dateigröße in Byte ein. Beide Dateigrößen müssen ganze Zahlen größer als null sein.

9. Klicken Sie auf **Speichern**.

Eine Dateiattributliste importieren

Verwenden Sie diese Option, wenn Sie eine korrekt formatierte `.dat`-Datei mit den Dateiattributlisten haben. Sie können die Datei generieren, indem Sie die Dateiattributlisten entweder von dem Server, auf den Sie gerade zugreifen, oder von einem anderen Server exportieren.

Prozedur

1. Navigieren Sie zu **Richtlinien** > **Richtlinienressourcen** > **DLP-Datenbezeichner**.

2. Klicken Sie auf die Registerkarte **File Attribute**.
3. Klicken Sie auf **Importieren** und suchen Sie dann die `.dat`-Datei, in der die Dateiattributlisten enthalten sind.
4. Klicken Sie auf **Öffnen**.

   Sie erhalten eine Nachricht, wenn der Import erfolgreich war. Wenn eine Dateiattributliste importiert werden soll, die bereits vorhanden ist, wird sie übersprungen.

Schlüsselwörter

Schlüsselwörter sind besondere Wörter oder Phrasen. Sie können miteinander verwandte Schlüsselwörter in eine Schlüsselwortliste eintragen, um bestimmte Arten von Daten zu identifizieren. Zum Beispiel sind "Prognose", "Blutgruppe", "Impfung" und "Arzt" Schlüsselwörter, die in einem Gesundheitsattest stehen könnten. Wenn Sie die Übertragung von Dateien mit Gesundheitsattesten verhindern wollen, können Sie diese Schlüsselwörter in einer DLP-Richtlinie verwenden und dann die Prävention vor Datenverlust so konfigurieren, dass Dateien mit diesen Schlüsselwörtern gesperrt werden.

Häufig benutzte Wörter können zu bedeutungsvollen Schlüsselwörtern kombiniert werden. Zum Beispiel können die Begriffe "end", "read", "if" and "at" zu Schlüsselwörtern in Quellcodes kombiniert werden, zum Beispiel als "END-IF", "END-READ" und "AT END".

Sie können vordefinierte und benutzerdefinierte Schlüsselwortlisten verwenden. Weitere Informationen finden Sie unter *Vordefinierte Schlüsselwortlisten auf Seite 3-26* und *Benutzerdefinierte Schlüsselwortlisten auf Seite 3-28*.

Vordefinierte Schlüsselwortlisten

Im Lieferumfang der Prävention vor Datenverlust ist eine Reihe vordefinierter Schlüsselwortlisten enthalten. Diese Schlüsselwortlisten können nicht geändert bzw. gelöscht werden. Jede Liste hat ihre eigenen integrierten Bedingungen, die festlegen, ob die Vorlage einen Richtlinienverstoß auslösen soll.

Weitere Informationen zu den vordefinierten Schlüsselwortlisten in der Prävention vor Datenverlust finden Sie im Dokument *Datenschutzlisten* unter:

https://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Wie funktionieren Schlüsselwortlisten

Bedingung "Anzahl der Schlüsselwörter"

Jede Schlüsselwortliste enthält eine Bedingung, mit der eine bestimmte Anzahl an Schlüsselwörtern festgelegt wird, die in einem Dokument enthalten sein muss, bevor die Liste einen Verstoß meldet.

Die Bedingung für die Anzahl der Schlüsselwörter enthält die folgenden Werte:

- **Alle**: Alle Schlüsselwörter in der Liste müssen im Dokument vorhanden sein.
- **Beliebig**: Eines der Schlüsselwörter in der Liste muss im Dokument vorhanden sein.
- **Bestimmte Anzahl**: Es muss mindestens die angegebene Anzahl an Schlüsselwörtern im Dokument enthalten sein. Wenn das Dokument mehr Schlüsselwörter als die angegebene Anzahl enthält, meldet die Prävention vor Datenverlust einen Verstoß.

Abstandsbedingung

Einige der Listen enthalten eine Abstandsbedingung zum Ermitteln eines Verstoßes. "Abstand" bezieht sich auf die Anzahl der Zeichen zwischen dem ersten Zeichen eines Schlüsselworts und dem ersten Zeichen eines anderen Schlüsselworts. Betrachten Sie den folgenden Eintrag:

F**irst Name:_John_ L**ast Name:_Smith_

Die Liste **Formulare - Vorname, Nachname** hat eine Abstandsbedingung von 50 und enthält die häufig verwendeten Formularfelder "Vorname" und "Nachname". Im obigen Beispiel meldet die Prävention vor Datenverlust einen Verstoß, da die Anzahl der Zeichen zwischen dem "F" in "First Name" und dem "L" in "Last Name" 18 beträgt.

Nachfolgend finden Sie ein Beispiel für einen Eintrag, der keinen Verstoß darstellt:

The f**irst name of our new employee from Switzerland is John. His l**ast name is Smith.

In diesem Beispiel beträgt die Anzahl der Zeichen zwischen dem "f" in "first name" und dem "l" in "last name" 72. Dieser Wert überschreitet den Abstandsschwellenwert und stellt keinen Verstoß dar.

Benutzerdefinierte Schlüsselwortlisten

Erstellen Sie benutzerdefinierte Schlüsselwortlisten, wenn keine der vorhandenen Schlüsselwortlisten Ihren Anforderungen entspricht.

Beim Erstellen einer Schlüsselwortliste können Sie aus mehreren Kriterien wählen. Eine Schlüsselwortliste muss die gewählten Kriterien erfüllen, bevor die Prävention vor Datenverlust sie für eine Richtlinie berücksichtigt. Wählen Sie eine der folgenden Kriterien für jede Schlüsselwortliste:

- **Beliebiges Schlüsselwort**
- **Alle Schlüsselwörter**
- **Alle Schlüsselwörter innerhalb von <x> Zeichen**
- **Die Gesamtbewertung für Schlüsselwörter ist größer als Grenzwert**

Details zu den Kriterienregeln finden Sie unter *Kriterien für benutzerdefinierte Schlüsselwortliste auf Seite 3-28*.

Kriterien für benutzerdefinierte Schlüsselwortliste

Kriterien anzeigen, die zur Erstellung benutzerdefinierter Schlüsselwortlisten für die Verwendung in Vorlagen für 'Prävention vor Datenverlust' verwendet werden.

TABELLE 3-3. Kriterien für eine Schlüsselwortliste

KRITERIEN	REGEL
Beliebiges Schlüsselwort	Eine Datei muss mindestens ein Schlüsselwort aus der Schlüsselwörterliste enthalten.

Kriterien	Regel
Alle Schlüsselwörter	Eine Datei muss alle Schlüsselwörter aus der Schlüsselwörterliste enthalten.
Alle Schlüsselwörter innerhalb von <x> Zeichen	Eine Datei muss alle Schlüsselwörter aus der Schlüsselwörterliste enthalten. Jedes Schlüsselwortpaar darf höchstens <x> Zeichen voneinander entfernt sein. Nehmen wir an, Ihre 3 Schlüsselwörter sind WEB, DISK und USB, und die von Ihnen angegebene Anzahl von Zeichen beträgt 20. Wenn die Funktion "Prävention vor Datenverlust" alle Schlüsselwörter in der Reihenfolge DISK, WEB und USB erkennt, darf die Anzahl der Zeichen von "D" (in DISK) bis "W" (in WEB) und von "W" bis "U" (in USB) höchstens 20 betragen. Die folgenden Daten entsprechen den Kriterien:DISK####WEB############USB Die folgenden Daten entsprechen nicht den Kriterien:DISK******************WEB****USB (23 Zeichen zwischen "D" und "W") Denken Sie beim Festlegen der Zeichenanzahl daran, dass sich durch eine kleine Anzahl, wie z. B. 10, die Suchgeschwindigkeit erhöht, aber nur ein relativ kleiner Bereich abgedeckt wird. Dadurch verringert sich die Wahrscheinlichkeit, dass sensible Daten entdeckt werden, vor allem in großen Dateien. Bei Verwendung einer größeren Anzahl an Zeichen wird der abgedeckte Bereich größer, es kann aber sein, dass sich dadurch die Suchzeiten verlängern

Kriterien	Regel
Die Gesamtbewertung für Schlüsselwörter ist größer als Grenzwert	Eine Datei muss ein oder mehrere Schlüsselwörter aus der Schlüsselwortliste enthalten. Wird nur ein Schlüsselwort entdeckt, muss seine Bewertung höher sein als der Grenzwert. Werden mehrere Schlüsselwörter entdeckt, muss die Gesamtbewertung höher sein als der Grenzwert. Weisen Sie jedem Schlüsselwort eine Punktezahl von 1 bis 10 zu. Streng vertrauliche Wörter oder Formulierungen, wie etwa "Gehaltserhöhung" in Zusammenhang mit der Personalabteilung, sollten eine relativ hohe Punktezahl haben. Wörter oder Phrasen, denen an sich keine besondere Bedeutung zukommt, können niedrigere Punktezahlen haben. Berücksichtigen Sie bei der Konfiguration des Grenzwerts die Punktezahl, die Sie den Schlüsselwörtern zugewiesen haben. Wenn Sie zum Beispiel fünf Schlüsselwörter haben und drei dieser Schlüsselwörter haben hohe Priorität, kann der Grenzwert gleich oder niedriger sein als die Gesamtpunktezahl der drei Schlüsselwörter mit hoher Priorität. Das bedeutet, dass die Entdeckung dieser drei Schlüsselwörter ausreicht, um die Datei als sensibel einzustufen.

Schlüsselwortlisten erstellen

Prozedur

1. Navigieren Sie zu **Richtlinien** > **Richtlinienressourcen** > **DLP-Datenbezeichner**.
2. Klicken Sie auf die Registerkarte **Schlüsselwort**.
3. Klicken Sie auf **Hinzufügen**.

   Ein neues Fenster wird geöffnet.
4. Geben Sie einen Namen für die Schlüsselwortliste ein. Der Name darf nicht länger als 100 Byte sein und folgende Zeichen dürfen nicht enthalten sein:

   - > < * ^ | & ? \ /
5. Geben Sie eine Beschreibung mit maximal 256 Byte ein.
6. Wählen Sie eines der folgenden Kriterien und konfigurieren Sie zusätzliche Einstellungen für die ausgewählten Kriterien:

- **Beliebiges Schlüsselwort**
- **Alle Schlüsselwörter**
- **Alle Schlüsselwörter innerhalb von <x> Zeichen**
- **Die Gesamtbewertung für Schlüsselwörter ist größer als der Grenzwert**

7. Schlüsselwörter manuell zur Liste hinzufügen:
   a. Geben Sie ein Schlüsselwort ein, das zwischen 3 und 40 Byte lang ist, und bestimmen Sie, ob zwischen Groß- und Kleinschreibung unterschieden werden soll.
   b. Klicken Sie auf **Hinzufügen**.
8. Schlüsselwörter mit der Option "Importieren" hinzufügen:

Hinweis

Verwenden Sie diese Option, wenn Sie über eine ordnungsgemäß formatierte `.csv`-Datei verfügen, in der die Schlüsselwörter gespeichert sind. Sie können die Datei erzeugen, indem Sie die Schlüsselwörter entweder über den Server, auf den Sie gerade zugreifen, oder über einen anderen Server exportieren.

   a. Klicken Sie auf **Importieren**, und suchen Sie die `.csv`-Datei, die die Schlüsselwörter enthält.
   b. Klicken Sie auf **Öffnen**.

      Sie erhalten eine Nachricht, wenn der Import erfolgreich war. Wenn ein Schlüsselwort importiert werden soll, das bereits vorhanden ist, wird es übersprungen.
9. Wählen Sie zum Löschen von Schlüsselwörtern die Schlüsselwörter aus, und klicken Sie auf **Delete**.
10. Schlüsselwörter exportieren:

Hinweis

Verwenden Sie die "Export"-Funktion, um die Schlüsselwörter zu sichern oder um sie in einen anderen Server zu importieren. Alle Schlüsselwörter in der Schlüsselwortliste werden exportiert. Das Exportieren einzelner Schlüsselwörter ist nicht möglich.

a. Klicken Sie auf **Exportieren**.

b. Speichern Sie die exportierte `.csv`-Datei am gewünschten Speicherort.

11. Klicken Sie auf **Speichern**.

Schlüsselwortlisten importieren

Verwenden Sie diese Option, wenn Sie über eine ordnungsgemäß formatierte `.dat`-Datei verfügen, in der die Schlüsselwortlisten gespeichert sind. Sie können die Datei erzeugen, indem Sie die Schlüsselwortlisten entweder über den Server, auf den Sie gerade zugreifen, oder über einen anderen Server exportieren.

Prozedur

1. Navigieren Sie zu **Richtlinien** > **Richtlinienressourcen** > **DLP-Datenbezeichner**.
2. Klicken Sie auf die Registerkarte **Schlüsselwort**.
3. Klicken Sie auf **Importieren** und suchen Sie dann die `.dat`-Datei, die die Schlüsselwortlisten enthält.
4. Klicken Sie auf **Öffnen**.

   Sie erhalten eine Nachricht, wenn der Import erfolgreich war. Wenn eine Schlüsselwortliste importiert werden soll, die bereits vorhanden ist, wird sie übersprungen.

Vorlagen für 'Prävention vor Datenverlust'

Eine DLP-Vorlage verbindet DLP-Datenbezeichner mit logischen Operatoren (Und, Oder, Außer) zur Erstellung von Bedingungsanweisungen. Nur Dateien oder Daten, die einer bestimmten Bedingungsanweisung entsprechen, unterliegen einer DLP-Richtlinie.

Zum Beispiel muss eine Datei eine Microsoft Word-Datei (Dateiattribut) sein UND bestimmte rechtliche Begriffe (Schlüsselwörter) UND Identifikationsnummern (Ausdrücke) enthalten, damit sie einer Richtlinie für "Anstellungsverträge" unterliegt. Auf Grund dieser Richtlinie können Mitarbeiter der Personalabteilung eine Datei an einen Drucker übertragen, damit die ausgedruckte Datei von einem Mitarbeiter unterschrieben werden kann. Die Übertragung über alle anderen möglichen Kanäle, wie etwa E-Mail, ist gesperrt.

Erstellen Sie Ihre eigenen Vorlagen, wenn Sie bereits über konfigurierte DLP-Datenbezeichner verfügen. Sie können auch vordefinierte Vorlagen verwenden. Weitere Informationen finden Sie unter *Benutzerdefinierte DLP-Vorlagen auf Seite 3-34* und *Vordefinierte DLP-Vorlagen auf Seite 3-33*.

Hinweis

Das Löschen einer Vorlage, die in einer DLP-Richtlinie verwendet wird, ist nicht möglich. Entfernen Sie die Vorlage aus der Richtlinie, bevor Sie sie löschen.

Vordefinierte DLP-Vorlagen

Die Prävention vor Datenverlust verfügt bereits über mehrere vordefinierte Vorlagen, die Sie zur Einhaltung verschiedener Regulierungsstandards verwenden können. Diese Vorlagen können weder geändert noch gelöscht werden.

- **GLBA**:Gramm-Leach-Billey Act
- **HIPAA**:Health Insurance Portability and Accountability Act
- **PCI-DSS**:PCI (Payment Card Industry Data Security Standard)

- **SB-1386**:US Senate Bill 1386
- **US PII**:Personenbezogene Daten (USA)

Eine detaillierte Liste zum Gebrauch aller vordefinierten Vorlagen und Beispiele zu den geschützten Daten finden Sie in der Dokumentation *Datenschutzlisten* unter:

https://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Benutzerdefinierte DLP-Vorlagen

Erstellen Sie Ihre eigenen DLP-Vorlagen, wenn Sie Datenbezeichner konfiguriert haben.

Eine DLP-Vorlage kombiniert Datenbezeichner und logische Operatoren (Und, Oder, Außer), um Bedingungsaussagen zu bilden.

Weitere Informationen und Beispiele zur Funktionsweise von Bedingungsanweisungen und logischen Operatoren finden Sie unter *Bedingungsanweisungen und logische pperatoren auf Seite 3-34*.

Bedingungsanweisungen und logische pperatoren

Bedingungen und Operatoren auf benutzerdefinierte DLP-Vorlagen anwenden.

Die Prävention vor Datenverlust überprüft Bedingungsanweisungen von links nach rechts. Seien Sie vorsichtig im Umgang mit logischen Operatoren bei der Konfiguration von Bedingungsanweisungen. Falscher Gebrauch von Operatoren führt zu einer fehlerhaften Bedingungsanweisung und zu eventuell unerwarteten Ergebnissen.

Die folgende Tabelle enthält einige Beispiele.

Tabelle 3-4. Beispielbedingungsaussagen

Bedingungsaussage	Interpretation und Beispiel
[Datenbezeichner 1] **Und** [Datenbezeichner 2] **Außer** [Datenbezeichner 3]	Eine Datei muss [Datenbezeichner 1] und [Datenbezeichner 2], aber nicht [Datenbezeichner 3] erfüllen. Beispiel: Eine Datei muss [ein Adobe PDF-Dokument] sein und muss [eine E-Mail-Adresse] enthalten, aber sollte kein [Schlüsselwort in der Liste der Schlüsselwörter] enthalten.
[Datenbezeichner 1] **Oder** [Datenbezeichner 2]	Eine Datei muss [Datenbezeichner 1] oder [Data Identifier 2] erfüllen. Beispiel: Eine Datei muss [ein Adobe PDF-Dokument] oder [ein Microsoft Word-Dokument] sein.
Außer [Datenbezeichner 1]	Eine Datei muss nicht [Datenbezeichner 1] erfüllen. Beispiel: Eine Datei muss keine [Multimedia-Datei] sein.

Wie das letzte Beispiel in der Tabelle zeigt, darf der erste Datenbezeichner in der Bedingungsanweisung den Operator "Außer" enthalten, wenn eine Datei nicht alle Datenbezeichner in der Anweisung erfüllen muss. In den meisten Fällen enthält der erste Datenbezeichner jedoch keinen Operator.

Vorlagen erstellen

Prozedur

1. Gehe zu **Richtlinien** > **Richtlinienressourcen** > **DLP-Vorlagen**.
2. Klicken Sie auf **Hinzufügen**.

   Ein neues Fenster wird geöffnet.
3. Geben Sie einen Namen für die Vorlage ein. Der Name darf nicht länger als 100 Byte sein und folgende Zeichen dürfen nicht enthalten sein:

   - > < * ^ | & ? \ /

4. Geben Sie eine Beschreibung mit maximal 256 Byte ein.
5. Wählen Sie die Datenbezeichner aus, und klicken Sie dann auf das Symbol "Hinzufügen".

   Zur Auswahl von Definitionen:

   - Wählen Sie mehrere Einträge aus, indem Sie die CTRL-Taste gedrückt halten und dann die Datenbezeichner auswählen.
   - Verwenden Sie die Suchfunktion, wenn Sie nach einer bestimmten Definition suchen. Sie können den Namen des Datenbezeichners vollständig oder teilweise eingeben.
   - Jede Vorlage darf nur maximal 30 Datenbezeichner enthalten.
6. Um einen neuen Ausdruck zu erstellen, klicken Sie auf **Ausdrücke**, und klicken Sie anschließend auf **Neuen Ausdruck hinzufügen**. Konfigurieren Sie die Einstellungen für den Ausdruck im Fenster, das angezeigt wird.
7. Um eine neue Dateiattributliste zu erstellen, klicken Sie auf **File attributes**, und klicken Sie anschließend auf **Neues Dateiattribut hinzufügen**. Konfigurieren Sie die Einstellungen für die Dateiattributliste im Fenster, das angezeigt wird.
8. Um eine neue Schlüsselwortliste zu erstellen, klicken Sie auf **Schlüsselwörter**, und klicken Sie anschließend auf **Neues Schlüsselwort hinzufügen**. Konfigurieren Sie die Einstellungen für die Schlüsselwortliste im Fenster, das angezeigt wird.
9. Wenn Sie einen Ausdruck ausgewählt haben, geben Sie die Anzahl der Vorkommen ein, das heißt die Anzahl, wie oft ein Ausdruck vorkommen muss, damit die Prävention vor Datenverlust ihn für eine Richtlinie berücksichtigt.
10. Wählen Sie einen logischen Operator für jede Definition.

Hinweis

Seien Sie vorsichtig im Umgang mit logischen Operatoren bei der Konfiguration von Bedingungsanweisungen. Falscher Gebrauch von Operatoren führt zu einer fehlerhaften Bedingungsanweisung und zu eventuell unerwarteten Ergebnissen. Beispiele für die richtige Verwendung finden Sie unter *Bedingungsanweisungen und logische pperatoren auf Seite 3-34*.

11. Um einen Datenbezeichner aus der Liste der ausgewählten Bezeichner zu entfernen, klicken Sie auf das Papierkorbsymbol.
12. Unterhalb der **Vorschau** überprüfen Sie die Bedingungsanweisung, und nehmen Sie Änderungen vor, wenn die Anweisung nicht Ihre Anforderungen erfüllt.
13. Klicken Sie auf **Speichern**.

Vorlagen importieren

Verwenden Sie diese Option, wenn Sie über eine ordnungsgemäß formatierte `.dat`-Datei verfügen, in der die Vorlagen gespeichert sind. Sie können die Datei erzeugen, indem Sie die Vorlagen entweder über den Server, auf den Sie gerade zugreifen, oder über einen anderen Server exportieren.

Prozedur

1. Navigieren Sie zu **Richtlinien** > **Richtlinienressourcen** > **DLP-Vorlagen**.
2. Klicken Sie auf **Importieren** und suchen Sie dann die `.dat`-Datei, in der die Vorlagen enthalten sind.
3. Klicken Sie auf **Öffnen**.

   Sie erhalten eine Nachricht, wenn der Import erfolgreich war. Wenn eine Vorlage importiert werden soll, die bereits vorhanden ist, wird sie übersprungen.

Regeln zum Eindringschutz

Der Bildschirm **Regeln zum Eindringschutz** zeigt die von der Trend Micro Apex Central Vulnerability Protection unterstützten Regeln zum Eindringschutz an. Regeln zum Eindringschutz untersuchen den tatsächlichen Inhalt von Netzwerkpaketen (und Paketfolgen). Basierend auf den in der Regel zum Eindringschutz festgelegten Bedingungen werden dann verschiedene Aktionen an diesen Paketen durchgeführt. Diese Aktionen umfassen das Ersetzen speziell definierter oder verdächtiger Byte-Sequenzen oder das vollständige Verwerfen von Paketen und das Zurücksetzen der Verbindung.

- Um die Liste der Regeln zu filtern, verwenden Sie das **Suchen**-Feld, um vollständige oder teilweise Zeichenfolgen anzugeben, die in einer der Spalten erscheinen.
- Um die Liste der Regeln zum Eindringschutz nach Spaltendaten zu sortieren, klicken Sie auf eine Spaltenüberschrift.
- Um die detaillierten Eigenschaften der Eindringungsschutzregel anzuzeigen, klicken Sie auf den Link in der Spalte **Regelname** einer Regel.
- Um den Datenverkehr von einem oder mehreren Quellendpunkten von der Vulnerability Protection-Überprüfung auszuschließen, klicken Sie auf **Ausnahmen konfigurieren** und geben Sie die Quell-IP-Adressen an.

  Hinweis

  Sie können bis zu 100 Einträge zur Ausnahmeliste hinzufügen.

Hinweis

Trend Micro Apex Central importiert/aktualisiert automatisch die Regeln zum Eindringschutz vom Apex One-Server während manueller oder geplanter Komponenten-Updates.

Wichtig

Jedes verwaltete Produkt bietet unterschiedliche Richtlinieneinstellungen, die Sie konfigurieren und auf Richtlinienziele anwenden können. Eine vollständige Liste der unterstützten verwalteten Produkte und der jeweiligen Richtlinieneinstellungen finden Sie im *Apex Central Widget- und Richtlinienverwaltungsleitfaden*.

Sie können eine PDF-Version des Handbuchs herunterladen oder das Handbuch online mithilfe des folgenden Links anzeigen:

https://docs.trendmicro.com/de-de/enterprise/apex-central.aspx

In der folgenden Tabelle werden die Regelinformationen erläutert, die im Fenster **Regeln zum Eindringschutz** angezeigt werden.

Spalte	Beschreibung
Kennung	Das eindeutige Identifizierungs-Tag für die Intrusion Prevention Regel
Regelname	Der Name der Eindringschutzregel
Anwendungstyp	Der Anwendungstyp, unter dem diese Eindringungsschutzregel gruppiert ist
Schweregrad	Der Schweregrad, den Trend Micro der Regel zuweist **Hinweis** Der Schweregrad einer Regel hat keinen Einfluss darauf, wie die Regel implementiert oder angewendet wird. Schweregrade können nützlich als Sortierkriterien sein, wenn eine Liste von Regeln zum Eindringschutz angezeigt wird.
Modus	Der Erkennungsmodus der Netzwerk-Engine, der vom Modul zur Eindringungsprävention verwendet wird. Klicken Sie auf einen Modus, um die Einstellung für die Regel zu konfigurieren.

Spalte	Beschreibung
Typ	Der erkannte Sicherheitstyp: • **Intelligent**: Bekannte oder unbekannte (zum Beispiel Zero-Day) Sicherheitslücke • **Schwachstelle**: Bekannter Exploit (normalerweise signaturbasiert) für eine bekannte Sicherheitslücke • **Sicherheitslücke**: Bekannte Sicherheitslücke, für die möglicherweise ein oder mehrere Exploits existieren
CVE	Die von MITRE zugewiesene Common Vulnerabilities and Exposures (CVE®)-Kennung für die Sicherheitslücke Weitere Informationen finden Sie unter http://cve.mitre.org/.
Microsoft	Die von Microsoft der Sicherheitslücke zugewiesene Common Vulnerabilities and Exposures (CVE®)-Kennung
CVSS-Bewertung	Der Schweregrad der Schwachstelle gemäß dem Common Vulnerability Scoring System (CVSS) und der nationalen Schwachstellendatenbank Weitere Informationen finden Sie unter http://nvd.nist.gov/cvss.cfm.
Zuletzt aktualisiert	Datum und Uhrzeit der letzten Änderung der Regel

Eigenschaften der Regeln zum Eindringschutz

Der Bildschirm **Eigenschaften der Regeln zum Eindringschutz** zeigt detaillierte Informationen zu einer bestimmten Eindringpräventionsregel und Sicherheitslücke an. Klicken Sie auf die Registerkarte **Allgemein** oder auf **Sicherheitslücke**, um Details zur Regel anzuzeigen.

Die folgenden Tabellen beschreiben die Informationen, die auf der Registerkarte **Allgemein** und der Registerkarte **Sicherheitslücke** bereitgestellt werden.

Tabelle 3-5. Allgemeine Informationen

Daten	Beschreibung
Kennung	Das eindeutige Identifizierungs-Tag für die Intrusion Prevention Regel

Daten	Beschreibung
Name	Der Name der Eindringschutzregel
Beschreibung	Die Beschreibung der Eindringschutzregel **Hinweis** Apex One Vulnerability Protection unterstützt nicht die Konfigurationsoptionen, die in der eigenständigen Version von Trend Micro Vulnerability Protection verfügbar sind.
Anwendungstyp	Der Anwendungstyp, unter dem diese Eindringungsschutzregel gruppiert ist
Priorität	Die Prioritätsstufe der Eindringungsschutzregel. Regeln mit höherer Priorität werden vor Regeln mit niedrigerer Priorität angewendet.
Schweregrad	Der Schweregrad, den Trend Micro der Regel zuweist **Hinweis** Der Schweregrad einer Regel hat keinen Einfluss darauf, wie die Regel implementiert oder angewendet wird. Schweregrade können nützlich als Sortierkriterien sein, wenn eine Liste von Regeln zum Eindringschutz angezeigt wird.
Modus	Der Erkennungsmodus der Netzwerk-Engine, der vom Modul zur Eindringungsprävention verwendet wird. Klicken Sie auf einen Modus, um die Einstellung für die Regel zu konfigurieren.
Typ	Der erkannte Sicherheitstyp: • **Intelligent**: Bekannte oder unbekannte (zum Beispiel Zero-Day) Sicherheitslücke • **Schwachstelle**: Bekannter Exploit (normalerweise signaturbasiert) für eine bekannte Sicherheitslücke • **Sicherheitslücke**: Bekannte Sicherheitslücke, für die möglicherweise ein oder mehrere Exploits existieren
Ausgestellt	Das Datum, an dem die Regel veröffentlicht wurde (nicht heruntergeladen)

Daten	Beschreibung
Zuletzt aktualisiert	Datum und Uhrzeit der letzten Änderung der Regel

Tabelle 3-6. Schwachstelleninformationen

Daten	Beschreibung
Schweregrad	Der Schweregrad der Sicherheitslücke
CVSS-Bewertung	Der Schweregrad der Schwachstelle gemäß dem Common Vulnerability Scoring System (CVSS) und der nationalen Schwachstellendatenbank Weitere Informationen finden Sie unter http://nvd.nist.gov/cvss.cfm.
Beschreibung	Die Beschreibung der Sicherheitslücke
Externe Referenzen	Bietet Links zu externen Referenzen für weitere Informationen über die Sicherheitslücke

Zulässige Geräte – Gerätesteuerung

Importieren oder exportieren Sie Listen von **Zulässige Geräte – Gerätesteuerung**, die für alle Apex One Security Agent-Richtlinienziele gelten.

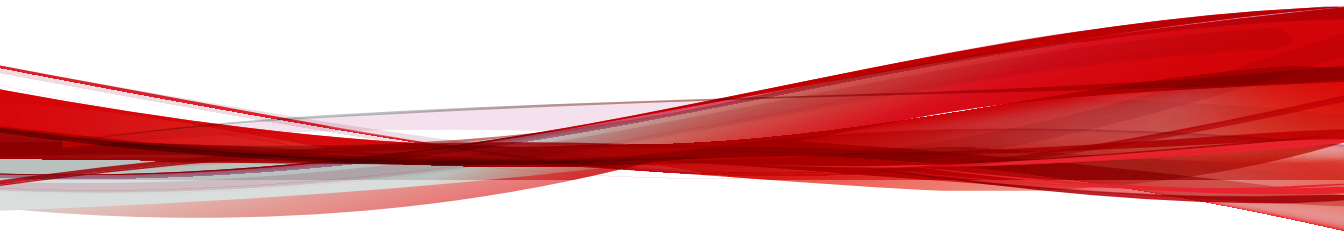
Hinweis

- Nur Security Agents mit aktiviertem Datenschutz überschreiben die Aktion „Sperren“ oder „Lesen“ bei Geräten, die zur Liste der erlaubten Geräte der Gerätesteuerung hinzugefügt wurden.
- Die Liste der erlaubten Geräte in der Gerätesteuerung gilt nicht für Security Agents ohne Datenschutz und Security Agents, bei denen die Berechtigung für die Gerätesteuerung nicht auf „Sperren“ oder „Lesen“ gesetzt ist.

Vorgang	Beschreibung
Importieren	Wählen Sie eine korrekt formatierte CSV-Datei aus, die eine Liste aller Geräte enthält, die Sie auf allen Apex One Security Agent Endpunkten zulassen möchten. **Wichtig** Das Importieren einer neuen Liste überschreibt die vorherige Liste vollständig. Um die bestehende Liste zu behalten, exportieren Sie die Liste, bevor Sie eine neue CSV-Datei importieren.
Zuletzt importiert	Das Datum/Uhrzeit, zu dem der Server die aktuelle Liste importiert hat
Gesamt erlaubte Geräte	Die Gesamtanzahl der erlaubten Geräte in der aktuell angewendeten Liste
Exportieren	Exportiert die aktuelle Zulassungsliste im CSV-Format

Teil II

Apex Central Widgets



Kapitel 4

Apex Central Dashboard-Widgets

Dieser Abschnitt enthält Hilfethemen für die Dashboard-Widgets, die spezifisch für das Trend Micro Apex Central-Managementkonsole-Dashboard sind.

Es werden folgende Themen behandelt:

Apex Central – häufigste dateibasierte Bedrohungen – Widgets

Dieses Widget verfolgt die Verteilung der häufigsten auf Endpunkten im Netzwerk erkannten Dateien und zeigt die vom Produkt erkannte Verteilung als eine der 10/25/50 häufigsten dateibasierten Bedrohungen (Viren und Spyware/Grayware).

Klicken Sie auf einen beliebigen Knoten in der Grafik, um ein Fenster mit ausführlichen Informationen anzuzeigen. Apex Central führt eine Protokollabfrage durch, um ausführliche Informationen anzugeben.

Geben Sie den Datumsbereich für die Daten an, die im Widget angezeigt werden:

- Heute
- 1 Woche
- 2 Wochen
- 1 Monat

Geben Sie die Bedrohung an, die im Widget angezeigt werden soll. Das Widget kann jeweils nur Daten für eine dateibasierte Bedrohung anzeigen. Standardmäßig zeigt das Widget alle Daten für alle verwalteten Produkte an, die gemäß den Kontoberechtigungen eines Benutzers zulässig sind.

Klicken Sie auf das Symbol mit den Widget-Einstellungen, um auf weitere Einstellungen zuzugreifen.

Einstellung	Beschreibung
Titel	Geben Sie einen neuen und aussagekräftigen Titel für das Widget in das Feld ein.
Bereich	Geben Sie den vom Widget angezeigten Datenbereich an. Der Bereich bestimmt die Produkte, die das Widget zum Anzeigen von Daten verwendet.
Häufigste Bedrohungen	Geben Sie die Anzahl der anzuzeigenden Bedrohungen an.

Klicken Sie auf **Speichern**, um Änderungen zu übernehmen und die Widget-Daten zu aktualisieren.

Endpunktschutzüberprüfung – Widget

Dieses Widget zeigt den Apex One- und Deep Security-Schutzstatus der Endpunkte einer integrierten Active Directory-Struktur an.

Wichtig

Vor der Verwendung dieses Widgets:

- Synchronisieren Sie die Apex One-Client-Ansicht mit der Active Directory-Struktur.

  Weitere Anweisungen finden Sie in der Dokumentation zu Apex One.

- Navigieren Sie zu **Administration** > **Einstellungen** > **Endpunktschutzüberprüfung**, um das Widget zu aktivieren und die Verbindungseinstellungen für den Active Directory-Server, den Apex One-Server und den Deep Security-Server zu konfigurieren.

Klicken Sie auf das Einstellungssymbol (>), um Folgendes zu konfigurieren:

- **Apex One-Server**: Klicken Sie auf die Schaltfläche zum Durchsuchen ( ), um die Apex One-Server anzugeben, die Daten für das Widget beitragen.
- **Deep Security-Server**: Klicken Sie auf die Schaltfläche zum Durchsuchen ( ), um die Deep Security-Server anzugeben, die Daten für das Widget beitragen.
- **Spalten**: Geben Sie die Spalten für das Widget an, die in der Datentabelle angezeigt werden sollen.

Klicken Sie auf eine Organisationseinheit in der Active Directory-Struktur, um die folgenden Informationen anzuzeigen.

Spalte	Beschreibung
Computer	Zeigt den Endpunktnamen an
Apex One	Zeigt an, ob der Endpunkt von einem Apex One- oder VDI-Client geschützt wird
Deep Security	Zeigt an, ob der Endpunkt von einem Deep Security-Agent geschützt wird
Physischer Host	Zeigt den physischen Server an, auf dem sich der virtuelle Endpunkt befindet
Pattern	Zeigt die Version der Pattern-Datei an, die der Apex One- oder VDI-Client verwendet
Scan Engine	Zeigt die Version der Scan Engine an, die der Apex One- oder VDI-Client verwendet
Client-Version	Zeigt die Version des Client-Programms an
Deep Security Profil	Zeigt das verwendete Deep Security-Profil an
Servername	Zeigt den Apex One- und/oder Deep Security-Server an, mit dem der Endpunkt eine Verbindung herstellt

Hosts mit C&C-Callback-Versuchen – Widget

Dieses Widget zeigt die Gesamtzahl eindeutig infizierter Hosts an und gruppiert diese nach C&C-Listenquelle.

Die Standardansicht enthält Daten für den aktuellen Tag.

Verwenden Sie die Dropdown-Liste **Bereich**, um den Zeitraum für die angezeigten Daten auszuwählen. Sie können Daten für **Heute**, **1 Woche**, **2 Wochen** oder **1 Monat** anzeigen.

Daten	Beschreibung
Hosts übereinstimmend mit Global Intelligence	Vom Trend Micro Global Intelligence-Netzwerk, einschließlich Smart Protection Network, erkannte C&C-Callbacks.

Daten	Beschreibung
Hosts übereinstimmend mit dynamischen Analyzern	Von dynamischen Analyzern, einschließlich Virtual Analyzer und der Prüf-Engine für Netzwerkinhalte, erkannte C&C-Callbacks. Analyzer sind in Produkte wie Deep Discovery Inspector und Apex One integriert.
Hosts übereinstimmend mit benutzerdefinierten Listen in verwalteten Produkten	Von Produkten mit Hilfe einer benutzerdefinierten Liste erkannte C&C-Callbacks. Ein Beispiel für eine benutzerdefinierte Liste ist die Liste 'Verweigern' in Deep Discovery Inspector.

Richtlinienstatus

Dieses Widget zeigt den Verteilungsstatus Ihrer Richtlinien an.

Durch Klicken auf den Namen einer Richtlinie oder die Anzahl der Ziele wird ein neues Fenster namens **Protokollabfrage** mit ausführlichen Informationen geöffnet.

Daten	Beschreibung
Richtlinie	Zeigt den Namen der Richtlinie an
Verteilungsstatus	Zeigt den Prozentsatz der Ziele an, die den Richtlinieneinstellungen entsprechen
Verteilt	Zeigt die Anzahl der Ziele an, auf die die Richtlinieneinstellungen angewendet wurden oder die über nicht aktivierte Produktdienste verfügen

Daten	Beschreibung
Ausstehend	Zeigt die Anzahl der Ziele an, auf die die Richtlinien nicht angewendet wurden **Hinweis** Wenn Hotfix 2575 nicht installiert ist, enthält die Spalte **Ausstehend** die Anzahl der Ziele, die über Offline-Agents verfügen.
Offline	Zeigt die Anzahl der Ziele an, die über Offline-Agents verfügen **Wichtig** Diese Funktion erfordert die Installation von Hotfix 2575. Andernfalls enthält die Spalte **Ausstehend** die Anzahl der Ziele, die Offline-Agents aufweisen, und die Spalte **Offline** wird nicht angezeigt.
Mit Problemen	Zeigt die Anzahl der Ziele an, auf die die Richtlinieneinstellungen aus folgenden Gründen nicht angewendet wurden: nicht unterstützte Richtlinienbereitstellung, keine Richtlinienkonfiguration, Systemfehler, Fehler bei der Kommunikation des Endpunkts mit dem Produktserver, nicht unterstützte Endpunkte, lokal geänderte Einstellungen, deaktivierte Produktdienste oder teilweise Bereitstellung
Endpunkte/Produkte ohne Richtlinien	Zeigt die Anzahl der Endpunkte oder der verwalteten Produkte an, auf die keine Richtlinie angewendet wurde
Gesamtzahl der Endpunkte/Produkte	Zeigt die Anzahl der Endpunkte oder der verwalteten Produkte an, die der Administrator verwalten kann

Schnellstart

Dieses Widget enthält Verknüpfungen zum **Produktverzeichnis** und zur **Richtlinienverwaltung**.

Eindeutige infizierte Hosts im Zeitverlauf – Widget

Dieses Widget zeigt die eindeutigen infizierten Hosts an, die innerhalb der letzten 30 Tage von verwalteten Produkten protokolliert wurden.

Dieses Widget gruppiert und zeigt die eindeutigen infizierten Hosts als Kreise an. Die Kreisgröße spiegelt die Anzahl der infizierten Hosts wieder.

- Klein: 1 bis 5
- Mittel: 6 bis 10
- Groß: 11 oder mehr

Bewegen Sie den Mauszeiger über das Symbol eines Computers oder den Namen eines Hosts, um weitere infizierte Hosts anzuzeigen.

Verwenden Sie die Dropdown-Liste **Callback-Adresse**, um infizierte Hosts mit Callback-Versuchen an der ausgewählten Callback-Adresse anzuzeigen.

Hinweis

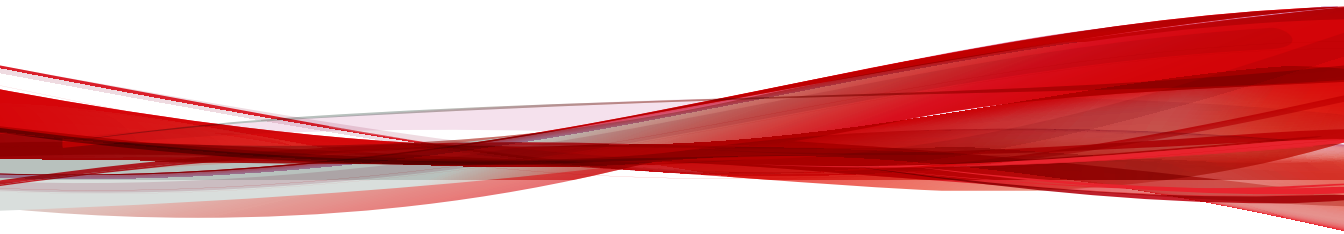
Die Dropdown-Liste **Callback-Adresse** enthält die 25 häufigsten Callback-Adressen.

Das Widget zeigt nur den ersten Callback-Versuch eines infizierten Hosts an der ausgewählten Callback-Adresse an.

Ändern Sie die verwalteten Produkte, die vom Widget als Quelle verwendet werden, indem Sie auf das Symbol für Einstellungen (>) klicken. Geben Sie im angezeigten Dialogfeld den **Bereich** an, indem Sie auf >> klicken und die als Quelle zu verwendenden verwalteten Produkte auswählen.

Teil III

Apex One Widgets



Kapitel 5

Apex One Dashboard-Widgets

In diesem Abschnitt werden die verfügbaren Apex One-Dashboard-Widgets in Trend Micro Apex Central beschrieben.

Es werden folgende Themen behandelt:

Erkennungs-Widget der Angriffserkennung

Dieses Widget zeigt die von der Endpoint Sensor Attack Discovery-Funktion generierten Erkennungsprotokolle basierend auf der Risikostufe für den angegebenen Zeitraum an.

Wichtig

Diese Funktion erfordert, dass Sie gültige Endpoint Sensor-Richtlinien auf Endpunkten bereitgestellt haben.

Klicken Sie auf den **Regelname**, um eine detaillierte Ansicht der Erkennung und aller zugehörigen Objekte anzuzeigen. Sie können eine Historische Untersuchung aller zugehörigen Objekte auslösen, indem Sie auf die Schaltfläche **Auswirkung bewerten** klicken.

Hinweis

Eine historische Untersuchung kann nur eine Bewertung basierend auf bestimmten Kriterientypen durchführen. Wenn Sie eine historische Untersuchung über das Angriffsentdeckungs-Widget durchführen, ignoriert die Untersuchung Objekte, für die keine Daten verfügbar sind.

Widget für schnelle Untersuchung

Dieses Widget ermöglicht es Ihnen, eine grundlegende historische Untersuchung in Ihrem Netzwerk mit einem einzigen Kriterientyp zu starten.

Wichtig

Diese Funktion erfordert, dass Sie gültige Endpoint Sensor-Richtlinien auf Endpunkten bereitgestellt haben.

Wählen Sie den Kriterientyp aus, geben Sie den Wert an und klicken Sie auf **Auswirkung bewerten**. Der Bildschirm **Verlaufsuntersuchung** erscheint mit den Bewertungsergebnissen.

Hinweis

Um eine komplexere Bewertung durchzuführen, verwenden Sie die Bildschirme für Historische Untersuchung oder Live-Untersuchung.

Top gesperrte Anwendungen

Dieses Widget bietet einen Überblick über die wichtigsten Anwendungen, auf die Benutzer in Verstoß gegen eine Application Control-Richtlinie zuzugreifen versuchten.

Verwenden Sie die Schaltfläche "Einstellungen", um die Standardanzahl der angezeigten Anwendungen zu ändern.

Top Endpunkte, die von IPS-Ereignissen betroffen sind Widget

Dieses Widget liefert Informationen über die Endpunkte, die von den meisten erkannten IPS-Ereignissen betroffen sind. IPS-Ereignisse werden durch Regeln zum Eindringschutz für Vulnerability Protection ausgelöst.

Verwenden Sie die Dropdown-Liste **Zeitraum**, um den Zeitraum für die angezeigten Daten auszuwählen.

Verwenden Sie das Einstellungssymbol (>), um die Standardanzahl der betroffenen Endpunkte zur Anzeige zu ändern.

Daten	Beschreibung
Endpunkt	Der Name des Endpunkts
IP-Adresse	IP-Adresse des Endpunkts
Funde	Die Anzahl der auf dem Endpunkt erkannten IPS-Ereignisse

Häufigste IPS-Angriffsquellen

Dieses Widget bietet Informationen über die wichtigsten Angriffsquellen für IPS-Ereignisse, die in Ihrem Netzwerk erkannt wurden. IPS-Ereignisse

werden durch Regeln zum Eindringschutz für Vulnerability Protection ausgelöst.

Verwenden Sie die Dropdown-Liste **Zeitraum**, um den Zeitraum für die angezeigten Daten auszuwählen.

Verwenden Sie das Einstellungssymbol (>), um die Standardanzahl der anzuzeigenden Angriffsquellen zu ändern.

Daten	Beschreibung
Angriffsquelle	Die IP-Adresse der Quelle des bekannten Angriffs
Speicherort	Der Standort der Angriffsquelle
Funde	Die Anzahl der auf dem Endpunkt erkannten IPS-Ereignisse

Top-IPS-Ereignisse

Dieses Widget bietet Informationen über die Regeln zum Eindringschutz, die die meisten IPS-Ereignisse in Ihrem Netzwerk auslösen. IPS-Ereignisse werden durch Regeln zum Eindringschutz für Vulnerability Protection ausgelöst.

Verwenden Sie die Dropdown-Liste **Zeitraum**, um den Zeitraum für die angezeigten Daten auszuwählen.

Sie können auch das zweite Dropdown-Menü verwenden, um nur die obersten **Entdeckt** oder **Verhindert** IPS-Ereignisse anzuzeigen.

Verwenden Sie das Einstellungssymbol (>), um die Standardanzahl der ausgelösten Regeln zum Eindringschutz anzuzeigen.

Daten	Beschreibung
Regelname	Der Name der Eindringschutzregel
Schweregrad	Der Schweregrad, den Trend Micro der Regel zuweist
Gesamt	Die Anzahl der durch die Intrusion Prevention-Regel ausgelösten IPS-Ereignisse

Top verletzte Application Control-Kriterien

Dieses Widget bietet einen Überblick über die wichtigsten Application Control-Kriterien, die Benutzer ausgelöst haben, als sie versuchten, auf nicht autorisierte Anwendungen zuzugreifen.

Verwenden Sie die Schaltfläche "Einstellungen", um die standardmäßige Anzahl der angezeigten Übereinstimmungen zu ändern.

Teil IV

Apex One Server-Richtlinieneinstellungen

In diesem Abschnitt wird beschrieben, wie Sie die Richtlinieneinstellungen des Apex One-Servers verwalten können.

Kapitel 6

Apex One Server-Richtlinieneinstellungen

In diesem Abschnitt wird beschrieben, wie Sie die Richtlinieneinstellungen des Apex One-Servers verwalten können.

Endpoint Sensor-Servereinstellungen konfigurieren

Wichtig

- Die Endpoint Sensor-Funktion erfordert eine spezielle Lizenzierung und zusätzliche Systemvoraussetzungen. Stellen Sie sicher, dass Sie die richtige Lizenz haben, bevor Sie Endpoint Sensor-Richtlinien auf Endpunkten bereitstellen. Für weitere Informationen zum Erwerb von Lizenzen wenden Sie sich an Ihren Support-Anbieter.
- Serverrichtlinien gelten nur für lokale Apex One-Server.

Prozedur

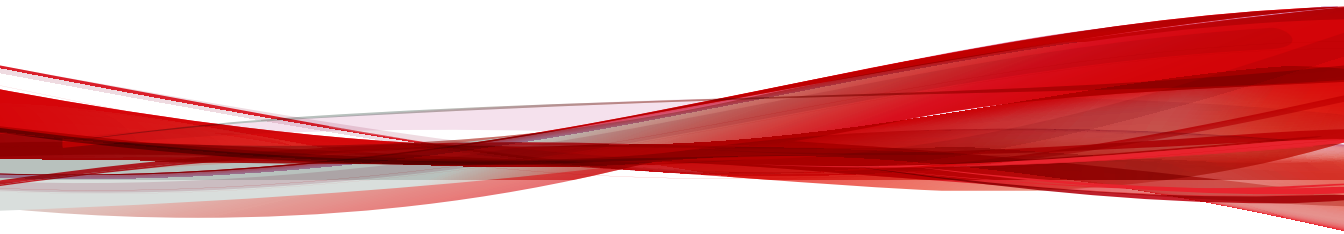
1. Wählen Sie **Apex One Server** als **Produkt** aus.
2. Erstellen oder bearbeiten Sie eine Richtlinie.
   a. Klicken Sie auf **Erstellen**, um eine Richtlinie zu erstellen.
   b. Um eine Richtlinie zu bearbeiten, klicken Sie auf einen Richtliniennamen in der **Richtlinie**-Spalte.
3. Konfigurieren Sie **Endpoint Sensor-Einstellungen**.

Optionen	Beschreibung
Maximale Metadatenspeicherung	Geben Sie die maximal zulässige Größe für die Metadatenspeicherung an. Geben Sie eine Größe zwischen 20 und 20480 GB an. Die standardmäßige Speichergröße beträgt 1024 GB (1 TB). Sobald die Metadatenspeicherung diese Größe erreicht, löscht der Server alte Datensätze, um Platz für neue zu schaffen. **Hinweis** Für Apex One mit Kritischen Patch 9601 (oder späteren Versionen) beträgt die Standard-Speichergröße 400 GB.
Maximale Speicherzuweisung	Geben Sie die maximale Menge an Speicher an, die dem Metadaten-Cache zugewiesen wird. Geben Sie eine Größe zwischen 4 GB und 48 GB an. Die neue angegebene Größe muss größer als die aktuelle Größe sein. Die standardmäßige Zuweisungsgröße beträgt 4 GB. **Hinweis** Die Speichergröße beeinflusst die Leistung von Daten-Uploads und die Geschwindigkeit der Untersuchung. Um die Leistung zu verbessern, erhöhen Sie die Speichergröße des betroffenen Servers.

4. Klicken Sie auf **Verteilen** oder **Speichern**.

Teil V

Apex One Security Agent Richtlinien



Kapitel 7

Agentenkonfigurationen

In diesem Abschnitt wird beschrieben, wie Sie das Security Agent-Programm auf Endpunkten verwalten können.

Es werden folgende Themen behandelt:

- *Update Agents auf Seite 7-2*
- *Berechtigungen und andere Einstellungen auf Seite 7-2*
- *Zusätzliche Diensteinstellungen auf Seite 7-19*

Update Agents

Für die Zuordnung des Verteilvorgangs von Komponenten, Domäneneinstellungen oder Agent-Programmen und Hotfixes an Security Agents verwenden Sie Security Agents als Update-Agents oder Update-Adressen für andere Security Agents. Auf diese Weise erhalten die Security Agents rechtzeitig ihre Updates, ohne die Verbindung zum Apex One Server durch ein hohes Netzwerk-Datenverkehrsvolumen zu belasten.

Wenn das Netzwerk beispielsweise nach Standorten segmentiert ist und das Datenaufkommen über die Netzwerkverbindung besonders hoch ist, sollten Sie mindestens einen Update-Agent pro Standort einrichten.

Hinweis

Security Agents Agents, für die die Aktualisierung von Komponenten über einen Update-Agent zugewiesen ist, erhalten über den Update-Agent nur aktualisierte Komponenten und Einstellungen. Alle Security Agents melden ihren Status weiterhin an den Apex One Server.

Security Agents als Update-Agents zuweisen

Prozedur

1. Wählen Sie die Komponenten aus, die Update-Agents freigeben können.
   - Komponenten-Updates
   - Domäneneinstellungen
   - Security Agent-Programme und Hotfixes

Berechtigungen und andere Einstellungen

Konfigurieren Sie Security Agents, um Benutzern Rechte zum Konfigurieren personalisierter Einstellungen zu erteilen, Benachrichtigungen anzuzeigen und wichtige Security Agent-Dateien und -Dienste zu schützen.

Agent-Berechtigungen konfigurieren

Prozedur

1. Konfigurieren Sie die gewünschten Einstellungen.

Abschnitt	Einstellungen
Unabhängiger Modus	**Unabhängigen Modus aktivieren**: Ermöglicht Benutzern die Deaktivierung der folgenden Funktionen im Security Agent, um zu verhindern, dass der Security Agent die Systemleistung negativ beeinflusst: • In diesem Modus akzeptiert der Security Agent keine Richtlinieneinstellungen vom Server. • In diesem Modus startet der Security Agent Suchbefehle über den Server. • In diesem Modus sendet der Security Agent keine Protokolle an den Server. Endbenutzer können Suchläufe und Updates auf Agents im unabhängigen Modus manuell starten.
Suchvorgänge	• **Manuelle Suche konfigurieren**: Ermöglicht Benutzern die Konfiguration der Einstellungen für die **Manuelle Suche** in der Security Agent-Konsole. • **Echtzeitsuche konfigurieren**: Ermöglicht Benutzern die Konfiguration der Einstellungen für die **Echtzeitsuche** in der Security Agent-Konsole. • **Zeitgesteuerte Suche konfigurieren**: Ermöglicht Benutzern die Konfiguration der Einstellungen für die **zeitgesteuerte Suche** in der Security Agent-Konsole.

Abschnitt	Einstellungen
Zeitgesteuerte Suche	• **Zeitgesteuerte Suche verschieben**: Ermöglicht Benutzern, eine zeitgesteuerte Suche zu verschieben, bevor die Suche gestartet wird, oder eine zurzeit ausgeführte Suche für eine bestimmte Zeit anzuhalten. **Hinweis** Benutzer können eine ausgeführte Suche nur ein Mal anhalten. Nachdem die Suche neu gestartet wurde, werden alle Dateien auf dem Endpunkt von Security Agent erneut durchsucht. • **Zeitgesteuerte Suche überspringen und beenden**: Ermöglicht Benutzern das einmalige Überspringen oder Beenden einer ausgeführten zeitgesteuerten Suche. **Hinweis** Benutzer können eine zeitgesteuerte Suche nur einmal überspringen oder beenden. Selbst nach einem Neustart des Systems setzt die zeitgesteuerte Suche die Suche basierend auf dem nächsten geplanten Zeitpunkt fort.

Abschnitt	Einstellungen
Firewall	• **Anzeige der Firewall-Einstellungen in der Security Agent-Konsole**: Ermöglicht Benutzern die Konfiguration der Einstellungen für die **Firewall** in der Security Agent-Konsole • **Benutzer dürfen Firewall, Intrusion Detection System (IDS) und Warnmeldung der Firewall aktivieren/deaktivieren**: Zeigt die Menüoptionen **Firewall aktivieren/deaktivieren** und **IDS-Modus aktivieren/deaktivieren** über das Security Agent-Taskleistensymbol an. **Hinweis** Die Apex One Firewall schützt Agents und Server im Netzwerk mit Stateful-Inspection-Technologie und leistungsstarkes Suchen und Entfernen von Netzwerkviren. Wenn Sie Benutzern die Berechtigung erteilen, die Firewall und ihre Funktionen zu aktivieren bzw. zu deaktivieren, warnen Sie sie vor der Deaktivierung der Firewall über einen längeren Zeitraum, um zu verhindern, dass die Gefahr von Intrusion- und Hackerangriffen für den Endpunkt entsteht. • **Security Agents erlauben, Firewall-Protokolle an den Apex One-Server zu senden**: Konfiguriert den Security Agent so, dass Firewall-Protokolle an den Server gesendet werden, damit der Netzwerkdatenverkehr analysiert werden kann
Verhaltensüberwachung	**Die Einstellungen für die Verhaltensüberwachung auf der Security Agent-Konsole anzeigen**: Ermöglicht Benutzern die Konfiguration der Einstellungen für die **Verhaltensüberwachung** in der Security Agent-Konsole
Liste der vertrauenswürdigen Programme	**Die Liste der vertrauenswürdigen Programme auf der Security Agent-Konsole anzeigen**: Ermöglicht Benutzern die Konfiguration der **Liste der vertrauenswürdigen Programme** in der Security Agent-Konsole

Abschnitt	Einstellungen
Mail Scan	**Zeigen Sie die Mail Scan-Einstellungen in der Security Agent-Konsole an**: Ermöglicht Benutzern die Konfiguration der Einstellungen für die **Mail Scan** in der Security Agent-Konsole Ist diese Option aktiviert, kann die Echtzeitsuche vom Mail-Server abgerufene POP3-E-Mail-Nachrichten erkennen, die bösartige Bedrohungen enthalten, und entsprechende Maßnahmen ergreifen.
Proxy-Einstellungen	**Benutzern die Konfiguration der Proxy-Einstellungen erlauben**: Ermöglicht Benutzern nur unter folgenden Umständen benutzerdefinierte Proxy-Einstellungen zu verwenden: • Wenn Security Agents "Jetzt aktualisieren" ausführen. • Wenn die automatischen Proxy-Einstellungen von den Benutzern deaktiviert oder vom Security Agent nicht erkannt werden. **Warnung!** Vom Benutzer fehlerhaft konfigurierte Proxy-Einstellungen können zu Update-Problemen führen. Gehen Sie mit Bedacht vor, wenn Sie Benutzern die Erlaubnis zur Konfiguration der Proxy-Einstellungen geben.
Komponenten -Updates	• **"Jetzt aktualisieren" ausführen**: Zeigt die Menüoption **Jetzt aktualisieren** über das Security Agent-Taskleistensymbol an. • **Zeitgesteuerte Updates aktivieren/deaktivieren**: Zeigt die Menüoption **Zeitgesteuerte Updates aktivieren/deaktivieren** über das Security Agent-Taskleistensymbol an. **Hinweis** Administratoren müssen zunächst auf der Registerkarte **Andere Einstellungen** die Option **Zeitgesteuerte Updates auf Security Agents aktivieren** auswählen, damit das entsprechende Menüelement im Security Agent-Menü angezeigt wird.

Abschnitt	Einstellungen
Beenden und entsperren	Die Berechtigung zum Beenden und Entsperren des Security Agents erlaubt dem Benutzer, den Security Agent vorübergehend anzuhalten oder mit oder ohne Kennwort auf erweiterte Webkonsolenfunktionen zuzugreifen. • **Kein Kennwort erforderlich** • **Kennwort erforderlich**: Geben Sie das erforderliche Kennwort und das Bestätigungskennwort ein. **Hinweis** Kennwörter müssen die folgenden Komplexitätsvoraussetzungen erfüllen: • Länge von 8 bis 32 Zeichen • Mindestens eines der folgenden Zeichen: Großbuchstaben (A-Z), Kleinbuchstaben (a-z), numerische Zeichen (0-9) und Sonderzeichen • Nicht druckbare ASCII-Zeichen dürfen nicht enthalten sein **Wichtig** Wenn Sie **Requires a password** auswählen und kein Passwort angeben, wendet Trend Micro Apex Central das folgende Standardpasswort an: • Für lokale Apex One Versionen: Das während der Serverinstallation angegebene Kennwort • Für Apex One als Service: Der Kontoname, der zur Bereitstellung der Konsole verwendet wird

Abschnitt	Einstellungen
Deinstallation	Die Security Agent-Deinstallationsberechtigung ermöglicht Benutzern die Deinstallation des Security Agent-Programms auf lokalen Endpunkten. • **Kein Kennwort erforderlich** • **Kennwort erforderlich**: Geben Sie das erforderliche Kennwort und das Bestätigungskennwort ein. **Hinweis** Kennwörter müssen die folgenden Komplexitätsvoraussetzungen erfüllen: • Länge von 8 bis 32 Zeichen • Mindestens eines der folgenden Zeichen: Großbuchstaben (A-Z), Kleinbuchstaben (a-z), numerische Zeichen (0-9) und Sonderzeichen • Nicht druckbare ASCII-Zeichen dürfen nicht enthalten sein **Wichtig** Wenn Sie **Requires a password** auswählen und kein Passwort angeben, wendet Trend Micro Apex Central das folgende Standardpasswort an: • Für lokale Apex One Versionen: Das während der Serverinstallation angegebene Kennwort • Für Apex One als Service: Der Kontoname, der zur Bereitstellung der Konsole verwendet wird

Andere Agent-Einstellungen konfigurieren

Prozedur

1. Konfigurieren Sie die gewünschten Einstellungen.

Abschnitt	Einstellungen
Konvertierung im Koexistenzmodus	**Security Agents im Koexistenzmodus dauerhaft in voll funktionsfähige Security Agents umwandeln**: Aktivierte alle Funktionen auf Security Agents, die im „Koexistenzmodus“ konfiguriert sind **Wichtig** Dieser Vorgang kann nicht rückgängig gemacht werden. Nachdem Sie Security Agents im Koexistenzmodus in voll funktionsfähige Security Agents konvertiert haben, versucht das Agent-Programm sämtliche inkompatible Sicherheitssoftware von Drittanbietern auf dem Endpunkt zu deinstallieren. Nach Abschluss der Konvertierung aktiviert Apex One alle erforderlichen Dienste und Funktionen im Zusammenhang mit der normalen Funktion von Security Agent. Wenn Sie einen Security Agent im Koexistenzmodus auf einem konvertierten Endpunkt verwenden müssen, deinstallieren Sie das Security Agent-Programm und führen Sie die Neuinstallation eines Security Agent im Koexistenzmodus durch.

Abschnitt	Einstellungen

Update-Einstellungen	• **Security Agents laden Updates vom Trend Micro ActiveUpdate Server herunter**: Hiermit werden Security Agents konfiguriert, die keine Verbindung zu der angegebenen Update-Quelle herstellen können, um ein Update über den Trend Micro ActiveUpdate Server durchzuführen
	• **Zeitgesteuerte Updates auf Security Agents aktivieren**: Konfiguriert alle Security Agents, um zeitgesteuerte Updates standardmäßig zu aktivieren
	• **Security Agents aktualisieren nur die folgenden Komponenten**: Hiermit wird gesteuert, wie Komponenten-Updates auf den Security Agents durchgeführt werden
	  • **Alle Komponenten (einschließlich Hotfixes und Agent-Programm)**: Security Agents aktualisiert alle Komponenten
	  • **Pattern-Dateien, Engines, Treiber**: Security Agents führen kein Upgrade des Security Agent-Programms durch und stellen keine Hotfixes bereit
	  • **Pattern-Dateien**: Security Agents führen kein Upgrade des Security Agent-Programms durch, stellen keine Hotfixes bereit und aktualisieren keine Engines und Treiber

Web-Reputation-Einstellungen	**Benachrichtigung anzeigen, wenn eine Website gesperrt ist**: Zeigt eine Benachrichtigung auf dem Security Agent an, nachdem eine URL gesperrt wurde, die eine Web-Reputation-Richtlinie verletzt.
Einstellungen der Verhaltensüberwachung	**Benachrichtigung anzeigen, wenn ein Programm gesperrt ist**: Zeigt eine Benachrichtigung auf dem Security Agent an, nachdem ein Programm gesperrt wurde, das eine Verhaltensüberwachungs-Richtlinie verletzt.
C&C-Kontakt – Alarmeinstellungen	**Benachrichtigung anzeigen, wenn ein C&C-Callback erkannt wird**: Zeigt eine Benachrichtigung auf dem Security Agent an, nachdem ein C&C-Callback erkannt wurde.
Einstellungen der zentralen Quarantänewiederherstellung	**Bei der Wiederherstellung einer Datei aus der Quarantäne eine Benachrichtigung anzeigen**: Zeigt eine Benachrichtigung auf dem Security Agent an, nachdem eine unter Quarantäne gestellte Datei wiederhergestellt wurde.

Abschnitt	Einstellungen
Einstellungen für das Vorrausschaunde Maschinenlernen	**Bei Bedrohungsfund Benachrichtigung anzeigen**: Zeigt eine Benachrichtigung auf dem Security Agent an, nachdem das vorausschauende Maschinenlernen eine unbekannte Bedrohung erkannt hat.
Eigenschutz des Security Agents	• **Security Agent-Dienste schützen**: Verhindert, dass Benutzer oder Anwendungen die Security Agent-Dienste beenden • **Dateien im Security Agent-Installationsordner schützen**: Verhindert, dass Benutzer oder Anwendungen Dateien im Security Agent-Installationsordner ändern oder löschen • **Security Agent-Registrierungsschlüssel schützen**: Verhindert, dass Benutzer oder Anwendungen vom Security Agent-Programm verwendete Registrierungswerte ändern, löschen oder hinzufügen • **Security Agent-Prozesse schützen**: Verhindert, dass Benutzer oder Anwendungen Security Agent-Prozesse beenden Weitere Informationen finden Sie unter *Security Agent Eigenschutz auf Seite 7-12*.
Einstellungen für die zeitgesteuerte Suche	**Benachrichtigung anzeigen, bevor die zeitgesteuerte Suche ausgeführt wird**: Zeigt eine Benachrichtigung auf dem Security Agent an, bevor eine konfigurierte, zeitgesteuerte Suche gestartet wird.
Cache-Einstellungen für die Suche	• **Digitalen Signatur-Cache aktivieren**: Konfiguriert den Security Agent für die Verwendung des Patterns für digitale Signaturen der Verhaltensüberwachung, um Dateien aus der manuellen Suche, der zeitgesteuerten Suche und der sofortigen Suche ("Jetzt durchsuchen") auszuschließen. • **Cache für die On-Demand-Suche aktivieren**: Konfiguriert den Security Agent für die Bereitstellung eines On-Demand-Caches für die Suche, um zwecks Leistungsverbesserung Dateien während der manuellen Suche, der zeitgesteuerten Suche und der sofortigen Suche ("Jetzt durchsuchen") auszuschließen. Weitere Informationen finden Sie unter *Cache-Einstellungen für die Suche auf Seite 7-15*.

Abschnitt	Einstellungen
Einstellungen für die Suche in POP3-Mails	**POP3-Mail durchsuchen**: Aktiviert die POP3-Mail-Suche auf dem Security Agent Weitere Informationen finden Sie unter *POP3 Mail Scan auf Seite 7-18*.
Einschränkung des Zugriffs auf Security Agent	**Den Zugriff auf die Security Agent-Konsole über die Taskleiste oder das Windows Start-Menü für Benutzer einschränken**: Deaktiviert den Benutzerzugriff auf die Security Agent-Konsole über die Taskleiste oder das Windows-Startmenü **Hinweis** Diese Einstellung deaktiviert nicht den Security Agent. Der Security Agent wird im Hintergrund ausgeführt und schützt so vor Sicherheitsrisiken.
Aufforderung zum Neustart	**Eine Benachrichtigung anzeigen, wenn der Endpunkt zum Säubern infizierter Dateien neu gestartet werden muss**: Zeigt eine Benachrichtigung auf dem Security Agent an, wenn der Benutzer den Endpunkt neu starten muss, um das Säubern einer bösartigen Datei abzuschließen.

Security Agent Eigenschutz

Der Eigenschutz des Security Agents ermöglicht dem Security Agent das Schützen der Prozesse und anderer Ressourcen, damit diese ordnungsgemäß funktionieren. Der Eigenschutz des Security Agents vereitelt Versuche von Programmen oder Benutzern, den Anti-Malware-Schutz zu deaktivieren.

Security Agent-Dienste schützen

Apex One sperrt alle Versuche, die folgenden Security Agent-Dienste zu beenden:

- Apex One NT Listener (`TmListen.exe`)
- Apex One NT RealTime Scan (`NTRtScan.exe`)
- Apex One NT Firewall (`TmPfw.exe`)

- Trend Micro Apex One Datenschutzdienst (`dsagent.exe`)
- Trend Micro Unauthorized Change Prevention Service (`TMBMSRV.exe`)

Hinweis

Wenn diese Option aktiviert ist, verhindert der Security Agent möglicherweise, dass Produkte anderer Hersteller erfolgreich auf den Endpunkten installiert werden. Wenn Sie dieses Problem feststellen, können Sie diese Option vorübergehend deaktivieren und nach der Installation des Fremdprodukts wieder aktivieren.

- Gemeinsames Client Solution Framework für Apex One (`TmCCSF.exe`)

Dateien im Security Agent-Installationsordner schützen

Um zu verhindern, dass andere Programme oder gar Benutzer die Security Agent-Dateien ändern oder löschen, sperrt Apex One die folgenden Dateien im `<Agent installation folder>`:

- Alle digital signierten Dateien mit den Dateinamenserweiterungen `.exe`, `.dll` und `.sys`
- Einige Dateien ohne digitale Signaturen, inkl.:
  - `bspatch.exe`
  - `bzip2.exe`
  - `INETWH32.dll`
  - `libcurl.dll`
  - `libeay32.dll`
  - `libMsgUtilExt.mt.dll`
  - `msvcm80.dll`
  - `MSVCP60.DLL`
  - `msvcp80.dll`
  - `msvcr80.dll`
  - `OfceSCV.dll`
  - `OFCESCVPack.exe`
  - `patchbld.dll`
  - `patchw32.dll`
  - `patchw64.dll`
  - `PiReg.exe`
  - `ssleay32.dll`
  - `Tmeng.dll`
  - `TMNotify.dll`
  - `zlibwapi.dll`

Security Agent-Registrierungsschlüssel schützen

Der Security Agent sperrt alle Versuche, unter den folgenden Registrierungsschlüsseln und Unterschlüsseln Einträge zu ändern, zu löschen oder neue Einträge hinzuzufügen:

- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion`
- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\NSC`
- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Osprey`
- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\AMSP`

Security Agent-Prozesse schützen

Der Security Agent sperrt alle Versuche, die Prozesse in der folgenden Tabelle zu beenden.

Prozess	Beschreibung
`TmListen.exe`	Empfängt Befehle und Benachrichtigungen vom Apex One Server und ermöglicht die Kommunikation zwischen Security Agent und Server
`NTRtScan.exe`	Führt die Echtzeitsuche, die zeitgesteuerte oder die manuelle Suche auf den Security Agents durch.
`TmPfw.exe`	Bietet eine Firewall auf Paketebene, Netzwerkvirensuche und Funktionen zur Erkennung von Eindringlingen.
`TMBMSRV.exe`	Reguliert den Zugriff auf externe Speichergeräte und verhindert unbefugte änderungen an Registrierungsschlüsseln und Prozessen.
`DSAgent.exe`	überwacht die übertragung vertraulicher Daten und steuert den Zugriff auf Geräte
`PccNTMon.exe`	Dieser Prozess ist verantwortlich für den Start der Security Agent-Konsole.
`TmCCSF.exe`	Führt die Funktion zur Verhinderung von Browser-Schwachstellen und die Arbeitsspeichersuche aus.

Der Security Agent kann auch vor dem Hinzufügen von Prozessen in den Microsoft-Richtlinien für Softwareeinschränkungen (Software Restriction

Policies, SRP) schützen. Durch Software Restriction Policies wird die Ausführung der aufgelisteten Anwendungen auf dem Endpunkt verhindert. So verhindern Sie das Hinzufügen von Security Agent Prozessen in der Software Restriction Policies-Liste:

1. Aktivieren Sie **Security Agent-Prozesse schützen**.
2. Aktivieren Sie den **Unauthorized Change Prevention Service**.

Cache-Einstellungen für die Suche

Der Security Agent kann eine digitale Signatur erstellen und bei Bedarf Dateien aus dem Cache durchsuchen, um die Suchleistung zu verbessern. Bei einer bedarfsorientierten Suche überprüft der Security Agent zuerst die Cache-Datei mit den digitalen Signaturen und dann die Cache-Datei nach Dateien, die von der Suche ausgeschlossen werden sollen. Die Suchdauer wird reduziert, wenn viele Dateien von der Suche ausgeschlossen werden.

Digitaler Signatur-Cache

Die Cache-Datei mit den digitalen Signaturen wird während der manuellen Suche, der zeitgesteuerten Suche und der Sofortsuche verwendet. Agents durchsuchen keine Dateien, deren Signaturen zur Cache-Datei mit den digitalen Signaturen hinzugefügt wurden.

Der Security Agent verwendet das gleiche Pattern für digitale Signaturen, das bei der Verhaltensüberwachung zur Erstellung der Datei mit den digitalen Signaturen verwendet wird. Das Pattern für digitale Signaturen enthält eine Liste von Dateien, die Trend Micro als vertrauenswürdig erachtet und deshalb von der Suche ausschließt.

Hinweis

Die Verhaltensüberwachung wird auf Windows Server-Plattformen automatisch deaktiviert. Wenn der Cache für digitale Signaturen aktiviert ist, laden Security Agents auf diesen Plattformen das Pattern für digitale Signaturen zur Verwendung im Cache herunter. Die Komponenten der Verhaltensüberwachung werden aber nicht heruntergeladen.

Agents erstellen die Cache-Datei mit den digitalen Signaturen nach einem Zeitplan, der über die Webkonsole konfiguriert werden kann. Agents gehen so vor, um:

- Die Signaturen neuer Dateien hinzuzufügen, die seit der letzten Erstellung der Cache-Datei in das System eingeführt wurden
- Die Signaturen der Dateien zu entfernen, die verändert oder aus dem System gelöscht wurden

Während der Cache-Erstellung überprüfen die Agents folgende Ordner auf vertrauenswürdige Dateien und fügen dann die Signaturen für diese Dateien zur Cache-Datei mit den digitalen Signaturen hinzu:

- `%PROGRAMFILES%`
- `%WINDIR%`

Die Cache-Erstellung hat keine Auswirkung auf die Leistung des Endpunkts, da die Agents während dieses Prozesses nur minimale Systemressourcen benötigen. Agents können auch eine bereits begonnene Cache-Erstellung wieder fortsetzen, wenn dieser Vorgang aus einem bestimmten Grund abgebrochen wurde (zum Beispiel, wenn der Rechner von der Stromquelle getrennt wurde oder wenn das Netzteil eines Wireless-Endpunkts nicht angeschlossen ist).

Cache für die On-Demand-Suche

Die Cache-Datei für die On-Demand-Suche wird während der manuellen Suche, der zeitgesteuerten Suche und der Sofortsuche verwendet.Security Agents durchsuchen keine Dateien, deren Cache zur Cache-Datei für die On-Demand-Suche hinzugefügt wurde.

Bei jeder Suche überprüft der Security Agent die Eigenschaften der bedrohungsfreien Dateien. Wenn eine bedrohungsfreie Datei in einem bestimmten (konfigurierbaren) Zeitraum nicht verändert wurde, fügt der Security Agent den Cache der Datei zur Cache-Datei für die On-Demand-Suche hinzu. Bei der nächsten Suche wird diese Datei dann nicht durchsucht, wenn ihr Cache nicht abgelaufen ist.

Der Cache einer bedrohungsfreien Datei läuft nach einer bestimmten (ebenfalls konfigurierbaren) Anzahl von Tagen ab. Wird die Suche bei

oder nach Ablauf des Caches durchgeführt, entfernt der Security Agent den abgelaufenen Cache und durchsucht die Datei nach Bedrohungen. Ist die Datei bedrohungsfrei und bleibt unverändert, wird der Cache der Datei wieder zur Cache-Datei für die bedarfsgesteuerte Suche hinzugefügt. Ist die Datei bedrohungsfrei, wurde aber vor kurzem verändert, wird der Cache nicht hinzugefügt, und die Datei wird bei der nächsten Suche wieder durchsucht.

Der Cache einer bedrohungsfreien Datei läuft ab, um den Auschluss infizierter Dateien von der Suche, wie in den folgenden Beispielen dargestellt, zu verhindern:

- Es ist möglich, dass eine stark veraltete Pattern-Datei eine infizierte, nicht veränderte Datei als bedrohungsfrei eingestuft hat. Wenn der Cache nicht abläuft, verbleibt die infizierte Datei im System, bis sie verändert und von der Echtzeitsuche entdeckt wird.
- Wenn eine gecachte Datei verändert wurde und die Echtzeitsuche zum Zeitpunkt der Dateiänderung nicht funktionsfähig war, muss der Cache ablaufen, damit die veränderte Datei nach Bedrohungen durchsucht werden kann.

Die Anzahl der Caches, die zur Cache-Datei für die bedarfsgesteuerte Suche hinzugefügt werden können, hängt von der Art der Suche und dem jeweiligen Ziel ab. Zum Beispiel könnte die Anzahl der Caches geringer sein, wenn der Security Agent bei der manuellen Suche nur 200 anstelle der 1.000 Dateien auf dem endpunkt durchsucht hat.

Wenn häufig bedarfsgesteuerte Suchen durchgeführt werden, reduziert die Cache-Datei für die bedarfsgesteuerte Suche den Suchzeitaufwand erheblich. Bei einer Aufgabe, bei der kein Cache abgelaufen ist, kann eine durchschnittliche Suchdauer von 12 Minuten auf 1 Minute reduziert werden. Reduziert man die Anzahl von Tagen, die eine Datei unverändert bleiben muss, und verlängert man die Ablaufzeit des Cache, erhöht sich normalerweise die Leistung. Da Dateien nur während einer relativ kurzen Zeitdauer unverändert bleiben müssen, können mehr Caches zur Cache-Datei hinzugefügt werden. Außerdem verlängert sich die Ablaufdauer der Caches, weshalb mehr Dateien von der Suche ausgeschlossen werden können.

Wenn nur selten bedarfsgesteuerte Suchen durchgeführt werden, können sie den Cache dafür deaktivieren, da die Caches ohnehin bis zur nächsten Suche abgelaufen sind.

POP3 Mail Scan

Wenn Security Agents die Mail Scan Berechtigungen haben, wird die **Mail Scan**-Option auf der Security Agent-Konsole angezeigt. Die **Mail Scan**-Option zeigt den POP3 Mail Scan.

In der folgenden Tabelle wird das POP3 Mail Scan-Programm beschrieben.

TABELLE 7-1. Mail Scan Programme

DETAILS	BESCHREIBUNG
Zweck	Durchsucht POP3 E-Mail-Nachrichten nach Viren/Malware
Voraussetzungen	• Müssen vom Administrator auf der Webkonsole aktiviert werden, bevor sie der Benutzer verwenden kann **Hinweis** Sie müssen die Berechtigung **Zeigen Sie die Mail Scan-Einstellungen in der Security Agent-Konsole an** aktivieren, um die POP3 Mail Scan zu ermöglichen. Weitere Informationen finden Sie unter *Agent-Berechtigungen konfigurieren auf Seite 7-3*. • Maßnahmen gegen Viren/Malware, die auf der Security Agent-Konsole, nicht aber auf der Webkonsole konfiguriert werden können
Unterstützte Suchtypen	Echtzeitsuche Eine Suche wird durchgeführt während E-Mail-Nachrichten vom POP3 Mail Server abgerufen werden.

Details	Beschreibung
Suchergebnis	• Informationen über entdeckte Sicherheitsrisiken liegen vor, sobald der Suchvorgang abgeschlossen ist • Suchergebnisse werden nicht im Fenster **Protokolle** der Security Agent-Konsole angezeigt • Suchergenisse werden nicht an den Server gesendet

Zusätzliche Diensteinstellungen

Für das Security Agent-Programm müssen zusätzliche Dienste aktiviert werden, damit bestimmte Funktionen ordnungsgemäß funktionieren. In der folgenden Tabelle sind die verfügbaren Dienste und die Funktionen, die für jeden Dienst erforderlich sind, beschrieben.

Dienst	Beschreibung	Funktionen
Unauthorized Change Prevention Service (`TMBMSRV.exe`)	Reguliert das Anwendungsverhalten und überprüft die Vertrauenswürdigkeit des Programms	• Vorausschauendes Maschinenlernen • Verhaltensüberwachung • Gerätesteuerung • Certified Safe Software Service • Eigenschutz des Agents
Firewall-Dienst (`TmPfw.exe`)	Reguliert die Zugriffsberechtigungen für die Netzwerkverbindung	• Apex One Firewall
Verdächtiger Verbindungsdienst	Bietet erweiterten Schutz vor C&C-Callbacks	• Benutzerdefinierte Listen mit zulässigen und gesperrten IP-Adressen • Globale C&C-IP-Liste (Prüf-Engine für Netzwerkinhalte) • Malware-Fingerabdruck für Netzwerk (Pattern der Relevanzregel)

Dienst	Beschreibung	Funktionen
Datenschutzdienst (`dsagent.exe`)	Bietet eine erweiterte Überwachung vertraulicher Daten und schränkt den Gerätezugriff auf den Endpunkten ein	• Prävention vor Datenverlust • Gerätesteuerung (Sperren des Zugriffs) • Datenentdeckung (verwaltet über die Trend Micro Apex Central-Konsole)
Erweiterter Schutzdienst (`TMCCSF.exe`))	Ermöglicht erweiterte Such- und Schutzfunktionen	• Vorausschauendes Maschinenlernen • Browser-Exploit-Schutz • Verhaltensüberwachung

Konfigurieren zusätzlicher Security Agent-Dienste

Prozedur

1. Wählen Sie, um den erforderlichen Dienst in den folgenden Abschnitten auf **Windows-Desktops** oder **Windows Server-Plattformen** zu aktivieren:
   - **Dienst zur Prävention unbefugter Änderungen**
   - **Firewall-Dienst**

     Wichtig

     Beim Aktivieren oder Deaktivieren des Diensts werden die Endpunkte vorübergehend vom Netzwerk getrennt. Ändern Sie die Einstellungen unbedingt nur außerhalb der Geschäftszeiten, um die Verbindungsunterbrechungen möglichst gering zu halten.
   - **Verdächtiger Verbindungsdienst**
   - **Datenschutzdienst**

Wichtig

Beim Aktivieren oder Deaktivieren des Diensts werden die Endpunkte vorübergehend vom Netzwerk getrennt. Ändern Sie die Einstellungen unbedingt nur außerhalb der Geschäftszeiten, um die Verbindungsunterbrechungen möglichst gering zu halten.

- **Erweiterter Schutzdienst**

Wichtig

Die Aktivierung zusätzlicher Dienste auf Windows Server-Plattformen kann die Serverleistung beeinträchtigen. Nach der Aktivierung eines Diensts auf einer Windows Server-Plattform empfiehlt Trend Micro, den Server eine Zeit lang zu überwachen, um sicherzustellen, dass keine Leistungsbeeinträchtigung auftritt.

Kapitel 8

Application Control-Richtlinieneinstellungen

In diesem Abschnitt wird beschrieben, wie die Application Control-Richtlinien für Security Agents konfiguriert werden.

Es werden folgende Themen behandelt:

- *Application Control auf Seite 8-2*

Application Control

Application Control bietet Ihnen die Möglichkeit, zu steuern, welche Benutzer Zugriff auf bestimmte Anwendungen auf bestimmten Endpunkten haben. Sie haben die Option, eine allgemeine Endpunkt-basierte Richtlinie zu erstellen oder, wenn sie mit Active Directory integriert ist, sehr granulare benutzerbasierte Richtlinien pro Endpunkt zu erstellen.

Nachdem Sie den Umfang der Richtlinie festgelegt haben, können Sie Anwendungsabgleichskriterien erstellen, die definieren, welche Anwendungen zugelassen, gesperrt oder überwacht werden sollen. Für erfahrene Benutzer können Sie „Lockdown"-Kriterien erstellen, die nur vertrauenswürdige Anwendungen ausführen lassen und alle Anwendungen sperren, die nicht ausdrücklich durch die Regeln zugelassen sind.

Konfigurieren der Einstellungen zur Anwendungssteuerung (Agent)

Bevor Sie eine Application Control-Richtlinie konfigurieren, stellen Sie sicher, dass Sie alle erforderlichen Application Control-Kriterien definieren. Application Control-Richtlinien erfordern die Verwendung vorkonfigurierter Kriterien, die festlegen, welche Anwendungen Sie auf einem Endpunkt oder für einen bestimmten Benutzer „Zulassen" oder „Sperren" möchten.

Weitere Informationen finden Sie unter *Application Control-Kriterien auf Seite 3-2*.

Prozedur

1. Wählen Sie **Application Control aktivieren**.
2. Weisen Sie im Abschnitt **Benutzerdefinierte Regeln** Regeln dem Endpunkt basierend auf dem angemeldeten Benutzerkonto zu.

Wichtig

- Benutzerbasierte Application Control ist nur verfügbar, wenn Sie Active Directory integriert haben. Wenn Sie keine Active Directory-Integration haben, können Sie Kriterien nur der Standardregel **Alle Benutzerkonten** zuweisen.
- Die standardmäßige **Alle Benutzerkonten** Regel kann nicht gelöscht werden.

a. Fügen Sie eine neue Regel hinzu oder ändern Sie eine bestehende Regel.

- Zum Hinzufügen einer neuen Regel klicken Sie auf **Regel zuweisen**.
- Um eine vorhandene Regel zu ändern, klicken Sie auf den Wert in der Spalte **Benutzerkonten** der Tabelle.

Das Fenster **Regel zuweisen** wird angezeigt.

b. Geben Sie das **Benutzerkonten** an, auf das Sie spezifische Application Control-Kriterien anwenden möchten.

Wichtig

- Benutzerbasierte Application Control ist nur verfügbar, wenn Sie Active Directory integriert haben. Wenn Sie keine Active Directory-Integration haben, können Sie Regeln nur der Standardregel **Alle Benutzerkonten** zuweisen.
- Sie können pro Regel nur 30 Benutzer oder Gruppen zuweisen. Erstellen Sie zusätzliche Regeln, wenn Sie eine größere Anzahl von Benutzern einer Richtlinie zuweisen müssen.

c. Verschieben Sie die erforderlichen Kriterien in die Tabelle **Ausgewählte Kriterien**, indem Sie auf die Kriterien **Name** klicken.

d. Klicken Sie auf **Save**.

Hinweis

Um die **Priorität**-Reihenfolge der Regeln zu ändern, wählen Sie die Regeln aus und ziehen Sie sie an verschiedene Positionen in der Liste. Application Control wendet eine Ersttrefferregel auf Benutzer an, die in mehreren Regeln enthalten sind.

3. Geben Sie im Abschnitt **Zusätzliche Aktionen** an, welche Aktion Application Control ausführt, wenn ein Benutzer versucht, eine Anwendung auszuführen, die keinem der **Benutzerdefinierte Regel**-Kriterien entspricht.

   - **Zulassen: Alle anderen Anwendungen können ausgeführt werden**: Application Control unternimmt keine Maßnahmen bei Anwendungen, die keinem der **Benutzerdefinierte Regel**-Kriterien entsprechen. Wählen Sie, wann Sie Application Control verwenden, um die Nutzung von Anwendungen zu sperren oder zu überwachen.
   - **Sperren: sperrt alle Anwendungen, die bei der letzten Bestandsdurchsuchung nicht identifiziert wurden**: Nachdem die Endpunkte diesen Befehl erhalten haben, führt Application Control die folgenden Aktionen aus:

     a. Die Application Control durchsucht den Endpunkt und erstellt einen vollständigen Anwendungsbestand.

     b. Application Control „sperrt“ den Endpunkt und erlaubt keinen Zugriff auf:

        - Jede Anwendung, die nicht speziell den **Zulassen**-Kriterien entspricht, die in der **Benutzerdefinierte Regel**-Tabelle definiert sind
        - Jede Anwendung, die nicht speziell den Bewertungsrichtlinien entspricht, die in der **Benutzerdefinierte Regel**-Tabelle definiert sind
        - Jede Anwendung, die in den Inventar-Durchsuchungsergebnissen für diesen bestimmten Endpunkt nicht gefunden wurde

- **Anwendungen von Trend Micro vertrauenswürdigen Anbietern ausschließen**: Auswählen, um alle Anwendungen, die von Trend Micro Bedrohungsexperten als von vertrauenswürdigen Anbietern bereitgestellt eingestuft wurden, automatisch zuzulassen
- **Bewertungsmodus aktivieren**: Wählen Sie, um den Zugriff auf Anwendungen zu protokollieren, die während des Lockdowns nicht ausdrücklich zur Ausführung zugelassen sind, aber die Anwendungen nicht zu sperren

Tipp

Verwenden Sie den Bewertungsmodus, um festzustellen, welche Anwendungen Benutzer benötigen könnten, bevor Sie den Zugriff auf alle Anwendungen sperren, die Sie nicht zu den Zulassungsregeln hinzugefügt haben.

4. Im Abschnitt **Agent-Benachrichtigungen** wählen Sie **Eine Benachrichtigung anzeigen, wenn eine Anwendung gesperrt wird**, um eine Benachrichtigung auf dem Endpunkt anzuzeigen, wenn Application Control eine Anwendung sperrt.
5. Im Abschnitt **Protokollwartung**:
   - **Maximales Log-Alter (in Tagen)**: Geben Sie die maximale Anzahl von Tagen an, die der Endpunkt Protokolldaten aufbewahren soll
   - **Maximale Anzahl von Protokollen, die ein Security Agent pro Stunde und Kriterium senden kann**: Geben Sie die maximale Anzahl von Protokollen an, die jeder Security Agent stündlich für jede Kriterienregel an den Apex One-Server senden kann

Hinweis

Je nach Anzahl der Security Agents und Ihren Netzwerkeinstellungen kann die Menge des Netzwerkverkehrs, die der Server empfängt, Leistungsprobleme verursachen.

Wichtig

Sie müssen daran denken, Ihre Apex One Security Agent-Richtlinie zu **Verteilen** oder zu **Speichern**, bevor Sie den Bildschirm verlassen. Wenn Sie die gesamte Richtlinie nicht speichern, gehen alle Änderungen verloren.

Kapitel 9

Einstellungen der Verhaltensüberwachungs-Richtlinie

In diesem Abschnitt wird beschrieben, wie Sie Richtlinien für die Verhaltensüberwachung in Security Agents konfigurieren.

Es werden folgende Themen behandelt:

- *Verhaltensüberwachung auf Seite 9-2*
- *Regeln und Ausnahmen der Verhaltensüberwachung konfigurieren auf Seite 9-17*

Verhaltensüberwachung

Die Verhaltensüberwachung überprüft regelmäßig Endpunkte auf ungewöhnliche Änderungen im Betriebssystem oder in installierter Software. Die Verhaltensüberwachung schützt Endpunkte durch **Sperrung bei Malware-Verhalten** und **Ereignisüberwachung**. Diese zwei Funktionen werden durch eine benutzerdefinierte **Ausschlussliste** und den **Certified Safe Software Service** ergänzt.

Wichtig

Die Verhaltensüberwachung ist in allen Versionen der Windows Server-Plattformen standardmäßig deaktiviert.

Verhaltensüberwachungsregeln

Konfigurieren Sie, wie die Verhaltensüberwachung auf die Richtlinie angewendet wird.

Wichtig

Die Verhaltensüberwachung ist in allen Versionen der Windows Server-Plattformen standardmäßig deaktiviert.

Bevor Sie die Verhaltensüberwachung konfigurieren, müssen Sie die Funktion aktivieren. Sobald sie aktiviert ist, konfigurieren Sie die folgenden Einstellungen.

Überwachungsstufe

Das Überwachungsniveau ist der Grad der Wachsamkeit und Strenge, der bei der Erkennung und Reaktion auf mögliche Bedrohungen angewendet wird. Eine Erhöhung des Niveaus steigert die Empfindlichkeit des Sensors, was die Anzahl der Erkennungen und Warnungen erhöht. Höhere Niveaus ermöglichen eine strengere Überwachung, um bei Situationen wie laufenden Bedrohungsuntersuchungen zu helfen, können jedoch eine große Anzahl nicht wesentlicher Protokolle erzeugen und die Leistung des Endpunkts beeinträchtigen. Trend Micro empfiehlt, das

Überwachungsniveau auf 2 - Mäßig einzustellen, um relevantere Daten mit minimalen Auswirkungen auf Ihre Endpunkte auszubalancieren. Einige Komponenten, die von höheren Überwachungsniveaus verwendet werden, sind nicht auf allen Plattformen verfügbar.

Sperrung bei Malware-Verhalten

Die Sperrung bei Malware-Verhalten bietet eine für zusätzlichen Schutz vor Bedrohungen durch Programme, die ein bösartiges Verhalten zeigen, erforderliche Schicht. Sie beobachtet über einen gewissen Zeitraum Systemereignisse. Während Programme verschiedene Kombinationen oder Folgen von Aktionen ausführen, erkennt die Sperrung bei Malware-Verhalten bekanntes bösartiges Verhalten und sperrt die entsprechenden Programme. Verwenden Sie diese Funktion, um einen besseren Schutz vor neuen, unbekannten und aufkommenden Bedrohungen zu gewährleisten.

Die Überwachung des Malware-Verhaltens bietet die folgenden Suchoptionen für Bedrohungsstufen:

- **Bekannte Bedrohungen**: Sperrt Verhaltensweisen im Zusammenhang mit bekannten Malware-Bedrohungen
- **Bekannte und potenzielle Bedrohungen**: Sperren von mit bekannten Bedrohungen verbundenem Verhalten und Ergreifen von Maßnahmen gegen potenziell bösartiges Verhalten

Nachdem das Sperren eines Programms mit Benachrichtigungen aktiviert wurde, zeigt der Security Agent eine Benachrichtigung auf dem Endpunkt an.

Schutz vor Ransomware

Ransomware-Schutz verhindert die unbefugte änderung oder Verschlüsselung von Dateien auf Agents durch „ransomware“-Bedrohungen. Ransomware ist eine Art von Malware, die den Zugriff auf Dateien beschränkt und verlangt, dass Sie für die Wiederherstellung der betroffenen Dateien bezahlen.

Apex One bietet die folgenden Methoden zum Schutz Ihrer Umgebung vor Ransomware-Bedrohungen.

Hinweis

Um zu vermeiden, dass der Security Agent einen sicheren Prozess als bösartig einstuft, stellen Sie sicher, dass der Agent Zugriff auf das Internet hat, damit weitere Verifizierungsprozesse unter Verwendung von Trend Micro Servern durchgeführt werden können.

Optionen	Beschreibung
Dokumente vor nicht autorisierter Verschlüsselung oder Veränderung schützen	Sie können Verhaltensüberwachung konfigurieren, um eine bestimmte Sequenz von Ereignissen zu erkennen, die möglicherweise auf einen Ransomware-Angriff hinweisen. Wenn die Verhaltensüberwachung alle der folgenden Kriterien erfüllt, beendet der Security Agent das böswillige Programm und versucht, es unter Quarantäne zu stellen. 1. Ein Prozess, der nicht als sicher erkannt wird, versucht, drei Dateien innerhalb eines bestimmten Zeitintervalls zu ändern, zu löschen oder umzubenennen. 2. Der Prozess hat versucht, eine Datei mit einer geschützten Erweiterung zu ändern Aktivieren Sie zusätzlich die Option **Automatically back up files changed by suspicious programs**, um Kopien von auf Endpunkten verschlüsselten Dateien zu erstellen. Wenn Apex One nach Abschluss der Verschlüsselung eine Ransomware-Bedrohung entdeckt, fordert Apex One Endbenutzer dazu auf, die betroffenen Dateien ohne Datenverlust wiederherzustellen. **Hinweis** Zur automatischen Dateisicherung werden mindestens 100 MB Festplattenspeicher auf dem Agent-Endpunkt benötigt und es werden nur Dateien gesichert, die kleiner als 10 MB sind. Der Speicherort des Sicherungsordners auf den Agent-Endpunkt befindet sich unter:<Installationsordner des Agents>\CCSF\module\DRE\data. **Warnung!** Wenn **Automatically back up files changed by suspicious programs** nicht aktiviert ist, kann Apex One die ersten von einer Ransomware-Bedrohung betroffenen Dateien nicht wiederherstellen.

Optionen	Beschreibung
Prozesse blockieren, die häufig mit Ransomware verknüpft sind	Vor dem Angriffsversuch auf Dateien werden häufig von Ransomware ausführbare Dateien an bestimmten Speicherorten auf Endpunkten verteilt. Durch das Sperren der Prozesse, die von diesen Speicherorten aus gestartet werden, kann verhindert werden, dass die Ransomware die Dateien angreifen kann.
Programmüberprüfung zum Erkennen und Sperren gefährdeter ausführbarer Dateien aktivieren	Die Programmüberprüfung überwacht Prozesse und führt API-Hooks aus, um festzustellen, ob sich ein Programm unerwartet verhält. Dieser Vorgang erhöht zwar den Gesamtanteil der erkannten gefährdeten ausführbaren Dateien, kann aber die Systemleistung verringern. **Tipp** Die Programmüberprüfung stellt erhöhte Sicherheit bereit, wenn Sie **Bekannte und potenzielle Bedrohungen** im Dropdown-Menü **Zu sperrende Bedrohungen** auswählen.

Schutz vor Schwachstellen

Schwachstellenschutz und Programmüberprüfung arbeiten zusammen, um das Verhalten von Programmen zu überwachen und ungewöhnliches Verhalten zu erkennen, das unter Umständen darauf hinweist, dass ein Angreifer eine Programmschwachstelle ausgenutzt hat. Wird solches Verhalten erkannt, beendet die Verhaltensüberwachung die Programmprozesse.

Wichtig

Für den Schwachstellenschutz muss die Option **Programmüberprüfung zum Erkennen und Sperren gefährdeter ausführbarer Dateien aktivieren** ausgewählt werden.

Schutz vor neu erkannten Programmen

Zusammen mit den Web-Reputation-Diensten und der Echtzeitsuche überprüft die Verhaltensüberwachung das bisherige Vorkommen von

Dateien, die über Internetkanäle, E-Mail-Anwendungen oder Microsoft Office-Makroskripts heruntergeladen wurden. Sobald eine "neu entdeckte" Datei erkannt wird können Administratoren eine Systemaufforderung an die Benutzer ausgeben, bevor sie die Datei ausführen. Trend Micro stuft ein Programm auf der Grundlage der Anzahl der Dateierkennungen oder des historischen Alters der Datei wie durch das Smart Protection Network als neu gefunden ein.

Die Verhaltensüberwachung überprüft für jeden Kanal die folgenden Dateitypen:

- Internet (HTTP/HTTPS): `.exe`-Dateien werden überprüft.
- E-Mail-Anwendungen: `.exe`-Dateien und komprimierte `.exe`-Dateien in unverschlüsselten `.zip`- und `.rar`-Dateien werden überprüft.

Hinweis

- Bevor diese Eingabeaufforderung angezeigt werden kann, müssen Administratoren die Web-Reputation-Dienste auf dem Agent aktivieren, damit der Security Agent HTTP- oder HTTPS-Datenverkehr durchsuchen kann.
- Der Security Agent führt einen Abgleich mit den Dateinamen durch, die während des Ausführungsvorgangs über E-Mail-Anwendungen heruntergeladen wurden. Wenn der Dateiname geändert wurde, erhält der Benutzer eine Eingabeaufforderung.

Ereignisüberwachung

Die Ereignisüberwachung bietet einen generischeren Ansatz zum Schutz vor nicht autorisierter Software und Malware-Angriffen. Sie überwacht Systembereiche auf bestimmte Ereignisse. Dies gibt Administratoren die Möglichkeit, Programme zu regulieren, die derartige Ereignisse auslösen. Verwenden Sie die Systemüberwachung, wenn Sie über den durch Sperrung bei Malware-Verhalten gebotenen Schutz hinaus spezielle Schutzanforderungen für das System benötigen.

Die folgende Tabelle enthält eine Liste der überwachten Systemereignisse.

TABELLE 9-1. Überwachte Systemereignisse

EREIGNISSE	BESCHREIBUNG
KI-App-Guard	Konfigurieren Sie diese Richtlinie so, dass KI-integrierte Anwendungen und zugehörige Dateien vor bösartigen Änderungen geschützt sind. **Hinweis** Eine Liste der Anwendungen, die der KI-App-Guard unterstützt, finden Sie im Wissensdatenbank-Artikel.
Duplizierte Systemdatei	Viele bösartige Programme erstellen Kopien von sich selbst oder anderen bösartigen Programmen unter Verwendung von Dateinamen, die von Windows Systemdateien verwendet werden. Dies geschieht in der Regel, um Systemdateien zu überschreiben oder zu ersetzen, sich zu verbergen oder zu verhindern, dass Benutzer die bösartigen Dateien löschen.
Änderung der Hosts-Datei	Die Hosts-Datei ordnet Domain-Namen IP-Adressen zu. Zahlreiche bösartige Programme verändern die Hosts-Datei so, dass der Webbrowser zu infizierten, nicht existierenden oder falschen Websites umgeleitet wird.
Verdächtiges Verhalten	Verdächtiges Verhalten kann sich in einer bestimmten Aktion oder einer Reihe von Aktionen zeigen, die normalerweise nicht von rechtmäßigen Programmen durchgeführt werden. Programme, die verdächtiges Verhalten aufweisen, sollten mit Vorsicht verwendet werden.
Neues Plug-in für den Internet Explorer	Spyware-/Grayware-Programme installieren oft unerwünschte Plug-ins für den Internet Explorer, wie z. B. Symbolleisten und Browser Helper Objects.
Änderungen an Einstellungen des Internet Explorers	Malware-Programme können die Einstellungen im Internet Explorer ändern, einschließlich Startseite, vertrauenswürdiger Websites, Proxy-Servereinstellungen und Menüerweiterungen.
Änderungen der Sicherheitsrichtlinien	Durch Änderungen der Sicherheitsrichtlinien können unerwünschte Anwendungen ausgeführt und Systemeinstellungen verändert werden.

Ereignisse	Beschreibung
Injektion einer Programmbibliothek	Viele bösartige Programme konfigurieren Windows so, dass alle Anwendungen automatisch eine Programmbibliothek (DLL) laden. Dadurch können bösartige Routinen in der DLL bei jedem Start einer Anwendung ausgeführt werden.
Shell-Änderungen	Viele bösartige Programme verändern die Einstellungen der Windows Shell, um sich selbst mit bestimmten Dateitypen zu verknüpfen. Durch diese Routine können bösartige Programme automatisch gestartet werden, wenn Benutzer die verknüpften Dateien im Windows Explorer öffnen. Durch Änderungen in der Windows Shell können bösartige Programme außerdem die verwendeten Programme nachverfolgen und wie rechtmäßige Programme gestartet werden.
Neuer Dienst	Windows Dienste sind Prozesse mit speziellen Funktionen. Sie werden in der Regel dauerhaft und mit vollständigen Administratorberechtigungen im Hintergrund ausgeführt. Bösartige Programme installieren sich in manchen Fällen als versteckte Dienste selbst.
Änderung von Systemdateien	Bestimmte Windows Systemdateien legen das Systemverhalten, einschließlich der Autostart-Programme und der Bildschirmschonereinstellungen, fest. Viele bösartige Programme verändern Systemdateien so, dass sie beim Start automatisch ausgeführt werden und das Systemverhalten steuern.
Änderungen der Firewall-Richtlinien	Die Windows Firewall-Richtlinie legt die Anwendungen fest, die auf das Netzwerk zugreifen können, die Ports, die für die Kommunikation geöffnet sind und die IP-Adressen, die mit dem Computer kommunizieren können. Viele bösartige Programme verändern die Richtlinie, um sich den Zugriff auf das Netzwerk und das Internet zu ermöglichen.
Änderungen an Systemprozessen	Viele bösartige Programme führen verschiedene Aktionen an integrierten Windows Prozessen durch. So beenden oder ändern sie beispielsweise aktive Prozesse.
Neues Autostart-Programm	Bösartige Anwendungen fügen der Windows-Registrierung gewöhnlich Autostart-Einträge hinzu oder ändern diese, so dass sie bei jedem Hochfahren des Computers automatisch gestartet werden.

Wenn von der Ereignisüberwachung ein überwachtes Systemereignis erkannt wird, wird die für dieses Ereignis konfigurierte Aktion ausgeführt.

Die folgende Tabelle enthält eine Liste der möglichen Aktionen, die Administratoren bei überwachten Systemereignissen ergreifen können.

TABELLE 9-2. Aktionen bei überwachten Systemereignissen

AKTION	BESCHREIBUNG
Bewerten	Der Security Agent lässt die Ausführung von Programmen, die einem Ereignis zugeordnet sind, immer zu und protokolliert das Ereignis zwecks Bewertung. Dies ist die Standardaktion für alle überwachten Systemereignisse. **Hinweis** Diese Option wird für das Ereignis 'Einschleusung in Programmbibliothek' (DLL-Injektion) auf 64-Bit-Systemen nicht unterstützt.
Zulassen	Der Security Agent lässt die Ausführungen von Programmen, die einem Ereignis zugeordnet sind, immer zu.
Bei Bedarf nachfragen	Der Security Agent fordert Benutzer auf, die Ausführung von Programmen, die einem Ereignis zugeordnet sind, zuzulassen oder abzulehnen und fügt die Programme in der Ausnahmeliste hinzu. Wenn der Benutzer nicht innerhalb eines bestimmten Zeitraums reagiert, lässt der Security Agent die Ausführung des Programms automatisch zu. Der Standardzeitraum beträgt 30 Sekunden. **Hinweis** Diese Option wird für das Ereignis 'Einschleusung in Programmbibliothek' (DLL-Injektion) auf 64-Bit-Systemen nicht unterstützt.
Verweigern	Der Security Agent sperrt stets die Ausführung von Programmen, die einem Ereignis zugeordnet sind, und protokolliert das Ereignis. Nachdem das Sperren eines Programms mit Benachrichtigungen aktiviert wurde, zeigt der Security Agent eine Benachrichtigung auf dem Endpunkt an.

Ausnahmeliste für Verhaltensüberwachung

Die Ausnahmeliste für Verhaltensüberwachung enthält Programme, die von Security Agent nicht mit Verhaltensüberwachung überwacht werden.

- **Zulässige Programme**: Der Security Agent gestattet allen Programmen in der Liste der zulässigen Programme, die Verhaltensüberwachung zu übergehen.

  Hinweis

  Obwohl die Verhaltensüberwachung für Programme, die der Liste der zulässigen Programme hinzugefügt wurden, keine Maßnahmen ergreift, werden die Programme weiterhin mit anderen Suchfunktionen (beispielsweise dateibasierte Suche) durchsucht, bevor die Ausführung der Programme zugelassen wird.

- **Gesperrte Programme**: Der Security Agent sperrt alle Programme in der Liste der gesperrten Programme. Zum Konfigurieren der Liste der gesperrten Programme aktivieren Sie die Ereignisüberwachung.

Sie können die Ausschlussliste über die Webkonsole konfigurieren. Sie können Benutzern auch die Berechtigung zum Konfigurieren einer eigenen Ausnahmeliste über die Security Agent-Konsole gewähren.

Weitere Informationen finden Sie unter *Agent-Berechtigungen konfigurieren auf Seite 7-3*.

Ausnahmeliste, Unterstützung von Platzhaltern

Die zulässige Liste der Verhaltensüberwachung unterstützt Platzhalterzeichen beim Definieren von Ausnahmetypen für den Dateipfad, den Dateinamen und die Dateierweiterung. Verwenden Sie die folgende Tabelle für eine ordnungsgemäße Formatierung Ihrer Ausnahmelisten, um sicherzustellen, dass Apex One die korrekten Dateien und Ordner von der Suche ausschließt.

Unterstützte Platzhalterzeichen:

- Sternchen (*): Steht für ein beliebiges Zeichen oder eine Zeichenfolge.

- Fragezeichen (?): Steht für ein einzelnes Zeichen

Wichtig

- Die zulässige Liste der Verhaltensüberwachung unterstützt die Verwendung von Platzhalterzeichen zum Ersetzen von Systemlaufwerksbezeichnungen oder UNC-Adressen nicht.
- Die Sperrliste der Verhaltensüberwachung unterstützt die Verwendung von Platzhalterzeichen zum Ersetzen von Ordnern nicht.

Typ der Ausnahme	Verwendung von Platzhalterzeichen	Stimmt überein	Stimmt nicht überein
Verzeichnisse	`C:\*` Schließt alle Dateien und Ordner im angegebenen Laufwerk aus.	• `C:\sample.exe` • `C:\Ordner\test.doc`	• `D:\sample.exe` • `E:\Ordner\test.doc`
Bestimmte Dateien unter einer bestimmten Ordnerebene	`C:\*\Sample.exe` Schließt die Datei `Sample.exe` nur dann aus, wenn sich die Datei in einem Unterordner des Verzeichnisses `C:\` befindet.	• `C:\Dateien\Sample.exe` • `C:\temp\Dateien\Sample.exe`	• `C:\sample.exe`

Typ der Ausnahme	Verwendung von Platzhalterzeichen	Stimmt überein	Stimmt nicht überein
UNC-Pfade	`\\<UNC-Pfad>\*\Sample.exe` Schließt die Datei `Sample.exe` nur dann aus, wenn sich die Datei in einem Unterordner des angegebenen UNC-Pfads befindet.	• `\\<UNC-Pfad\Dateien\Sample.exe` • `\\<UNC-Pfad>\temp\Dateien\Sample.exe`	• `R:\Dateien\Sample.exe` Grund: Zugeordnete Laufwerke werden nicht unterstützt. • `\\<UNC-Pfad>\Sample.exe` Grund: Die Datei ist nicht in einem Unterordner des UNC-Pfads vorhanden.
Dateinamen und Erweiterungen	`C:\*.*` Schließt alle Dateien mit Erweiterungen in allen Ordnern und Unterordnern des Verzeichnisses `C:\` aus.	• `C:\Sample.exe` • `C:\temp\Sample.exe` • `C:\test.doc`	• `D:\sample.exe` • `C:\Sample` **Hinweis** `C:\Sample` hat keine Dateierweiterung und wird daher nicht aus der Suche ausgeschlossen.

Typ der Ausnahme	Verwendung von Platzhalterzeichen	Stimmt überein	Stimmt nicht überein
Dateiname	`C:\*.exe` Schließt alle Dateien mit der Erweiterung `.exe` in allen Ordnern und Unterordnern des Verzeichnisses `C:\` aus.	• `C:\Sample.exe` • `C:\temp\test.exe`	• `C:\Sample.doc` • `C:\temp\test.bat` • `C:\Sample` **Hinweis** `C:\Sample` hat keine Dateierweiterung und wird daher nicht aus der Suche ausgeschlossen.

Typ der Ausnahme	Verwendung von Platzhalterzeichen	Stimmt überein	Stimmt nicht überein
Dateierweiterungen	`C:\Sample.*` Schließt alle Dateien mit dem Namen `Sample` und einer beliebigen Erweiterung im Verzeichnis `C:\`.	• `C:\Sample.exe`	• `C:\Sample1.doc` • `C:\temp\Sample.bat` • `C:\Sample` **Hinweis** `C:\Sample` hat keine Dateierweiterung und wird daher nicht aus der Suche ausgeschlossen.
Dateien in bestimmten Verzeichnisstrukturen	`C:\*\*\Sample.exe` Schließt alle Dateien in der zweiten Unterordnerebene oder beliebigen nachfolgenden Unterordnern des Verzeichnisses `C:\` aus, die den Namen und die Erweiterung `Sample.exe` haben.	• `C:\Dateien\temp\Sample.exe` • `C:\Dateien\temp\test\Sample.exe`	• `C:\Sample.exe` • `C:\temp\Sample.exe` • `C:\Dateien\temp\Sample.doc`

Typ der Ausnahme	Verwendung von Platzhalterzeichen	Stimmt überein	Stimmt nicht überein
Komplexe Pfade oder Dateinamen	`C:\Sam*e??.exe` Schließt alle Dateien aus, deren Namen die folgenden Bedingungen erfüllen: • Sie beginnen mit den Zeichen 'Sam'. • Das drittletzte Zeichen der Datei muss ein 'e' sein. • Zwischen der Zeichenfolge 'Sam' am Anfang und 'e??' am Ende des Dateinamens muss mindestens 1 Zeichen vorhanden sein. • Vor der Dateierweiterung und nach dem 'e' im Dateinamen sind genau 2 Zeichen vorhanden. • Die Dateierweiterung ist `.exe`. Wenn eine Datei alle erforderlichen Bedingungen erfüllt und sich im Verzeichnis `C:\` befindet, schließt die Verhaltensüberwachung die Datei von der Suche aus.	• `C:\Sample12.exe` • `C:\SamSamSample12.exe`	• `C:\SaSmple12.exe` Grund: Beginnt nicht mit 'Sam'. • `C:\SamSamSam12.exe` Grund: Enthält nicht das Zeichen 'e' als drittletztes Zeichen. • `C:\Same12.exe` Grund: Enthält keine Zeichen zwischen der beginnenden Zeichenfolge 'Sam' und dem drittletzten Zeichen 'e'. • `C:\Sample1.exe` Grund: Enthält keine 2 Zeichen vor der Erweiterung und nach dem 'e'. • `C:\Sample12.doc` Grund: Falsche Erweiterung

Ausnahmeliste, Unterstützung von Umgebungsvariablen

Die folgende Tabelle listet die Umgebungsvariablen auf, die Sie verwenden können, wenn Sie einen Datei- oder Ordnerpfad zur Liste hinzufügen.

Umgebungsvariable	Beispiel	Entsprechender Pfad
$allappdata$	$allappdata$\test\sample.exe	C:\ProgramData\test\sample.exe
$allprograms$	$allprograms$\test\sample.exe	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\test\sample.exe
$programdir$	$programdir$\test\sample.exe	C:\Programme\test\sample.exe
$programdirx86$	$programdirx86$\test\sample.exe	C:\Programme (x86)\test\sample.exe
$rootdir$	$rootdir$\test\sample.exe	C:\test\sample.exe
$systemdir$	$systemdir$\test\sample.exe	C:\Windows\System32\test\sample.exe
$systemdirx86$	$systemdirx86$\test\sample.exe	C:\Windows\SysWOW64\test\sample.exe
$tempdir$	$tempdir$\test\sample.exe	C:\Windows\Temp\test\sample.exe
$userprofile$	$userprofile$\test\sample.exe	C:\user\{current_user_account}\test\sample.exe
$windir$	$windir$\test\sample.exe	C:\Windows\test\sample.exe

Regeln und Ausnahmen der Verhaltensüberwachung konfigurieren

Konfigurieren Sie Richtlinien zur Verhaltensüberwachung, um Endpunkte vor Ransomware, Angriffen auf Schwachstellen und aufkommenden Bedrohungen zu schützen. Mit der Funktion Ereignisüberwachung können Verhaltensweisen im Zusammenhang mit Malware-Bedrohungen bewertet und blockiert werden.

Hinweis

Die Verhaltensüberwachung ist in allen Versionen der Windows Server-Plattformen standardmäßig deaktiviert.

Prozedur

1. Klicken Sie auf die Registerkarte **Regeln**.
2. Wählen Sie **Verhaltensüberwachung aktivieren**.
3. Konfigurieren Sie die **Überwachungsstufe**-Einstellungen für **Erkennung** und **Prävention**.

   Wichtig

   - Höhere Überwachungsstufen bieten eine größere Sensibilität, können jedoch eine große Anzahl nicht wesentlicher Protokolle erzeugen und die Leistung des Endpunkts beeinträchtigen. Trend Micro empfiehlt, **2 - Mäßig** auszuwählen, um relevantere Daten mit minimalen Auswirkungen auf Ihre Endpunkte zu erhalten.
   - Die **Prävention**-Stufe muss gleich oder niedriger als **Erkennung** sein.
   - Die Auswahl von **Bedrohungen zum Sperren** kann die Präventionsmaßnahmen für das ausgewählte Präventionsniveau beeinflussen.

4. Wählen Sie aus, welche **Bedrohungen zum Sperren**.
   - **Bekannte Bedrohungen**: Hiermit wird mit bekannten Bedrohungen verbundenes Malware-Verhalten blockiert.
   - **Bekannte und potenzielle Bedrohungen**: Hiermit wird mit bekannten Bedrohungen verbundenes Verhalten blockiert und es werden entsprechende Maßnahmen gegen potenziell bösartiges Verhalten ergriffen.
5. Wählen Sie aus, welche Ransomware-Schutzfunktionen aktiviert werden sollen, um Dokumente vor Ransomware-Bedrohungen zu schützen.

- **Dokumente vor nicht autorisierter Verschlüsselung oder Veränderung schützen**: Beendet potentielle Ransomware-Bedrohungen, sodass sie Inhalte von Dokumenten nicht verschlüsseln oder verändern können.

  - **Die durch verdächtige Programme geänderten Dateien automatisch sichern und wiederherstellen**: Erstellt zur Vermeidung von Datenverlust Sicherungskopien von auf Endpoints verschlüsselten Dateien, nachdem eine Bedrohung durch Ransomware erkannt wurde.

Hinweis

Zur automatischen Dateisicherung werden mindestens 100 MB Festplattenspeicher auf dem Agent-Endpunkt benötigt und es werden nur Dateien gesichert, die kleiner als 10 MB sind.

- **Prozesse sperren, die häufig mit Ransomware verknüpft sind**: Sperrt Prozesse, die mit bekannten Ransomware-Bedrohungen verknüpft sind, bevor eine Verschlüsselung oder Veränderung von Dokumenten auftreten kann.

- **Programmüberprüfung zum Erkennen und Sperren gefährdeter ausführbarer Dateien aktivieren**: Die Programmüberprüfung überprüft Prozesse und führt API-Hooking durch, um festzustellen, ob ein Programm unerwartetes Verhalten zeigt. Dieses Verfahren erhöht zwar den Gesamterkennungsgrad gefährdeter ausführbarer Dateien, setzt aber möglicherweise die Systemleistung herab.

Hinweis

Die Programmüberprüfung stellt erhöhte Sicherheit bereit, wenn Sie **Bekannte und potenzielle Bedrohungen** im Dropdown-Menü **Zu sperrende Bedrohungen** auswählen.

6. Aktivieren Sie unter **Schutz vor Schwachstellen** die Option **Programme beenden, die ungewöhnliches Verhalten im Zusammenhang mit Angriffen auf Schwachstellen zeigen**, um Schutz vor Programmen mit Sicherheitslücken bereitzustellen.

Wichtig

Schutz vor Schwachstellen erfordert, dass Sie **Programmüberprüfung zum Erkennen und Sperren gefährdeter ausführbarer Dateien aktivieren** auswählen. Für weitere Informationen siehe *Schutz vor Schwachstellen auf Seite 9-6*.

Der Schutz vor Schwachstellen arbeitet zusammen mit der Echtzeitsuche (**Verschiedene Varianten von Malware in Speicher entdeckt**), um einen verbesserten Schutz vor dateilosen Angriffen zu bieten. Weitere Informationen finden Sie unter *Echtzeitsuche: Registerkarte "Ziel" auf Seite 10-6*.

7. Gehen Sie im Abschnitt **Ereignisüberwachung** wie folgt vor:

   a. Wählen Sie **Ereignisüberwachung aktivieren**.

   b. Klicken Sie auf **Detaillierte Einstellungen angeben**, um die Arten der zu überwachenden Ereignisse auszuwählen.

   c. Wählen Sie die zu überwachenden Systemereignisse und wählen Sie eine Aktion für die einzelnen ausgewählten Ereignisse.

      Weitere Informationen zu überwachten Systemereignissen und Aktionen finden Sie unter *Ereignisüberwachung auf Seite 9-7*.

8. Klicken Sie auf die Registerkarte **Ausnahmen**, um die Ausnahmelisten zu konfigurieren.

   a. Geben Sie bei der Konfiguration einer übergeordneten Richtlinie an, wie andere Benutzer untergeordnete Richtlinien konfigurieren können.

      - **Von übergeordnetem Element erben**: Untergeordnete Richtlinien müssen die Einstellungen verwenden, die in der übergeordneten Richtlinie konfiguriert wurden
      - **Von übergeordnetem Element erweitern**: Untergeordnete Richtlinien können zusätzliche Einstellungen an die Einstellungen anhängen, die von der übergeordneten Richtlinie vererbt wurden

Hinweis

Wenn Ihre Kinderrichtlinien **Von übergeordnetem Element erweitern** sind, können Sie **Einschränkungen der Kinderpolitik** konfigurieren, um zu verhindern, dass Kinderrichtlinien bestimmte Regeln zur Liste der Ausnahmeregeln hinzufügen.

b. Geben Sie den vollständigen Programmpfad in das verfügbare Textfeld ein.

Hinweis

- Trennen Sie mehrere Einträge durch Strichpunkte (;) voneinander.
- Verwenden Sie die Schaltflächen **Importieren** und **Exportieren**, um die Liste mit verschiedenen Richtlinien zu teilen.
- Der **Zulässige Liste** unterstützt die Verwendung von Platzhalterzeichen.

  Weitere Informationen finden Sie unter *Ausnahmeliste, Unterstützung von Platzhaltern auf Seite 9-11*.

c. Klicken Sie auf **Hinzufügen**.

d. Um ein gesperrtes oder zugelassenes Programm aus der Liste zu entfernen, klicken Sie neben dem Programm auf das Papierkorbsymbol).

Hinweis

In Apex One sind insgesamt maximal 1.024 zugelassene Programme und gesperrte Programme möglich.

Kapitel 10

Anti-Malware-Scans

In diesem Abschnitt wird beschrieben, wie die Anti-Malware-Suche in Security Agents konfiguriert wird.

Es werden folgende Themen behandelt:

- *Allgemeine Einstellungen auf Seite 10-2*
- *Manuelle Suche auf Seite 10-32*
- *Echtzeitsuche auf Seite 10-5*
- *Jetzt durchsuchen auf Seite 10-43*
- *Zeitgesteuerte Suche auf Seite 10-18*
- *Suchaktionen auf Seite 10-54*
- *Unterstützung der Suchausschlüsse auf Seite 10-63*

Allgemeine Einstellungen

Der Bildschirm für Allgemeine Einstellungen ist der Ort, an dem Sie **Suchmethoden** und **Überwachungsstufe** konfigurieren können.

Bei der Suche nach Sicherheitsrisiken können Security Agents eine von zwei Suchmethoden anwenden: Die Suchmethoden sind intelligente Suche und herkömmliche Suche.

- **Intelligente Suche**

  Security Agents, die die intelligente Suche anwenden, werden in diesem Dokument als **Agents mit intelligenter Suche** bezeichnet. Smart Scan Agents nutzen die lokale Suche und webbasierte Abfragen, die von File-Reputation-Diensten bereitgestellt werden.

- **Herkömmliche Suche**

  Agents, die keine intelligente Suche durchführen, werden als **Agents der herkömmlichen Suche** bezeichnet. Ein Agent der herkömmlichen Suche speichert alle Security Agent-Komponenten auf dem Endpunkt und durchsucht alle Dateien lokal.

Bevor Sie die Suchmethoden ändern, überprüfen Sie *Richtlinien für das Wechseln der Suchmethoden auf Seite 10-3*.

Wichtig

Um die maximale Sicherheitsfähigkeit zu gewährleisten, aktivieren Sie die Funktionen Anti-Malware, Verhaltensüberwachung, Vorausschauendes Maschinenlernen und Verdächtige Verbindung.

Das Überwachungsniveau ist der Grad der Wachsamkeit und Strenge, der bei der Erkennung und Reaktion auf mögliche Bedrohungen angewendet wird. Eine Erhöhung des Niveaus steigert die Empfindlichkeit des Sensors, was die Anzahl der Erkennungen und Warnungen erhöht. Höhere Niveaus ermöglichen eine strengere Überwachung, um bei Situationen wie laufenden Bedrohungsuntersuchungen zu helfen, können jedoch eine große Anzahl nicht wesentlicher Protokolle erzeugen und die Leistung des Endpunkts beeinträchtigen. Trend Micro empfiehlt, das

Überwachungsniveau auf 2 - Moderat einzustellen, um relevantere Daten mit minimaler Auswirkung auf Ihre Endpunkte auszugleichen. Einige Komponenten, die von höheren Überwachungsniveaus verwendet werden, sind nicht auf allen Plattformen verfügbar.

Richtlinien für das Wechseln der Suchmethoden

Die folgende Tabelle enthält einige Überlegungen, die Sie beachten sollten, bevor Sie die Suchmethode ändern, die Security Agents verwendet.

Tabelle 10-1. Überlegungen bei der Umstellung auf die intelligente Suche

Überlegung	Details
Produktlizenz	Stellen Sie sicher, dass alle erforderliche Lizenzen für die neue Suchmethode aktiviert wurden.
Apex One Server	Stellen Sie sicher, dass die Agents eine Verbindung zum Apex One Server herstellen können. Apex One benachrichtigt nur Online-Agents über den Wechsel der Suchmethode. Offline-Agents erhalten die Benachrichtigung erst dann, wenn sie wieder online gehen. Unabhängige Agents werden benachrichtigt, wenn sie wieder online sind oder wenn zeitgesteuerte Updates ausgeführt werden (wenn der Agent Berechtigungen für zeitgesteuerte Updates aufweist). Überprüfen Sie außerdem, ob der Apex One Server über die neuesten Komponenten verfügt, um sicherzustellen, dass Security Agents die richtigen Patterns vom Server herunterladen können.
Anzahl der umzuschaltenden Security Agents	Wenn Sie eine relativ kleine Anzahl von Security Agents gleichzeitig umschalten, werden die Ressourcen von Apex One Server und Smart Protection Server effizient genutzt. Diese Server können andere wichtige Aufgaben ausführen, während Security Agents die Suchmethoden ändern.

Überlegung	Details
Timing	Wenn Suchmethoden geändert werden, müssen Security Agents die Vollversionen der erforderlichen Pattern-Dateien für die neue Suchmethode herunterladen. Der Wechsel sollte außerhalb der Spitzenzeiten erfolgen, um die Auswirkungen auf die Bandbreite und die Unterbrechung der täglichen Aufgaben der Endbenutzer möglichst gering zu halten. Trend Micro empfiehlt, während des Konvertierungsvorgangs die Option "Jetzt aktualisieren" in Security Agents zu deaktivieren.
IPv6-Unterstützung **Wichtig** Nur verfügbar für Security Agents, die an einen lokalen Apex One Server berichten.	Die Agents der intelligenten Suche senden Suchabfragen an Smart Protection Quellen. Ein reiner IPv6-Agent der intelligenten Suche kann Abfragen nicht direkt an IPv4-Quellen senden wie zum Beispiel: • Smart Protection Server 2.0 (integriert oder standalone) **Hinweis** IPv6-Unterstützung für Smart Protection Server ist ab Version 2.5 verfügbar. • Trend Micro Smart Protection Network Entsprechend kann ein reiner IPv4-Agent der intelligenten Suche ebenfalls keine Abfragen an reine IPv6 Smart Protection Server senden. Ein Dual-Stack-Proxy-Server wie beispielsweise DeleGate, der IP-Adressen konvertieren kann, muss ermöglichen, dass Agents der intelligenten Suche eine Verbindung zu den Quellen herstellen können.

Überlegung	Details
Smart Protection Services **Wichtig** Nur verfügbar für Security Agents, die an einen lokalen Apex One Server berichten.	Wenn Sie Security Agents von der herkömmlichen Suche auf die intelligente Suche umstellen, sollte Smart Protection-Dienste eingerichtet sein.

Echtzeitsuche

Die Echtzeitsuche wird kontinuierlich und dauerhaft ausgeführt. Bei jedem Empfang, Öffnen, Herunterladen, Kopieren oder Ändern einer Datei wird diese durch die Echtzeitsuche durchsucht. Wenn der Security Agent kein Sicherheitsrisiko erkennt, können Benutzer mit dem Zugriff auf die Datei fortfahren. Wenn der Security Agent ein Sicherheitsrisiko oder eine mögliche Viren-/Malware-Infektion erkennt, wird eine Benachrichtigung mit dem Namen der infizierten Datei und des speziellen Sicherheitsrisikos angezeigt.

Die Echtzeitsuche verwaltet einen permanenten Zwischenspeicher für die Suche, der bei jedem Start des Security Agent neu geladen wird. Der Security Agent verfolgt Änderungen an Dateien oder Ordnern nach, die seit dem Beenden des Security Agents erfolgt sind, und entfernt diese Dateien aus dem Zwischenspeicher.

Einstellungen der Echtzeitsuche konfigurieren

Prozedur

1. Wählen Sie die folgenden Optionen:
   - **Suche nach Virus/Malware aktivieren**

- **Suche nach Spyware/Grayware aktivieren**

Hinweis

Bevor Sie nach Spyware/Grayware suchen können, müssen Sie die Viren-/Malware-Suche aktivieren. Während eines Virenausbruchs aktiviert der Security Agent automatisch die Echtzeitsuche.
Sie können die Suche erst nach Ende des Ausbruchs wieder deaktivieren. Die Echtzeitsuche hilft, den Virus daran zu hindern, Dateien und Ordner auf Endpunkten zu ändern oder zu löschen.

2. Konfigurieren Sie die Einstellungen für **Ziel**.

   Weitere Informationen finden Sie unter *Echtzeitsuche: Registerkarte "Ziel" auf Seite 10-6*.

3. Konfigurieren Sie die Einstellungen für **Aktion**.

   Weitere Informationen finden Sie unter *Echtzeitsuche: Registerkarte "Aktion" auf Seite 10-11*.

4. Konfigurieren Sie die Einstellungen für **Suchausschluss**.

   Weitere Informationen finden Sie unter *Echtzeitsuche: Registerkarte "Suchausschluss" auf Seite 10-15*.

Echtzeitsuche: Registerkarte "Ziel"

Prozedur

1. Wählen Sie im Abschnitt **Benutzerdefinierte Aktionen für Dateien** im Listenfeld **Diese Dateien durchsuchen** aus, welche Dateivorgänge die Suche auslösen.

   - **erstellt/bearbeitet und gelesen**: Durchsucht alle Dateien, die auf dem Endpunkt erstellt, geändert oder geöffnet wurden
   - **erstellt/bearbeitet**: Durchsucht alle Dateien, die auf dem Endpunkt erstellt oder geändert wurden

- **abgerufen**: Durchsucht alle Dateien, die auf dem Endpunkt geöffnet wurden

2. Wählen Sie im Abschnitt **Zu durchsuchende Dateien** eine der folgenden Optionen aus:

   - **Alle durchsuchbaren Dateien**: Alle durchsuchbaren Dateien werden berücksichtigt. Zu den nicht durchsuchbaren Dateien gehören kennwortgeschützte und verschlüsselte Dateien sowie Dateien, die die vom Benutzer festgelegten Suchkriterien nicht erfüllen.

     Hinweis

     Diese Option bietet die höchstmögliche Sicherheit. Das Durchsuchen jeder Datei erfordert allerdings viel Zeit und viele Ressourcen und ist möglicherweise in manchen Fällen gar nicht notwendig. Deshalb können Sie bei Bedarf die Anzahl der durchsuchten Dateien begrenzen.

   - **Von IntelliScan durchsuchte Dateitypen**: Durchsucht Dateien auf Grundlage des ursprünglichen Dateityps.
   - **Dateien mit den folgenden Erweiterungen (mehrere Einträge mit Komma voneinander trennen)**: Legen Sie manuell fest, welche Dateien anhand der Dateierweiterung durchsucht werden sollen. Trennen Sie mehrere Einträge mit Kommas.

Hinweis

Geben Sie bei der Konfiguration einer übergeordneten Richtlinie an, wie andere Benutzer untergeordnete Richtlinien konfigurieren können.

- **Von übergeordnetem Element erben**: Untergeordnete Richtlinien müssen die Einstellungen verwenden, die in der übergeordneten Richtlinie konfiguriert wurden
- **Von übergeordnetem Element erweitern**: Untergeordnete Richtlinien können zusätzliche Einstellungen an die Einstellungen anhängen, die von der übergeordneten Richtlinie vererbt wurden

3. Konfigurieren Sie im Abschnitt **Sucheinstellungen** die erforderlichen Einstellungen.

Einstellung	Beschreibung
Diskettenlaufwerke beim Herunterfahren durchsuchen	Durchsucht Diskettenlaufwerke beim Herunterfahren.
Bootsektor des USB-Speichergeräts nach dem Anschließen durchsuchen	Durchsucht jedes Mal, wenn ein USB-Speichergerät angeschlossen wird, automatisch den Bootsektor des Geräts.
Alle Dateien auf Wechsellaufwerken nach dem Anschließen durchsuchen	Durchsucht jedes Mal, wenn ein USB-Speichergerät angeschlossen wird, automatisch alle Dateien auf dem Gerät.

Einstellung	Beschreibung
Verschiedene Varianten von Malware in Speicher entdeckt	Verhaltensüberwachung durchsucht den Systemspeicher nach verdächtigen Prozessen, und durch die Echtzeitsuche wird der Prozess zugeordnet und nach Bedrohungen durch Malware durchsucht. Falls eine Bedrohung durch Malware vorhanden ist, wird der Prozess bzw. die Datei durch die Echtzeitsuche in Quarantäne verschoben. **Hinweis** Die Arbeitsspeichersuche funktioniert in Verbindung mit dem Anti-Exploit-Schutz in der Verhaltensüberwachung, um verbesserten Schutz vor dateilosen Angriffen zu bieten. Weitere Informationen finden Sie unter *Regeln und Ausnahmen der Verhaltensüberwachung konfigurieren auf Seite 9-17*.

Einstellung	Beschreibung
Komprimierte Dateien durchsuchen	Durchsucht die angegebene Anzahl von Komprimierungsebenen innerhalb einer archivierten Datei. **Hinweis** Durch das Durchsuchen mehrerer Ebenen kann Malware erkannt werden, die absichtlich in einem komprimierten Archiv verborgen ist. Die Suche kann jedoch die Systemleistung beeinträchtigen. Wählen Sie diese Option aus und konfigurieren Sie die folgenden Einstellungen: • **Maximale Schichtenanzahl**: Durchsucht die angegebene Anzahl von Komprimierungsebenen innerhalb einer archivierten Datei **Hinweis** Durch das Durchsuchen mehrerer Ebenen kann Malware erkannt werden, die absichtlich in einem komprimierten Archiv verborgen ist. Die Suche kann jedoch die Systemleistung beeinträchtigen. • **Durchsuchen Sie keine Dateien, wenn die komprimierte Dateigröße XX MB überschreitet**: Ermöglicht es Security Agent, die Größe einzelner Dateien in einem komprimierten Archiv zu überprüfen und das Durchsuchen von Dateien zu überspringen, wenn die Größe der einzelnen Dateien den konfigurierten Schwellenwert überschreitet • **Durchsuchen Sie in einer komprimierten Datei nur die ersten XX Dateien**: Verhindert, dass Security Agent alle Dateien in Archiven durchsucht, die mehr Dateien als den konfigurierten Schwellenwert enthalten

Einstellung	Beschreibung
OLE-Objekte durchsuchen	Durchsucht die angegebene Anzahl der OLE-Ebenen (Object Linking and Embedding) in einer Datei. **Exploit-Code in OLE-Dateien erkennen**: Bei der Funktion 'Erkennung von ausgenutzten OLE-Schwachstellen' wird Malware heuristisch gesucht, indem in Dateien von Microsoft Office nach Exploit-Code gesucht wird. **Hinweis** Die angegebene Anzahl Ebenen betrifft die Optionen **OLE-Objekte durchsuchen** und **Exploit-Code in OLE-Dateien erkennen**.
IntelliTrap aktivieren	Erkennt bösartigen Code, beispielsweise Bots, in komprimierten Dateien.
Aktivieren Sie die Suche nach CVE-Schwachstellen für Dateien, die über Internet- oder E-Mail-Kanäle heruntergeladen wurden	Sperrt Prozesse, die bekannte Schwachstellen in handelsüblichen Produkten ausnutzen, basierend auf dem CVE-System (Common Vulnerabilities and Exposures).

Echtzeitsuche: Registerkarte "Aktion"

Prozedur

1. Konfigurieren Sie im Abschnitt **Virus/Malware** die erforderlichen Einstellungen.
   a. Wählen Sie die Art der Maßnahme aus, die der Security Agent ergreift, nachdem eine Sicherheitsbedrohung erkannt wurde.
      - **ActiveAction verwenden**: Wählen Sie diese Option aus, um mehrere vorkonfigurierte Aktionen für die Suche nach Viren/Malware zu verwenden

Weitere Informationen finden Sie unter *ActiveAction auf Seite 10-54*.

- **Benutzerdefinierte Aktion bei Viren/Malware-Verdacht**: Wählen Sie die Aktion aus, die der Security Agent bei wahrscheinlichen Malware-Bedrohungen ausführt bzw. geben Sie die Aktion an.

- **Gleiche Aktion für alle Arten von Viren/Malware**: Geben Sie die Aktion an, die der Security Agent bei allen Malware-Bedrohungen ausführt.
- **Bestimmte Aktion für jede Art von Viren/Malware**: Geben Sie die Aktion an, die der Security Agent bei bestimmten Sicherheitsbedrohungen ausführt.

  Weitere Informationen finden Sie unter *Aktionen bei der benutzerdefinierten Suche auf Seite 10-56*.

b. Wählen Sie die Benachrichtigungstypen aus, die Endbenutzern angezeigt werden.

- **Bei Viren-/Malware-Fund Benachrichtigung anzeigen**: Wählen Sie diese Option aus, um eine Benachrichtigung anzuzeigen, die den Security Agent-Benutzer informiert, wenn ein Malware-Fund stattgefunden hat.
- **Bei Viren-/Malware-Verdacht Benachrichtigung anzeigen**: Wählen Sie diese Option aus, um eine Benachrichtigung anzuzeigen, die den Security Agent-Benutzer informiert, wenn ein wahrscheinlicher Malware-Fund stattgefunden hat.

c. Wählen Sie **Dateien vor dem Säubern sichern** aus, um eine verschlüsselte Kopie der infizierten Datei auf dem Endpunkt im Ordner `<Installationsordner des Agents>\Backup` zu erstellen.

Wenn Sie eine Sicherungskopie der Datei erstellen, können Sie bei Bedarf die ursprüngliche Version der Datei wiederherstellen.

d. Geben Sie den Speicherort des Quarantäne-Ordners an.

- **Quarantäne auf dem Security Agent-Verwaltungsserver**: Der Security Agent sendet eine verschlüsselte Kopie aller unter

Quarantäne gestellten Dateien an den verwaltenden Apex One-Server.

- **Quarantäne-Ordner**: Der Security Agent sendet eine verschlüsselte Kopie aller unter Quarantäne gestellten Dateien an den angegebenen Speicherort.

Weitere Informationen finden Sie unter *Quarantäne-Verzeichnis auf Seite 10-57*.

e. Konfigurieren Sie im Abschnitt **Damage Cleanup Services** die folgenden Einstellungen:

- **Säuberung durchführen, wenn mögliche Viren/Malware erkannt werden**: Führt den konfigurierten Säuberungstyp bei wahrscheinlichen Bedrohungen durch Malware durch.

Hinweis

Sie können diese Option nur auswählen, wenn die Aktion bei Viren-/Malware-Verdacht nicht **übergehen** oder **Zugriff verweigern** ist.

2. Wählen Sie im Abschnitt **Spyware/Grayware** die Aktion aus, die der Security Agent ausführt, nachdem Spyware- oder Grayware-Programme erkannt wurden.

- **Säubern**: Beendet alle zugehörigen Prozesse und löscht zugeordnete Registrierungswerte, Dateien, Cookies und Verknüpfungen.

Hinweis

Nach dem Säubern von Spyware/Grayware sichern die Security Agents Spyware-/Grayware-Daten, die Sie wiederherstellen können, wenn Sie den Zugriff auf die entsprechende Spyware/Grayware für sicher halten.

- **Übergehen**: Protokolliert den Fund, lässt aber die Programmausführung zu.

- **Zugriff verweigern**: Hindert den Endbenutzer am Öffnen oder Kopieren der Spyware- oder Grayware-Komponenten.
- **Bei Spyware-/Grayware-Fund Benachrichtigung auf Endpunkten anzeigen**: Wählen Sie diese Option aus, um eine Benachrichtigung anzuzeigen, die den Security Agent-Benutzer bei einem Spyware-/Grayware-Fund informiert.

3. Wählen Sie im Abschnitt **Erweiterte Malware-Erkennung** eine Option aus und konfigurieren Sie die erforderliche Einstellung.

   - **ActiveAction verwenden**: Wählen Sie diese Option, um eine Reihe vorkonfigurierter Suchaktionen auf erkannte portable ausführbare Dateien anzuwenden. Dies ist die empfohlene Option.

     Weitere Informationen finden Sie unter *ActiveAction auf Seite 10-54*.

   - **Verwenden Sie die gleiche Aktion für alle portablen ausführbaren Dateien mit Bedrohungen**: Wählen Sie, um eine der folgenden Aktionen auf erkannte portable ausführbare Dateien anzuwenden.

     - **Quarantäne**: Das System stellt die erkannten portablen ausführbaren Dateien automatisch unter Quarantäne.
     - **Übergehen**: Das System erstellt ein Erkennungsprotokoll, führt jedoch keine Aktion bei erkannten portablen ausführbaren Dateien aus.

Hinweis

Wenn eine erkannte portable ausführbare Datei in der Suchausschlussliste enthalten ist, führt das System keine Aktion an der Datei aus.

Echtzeitsuche: Registerkarte "Suchausschluss"

Prozedur

1. Wählen Sie **Suchausschluss aktivieren**.
2. Konfigurieren Sie im Abschnitt **Scan Exclusion List (Directories)** die erforderlichen Einstellungen.
   a. Wählen Sie **Verzeichnisse, in denen Trend Micro Produkte installiert sind, ausschließen**, um Verzeichnisse, die mit anderen Trend Micro-Produkten verbunden sind, automatisch auszuschließen.

      Weitere Informationen finden Sie unter *Trend Micro Produktverzeichnis, Ausschlüsse auf Seite 10-63*.

   b. Geben Sie bei der Konfiguration einer übergeordneten Richtlinie an, wie andere Benutzer untergeordnete Richtlinien konfigurieren können.

      - **Von übergeordnetem Element erben**: Untergeordnete Richtlinien müssen die Einstellungen verwenden, die in der übergeordneten Richtlinie konfiguriert wurden
      - **Von übergeordnetem Element erweitern**: Untergeordnete Richtlinien können zusätzliche Einstellungen an die Einstellungen anhängen, die von der übergeordneten Richtlinie vererbt wurden

      Hinweis

      Wenn Ihre Kinderrichtlinien **Von übergeordnetem Element erweitern** sind, können Sie **Einschränkungen der Kinderpolitik** konfigurieren, um zu verhindern, dass Kinderrichtlinien bestimmte Regeln zur Liste der Ausnahmeregeln hinzufügen.

   c. Geben Sie einen Verzeichnispfad ein, der aus DURCHSUCHEN ausgeschlossen werden soll, und klicken Sie auf die Schaltfläche **+**.

Der Security Agent durchsucht keine Dateien, die sich in dem angegebenen Verzeichnis (und dessen Unterverzeichnissen) befinden.

Hinweis

- Sie können maximal 256 Verzeichnisse angeben, die von der Suche ausgeschlossen werden sollen.
- Verwenden Sie die Schaltflächen **Importieren** und **Exportieren**, um die Liste mit verschiedenen Richtlinien zu teilen.
- Bei Verzeichnisausschlüssen können Platzhalterzeichen verwendet werden.

  Weitere Informationen finden Sie unter *Ausnahmen mit Platzhaltern auf Seite 10-64*.

3. Konfigurieren Sie im Abschnitt **Ausschlussliste für Virensuche (Dateien)** die erforderlichen Einstellungen.

   a. Geben Sie bei der Konfiguration einer übergeordneten Richtlinie an, wie andere Benutzer untergeordnete Richtlinien konfigurieren können.

   - **Von übergeordnetem Element erben**: Untergeordnete Richtlinien müssen die Einstellungen verwenden, die in der übergeordneten Richtlinie konfiguriert wurden
   - **Von übergeordnetem Element erweitern**: Untergeordnete Richtlinien können zusätzliche Einstellungen an die Einstellungen anhängen, die von der übergeordneten Richtlinie vererbt wurden

   b. Geben Sie einen Dateinamen oder den Dateinamen mit dem vollständigen Verzeichnispfad für den Ausschluss aus DURCHSUCHEN ein und klicken Sie auf die Schaltfläche **+**.

Hinweis

- Sie können maximal 256 Dateien angeben, die von der Suche ausgeschlossen werden sollen.
- Verwenden Sie die Schaltflächen **Importieren** und **Exportieren**, um die Liste mit verschiedenen Richtlinien zu teilen.
- Bei Dateiausschlüssen können Platzhalterzeichen verwendet werden.

  Weitere Informationen finden Sie unter *Ausnahmen mit Platzhaltern auf Seite 10-64*.

4. Konfigurieren Sie im Abschnitt **Ausschlussliste für Virensuche (Dateierweiterungen)** die erforderlichen Einstellungen.

   a. Geben Sie bei der Konfiguration einer übergeordneten Richtlinie an, wie andere Benutzer untergeordnete Richtlinien konfigurieren können.

      - **Von übergeordnetem Element erben**: Untergeordnete Richtlinien müssen die Einstellungen verwenden, die in der übergeordneten Richtlinie konfiguriert wurden
      - **Von übergeordnetem Element erweitern**: Untergeordnete Richtlinien können zusätzliche Einstellungen an die Einstellungen anhängen, die von der übergeordneten Richtlinie vererbt wurden

   b. Geben Sie eine Dateierweiterung ein, die aus Durchsuchvorgängen ausgeschlossen werden soll, oder wählen Sie diese aus und klicken Sie auf die Schaltfläche **Hinzufügen >**.

Hinweis

- Sie können maximal 256 Dateierweiterungen angeben, die von der Suche ausgeschlossen werden sollen.
- Verwenden Sie die Schaltflächen **Importieren** und **Exportieren**, um die Liste mit verschiedenen Richtlinien zu teilen.
- Die Echtzeitsuche bietet keine Unterstützung für die Verwendung von Platzhalterzeichen bei der Angabe von Ausschlüssen für Dateierweiterungen.

Zeitgesteuerte Suche

Die zeitgesteuerte Suche wird automatisch zur angegebenen Uhrzeit am angegebenen Datum ausgeführt. Verwenden Sie die zeitgesteuerte Suche, um die routinemäßige Suche auf dem Agent zu automatisieren und die Verwaltung der Virensuche zu optimieren.

Sie können die Einstellungen für die zeitgesteuerte Suche für einen oder mehrere Agents und Domänen bzw. für alle Agents, die vom Server verwaltet werden, konfigurieren und anwenden.

Einstellungen für zeitgesteuerte Suche konfigurieren

Prozedur

1. Wählen Sie die folgenden Optionen:
   - **Suche nach Virus/Malware aktivieren**
   - **Suche nach Spyware/Grayware aktivieren**

Hinweis

Bevor Sie nach Spyware/Grayware suchen können, müssen Sie die Viren-/Malware-Suche aktivieren.

2. Konfigurieren Sie die Einstellungen für **Ziel**.

   Weitere Informationen finden Sie unter *Zeitgesteuerte Suche: Registerkarte "Ziel" auf Seite 10-19*.

3. Konfigurieren Sie die Einstellungen für **Aktion**.

   Weitere Informationen finden Sie unter *Zeitgesteuerte Suche: Registerkarte "Aktion" auf Seite 10-25*.

4. Konfigurieren Sie die Einstellungen für **Suchausschluss**.

   Weitere Informationen finden Sie unter *Zeitgesteuerte Suche: Registerkarte "Suchausschluss" auf Seite 10-29*.

Zeitgesteuerte Suche: Registerkarte "Ziel"

Prozedur

1. Geben Sie im Abschnitt **Zeitplan** die Häufigkeit der zeitgesteuerten Suche an:

   - **Täglich**: Die Suche wird jeden Tag zur angegebenen Zeit durchgeführt.
   - **Wöchentlich, jeden <Wochentag>**: Die Suche wird ein Mal pro Woche am angegebenen Tag zur angegebenen Uhrzeit durchgeführt.
   - **Monatlich, am <Zahl>**: Die Suche wird ein Mal pro Monat am angegebenen Tag zur angegebenen Uhrzeit durchgeführt.
   - **Monatlich, am <xten> <Tag der Woche>**: Die Suche wird ein Mal pro Monat am angegebenen Wochentag zur angegebenen Uhrzeit durchgeführt.

   Wichtig

   Wenn Sie einen Tag wählen, der in einem bestimmten Monat nicht existiert (beispielsweise gibt es den Tag „30“ im Februar nicht) wird die zeitgesteuerte Suche am letzten Tag dieses Monats durchgeführt.

Hinweis

Geben Sie bei der Konfiguration einer übergeordneten Richtlinie an, wie andere Benutzer untergeordnete Richtlinien konfigurieren können.

- **Von übergeordnetem Element erben**: Untergeordnete Richtlinien müssen die Einstellungen verwenden, die in der übergeordneten Richtlinie konfiguriert wurden
- **Sind anpassbar**: Andere Administratoren können untergeordnete Richtlinien so konfigurieren, dass sie sich von den Einstellungen für übergeordnete Richtlinien unterscheiden.

2. Wählen Sie im Abschnitt **Zu durchsuchende Dateien** eine der folgenden Optionen aus:

   - **Alle durchsuchbaren Dateien**: Alle durchsuchbaren Dateien werden berücksichtigt. Zu den nicht durchsuchbaren Dateien gehören kennwortgeschützte und verschlüsselte Dateien sowie Dateien, die die vom Benutzer festgelegten Suchkriterien nicht erfüllen.

     Hinweis

     Diese Option bietet die höchstmögliche Sicherheit. Das Durchsuchen jeder Datei erfordert allerdings viel Zeit und viele Ressourcen und ist möglicherweise in manchen Fällen gar nicht notwendig. Deshalb können Sie bei Bedarf die Anzahl der durchsuchten Dateien begrenzen.

   - **Von IntelliScan durchsuchte Dateitypen**: Durchsucht Dateien auf Grundlage des ursprünglichen Dateityps.
   - **Dateien mit den folgenden Erweiterungen (mehrere Einträge mit Komma voneinander trennen)**: Legen Sie manuell fest, welche Dateien anhand der Dateierweiterung durchsucht werden sollen. Trennen Sie mehrere Einträge mit Kommas.

Hinweis

Geben Sie bei der Konfiguration einer übergeordneten Richtlinie an, wie andere Benutzer untergeordnete Richtlinien konfigurieren können.

- **Von übergeordnetem Element erben**: Untergeordnete Richtlinien müssen die Einstellungen verwenden, die in der übergeordneten Richtlinie konfiguriert wurden
- **Von übergeordnetem Element erweitern**: Untergeordnete Richtlinien können zusätzliche Einstellungen an die Einstellungen anhängen, die von der übergeordneten Richtlinie vererbt wurden

3. Konfigurieren Sie im Abschnitt **Sucheinstellungen** die erforderlichen Einstellungen.

Einstellung	Beschreibung
OLE-Objekte durchsuchen	Durchsucht die angegebene Anzahl der OLE-Ebenen (Object Linking and Embedding) in einer Datei. **Exploit-Code in OLE-Dateien erkennen**: Bei der Funktion 'Erkennung von ausgenutzten OLE-Schwachstellen' wird Malware heuristisch gesucht, indem in Dateien von Microsoft Office nach Exploit-Code gesucht wird. **Hinweis** Die angegebene Anzahl Ebenen betrifft die Optionen **OLE-Objekte durchsuchen** und **Exploit-Code in OLE-Dateien erkennen**.

Einstellung	Beschreibung
Benutzer XX Minuten vor Suchbeginn an die zeitgesteuerte Suche erinnern	Wählen Sie diese Option, um eine Benachrichtigung auf dem Endpunkt anzuzeigen, bevor die zeitgesteuerte Suche beginnt. **Hinweis** Sie können die Benachrichtigung auf der Registerkarte **Andere Einstellungen** im Fenster **Berechtigungen und anderen Einstellungen** deaktivieren.
Verschieben Zeitgesteuerte Suche um bis zu XX Stunde(n) und XX Minute(n)	Legen Sie die maximale Zeit fest, die Benutzer mit dem **Zeitgesteuerte Suche verschieben**-Privileg eine zeitgesteuerte Suche verzögern oder pausieren können. **Hinweis** Sie können die Berechtigung **Zeitgesteuerte Suche verschieben** auf der Registerkarte **Berechtigungen** des Fensters **Berechtigungen und anderen Einstellungen** erteilen.
Zeitgesteuerte Suche automatisch anhalten, wenn Suche länger als XX Stunde(n) und XX Minute(n) dauert	Beendet eine lange zeitgesteuerte Suche, nachdem die konfigurierte Zeitdauer erreicht wurde.
Zeitgesteuerte Suche überspringen, wenn die Akkulaufzeit eines Wireless-Endpunkts weniger als XX% beträgt und der AC-Adapter nicht angeschlossen ist	Verhindert, dass der Security Agent eine zeitgesteuerte Suche startet, wenn der Akkustand niedrig ist.

Einstellung	Beschreibung
Eine unterbrochene zeitgesteuerte Suche fortsetzen	Setzt eine zeitgesteuerte Suche zu der angegebenen Zeit fort, wenn der Benutzer die Suche durch Deaktivieren des Endpunkts unterbrochen hat.
Eine verpasste zeitgesteuerte Suche fortsetzen	Startet eine zeitgesteuerte Suche zum angegebenen Zeitpunkt, falls der Endpunkt nicht ausgeführt wurde, als die zeitgesteuerte Suche gestartet werden sollte.

Einstellung	Beschreibung
Komprimierte Dateien durchsuchen	Durchsucht die angegebene Anzahl von Komprimierungsebenen innerhalb einer archivierten Datei. **Hinweis** Durch das Durchsuchen mehrerer Ebenen kann Malware erkannt werden, die absichtlich in einem komprimierten Archiv verborgen ist. Die Suche kann jedoch die Systemleistung beeinträchtigen. Wählen Sie diese Option aus und konfigurieren Sie die folgenden Einstellungen: • **Maximale Schichtenanzahl**: Durchsucht die angegebene Anzahl von Komprimierungsebenen innerhalb einer archivierten Datei **Hinweis** Durch das Durchsuchen mehrerer Ebenen kann Malware erkannt werden, die absichtlich in einem komprimierten Archiv verborgen ist. Die Suche kann jedoch die Systemleistung beeinträchtigen. • **Durchsuchen Sie keine Dateien, wenn die komprimierte Dateigröße XX MB überschreitet**: Ermöglicht es Security Agent, die Größe einzelner Dateien in einem komprimierten Archiv zu überprüfen und das Durchsuchen von Dateien zu überspringen, wenn die Größe der einzelnen Dateien den konfigurierten Schwellenwert überschreitet • **Durchsuchen Sie in einer komprimierten Datei nur die ersten XX Dateien**: Verhindert, dass Security Agent alle Dateien in Archiven durchsucht, die mehr Dateien als den konfigurierten Schwellenwert enthalten
Bootbereich durchsuchen	Durchsucht den Bootsektor der Festplatte auf dem Endpunkt nach Viren/Malware.

4. Wählen Sie im Abschnitt **CPU-Auslastung** unter den folgenden Optionen:

   - **Hoch**: Ohne Pause zwischen den Suchläufen
   - **Mittel**: Pause zwischen den Suchläufen, wenn die CPU-Auslastung über 50 % liegt, sonst keine Pause
   - **Niedrig**: Pause zwischen den Suchläufen, wenn die CPU-Auslastung über 20 % liegt, sonst keine Pause

Zeitgesteuerte Suche: Registerkarte "Aktion"

Prozedur

1. Konfigurieren Sie im Abschnitt **Virus/Malware** die erforderlichen Einstellungen.

   a. Wählen Sie die Art der Maßnahme aus, die der Security Agent ergreift, nachdem eine Sicherheitsbedrohung erkannt wurde.

      - **ActiveAction verwenden**: Wählen Sie diese Option aus, um mehrere vorkonfigurierte Aktionen für die Suche nach Viren/Malware zu verwenden

        Weitere Informationen finden Sie unter *ActiveAction auf Seite 10-54*.

        - **Benutzerdefinierte Aktion bei Viren/Malware-Verdacht**: Wählen Sie die Aktion aus, die der Security Agent bei wahrscheinlichen Malware-Bedrohungen ausführt bzw. geben Sie die Aktion an.

      - **Gleiche Aktion für alle Arten von Viren/Malware**: Geben Sie die Aktion an, die der Security Agent bei allen Malware-Bedrohungen ausführt.
      - **Bestimmte Aktion für jede Art von Viren/Malware**: Geben Sie die Aktion an, die der Security Agent bei bestimmten Sicherheitsbedrohungen ausführt.

Weitere Informationen finden Sie unter *Aktionen bei der benutzerdefinierten Suche auf Seite 10-56*.

b. Wählen Sie die Benachrichtigungstypen aus, die Endbenutzern angezeigt werden.

- **Bei Viren-/Malware-Fund Benachrichtigung anzeigen**: Wählen Sie diese Option aus, um eine Benachrichtigung anzuzeigen, die den Security Agent-Benutzer informiert, wenn ein Malware-Fund stattgefunden hat.
- **Bei Viren-/Malware-Verdacht Benachrichtigung anzeigen**: Wählen Sie diese Option aus, um eine Benachrichtigung anzuzeigen, die den Security Agent-Benutzer informiert, wenn ein wahrscheinlicher Malware-Fund stattgefunden hat.

c. Wählen Sie **Dateien vor dem Säubern sichern** aus, um eine verschlüsselte Kopie der infizierten Datei auf dem Endpunkt im Ordner `<Installationsordner des Agents>\Backup` zu erstellen.

Wenn Sie eine Sicherungskopie der Datei erstellen, können Sie bei Bedarf die ursprüngliche Version der Datei wiederherstellen.

d. Geben Sie den Speicherort des Quarantäne-Ordners an.

- **Quarantäne auf dem Security Agent-Verwaltungsserver**: Der Security Agent sendet eine verschlüsselte Kopie aller unter Quarantäne gestellten Dateien an den verwaltenden Apex One-Server.
- **Quarantäne-Ordner**: Der Security Agent sendet eine verschlüsselte Kopie aller unter Quarantäne gestellten Dateien an den angegebenen Speicherort.

Weitere Informationen finden Sie unter *Quarantäne-Verzeichnis auf Seite 10-57*.

e. Konfigurieren Sie im Abschnitt **Damage Cleanup Services** die folgenden Einstellungen:

- **Säuberungstyp**

- **Standardsäuberung**: Während einer Standardsäuberung führt der Security Agent die folgenden Aktionen durch:
  - Entdeckt und entfernt aktive Trojaner
  - Beendet durch Trojaner ausgelöste Prozesse
  - Repariert von Trojanern geänderte Systemdateien
  - Löscht von Trojanern hinterlassene Dateien und Anwendungen
- **Erweiterte Säuberung**: Zusätzlich zu den durchgeführten Standardsäuberungsaktionen beendet der Security Agent Aktivitäten, die von einer bösartigen Sicherheitssoftware (auch als FakeAV bekannt) und bestimmten Rootkit-Varianten ausgeführt werden.

- **Säuberung durchführen, wenn mögliche Viren/Malware erkannt werden**: Führt den konfigurierten Säuberungstyp bei wahrscheinlichen Bedrohungen durch Malware durch.

Hinweis

Sie können diese Option nur auswählen, wenn die Aktion bei Viren-/Malware-Verdacht nicht **übergehen** oder **Zugriff verweigern** ist.

2. Wählen Sie im Abschnitt **Spyware/Grayware** die Aktion aus, die der Security Agent ausführt, nachdem Spyware- oder Grayware-Programme erkannt wurden.
   - **Säubern**: Beendet alle zugehörigen Prozesse und löscht zugeordnete Registrierungswerte, Dateien, Cookies und Verknüpfungen.

Hinweis

Nach dem Säubern von Spyware/Grayware sichern die Security Agents Spyware-/Grayware-Daten, die Sie wiederherstellen können, wenn Sie den Zugriff auf die entsprechende Spyware/Grayware für sicher halten.

- **Übergehen**: Protokolliert den Fund, lässt aber die Programmausführung zu.
- **Bei Spyware-/Grayware-Fund Benachrichtigung auf Endpunkten anzeigen**: Wählen Sie diese Option aus, um eine Benachrichtigung anzuzeigen, die den Security Agent-Benutzer bei einem Spyware-/Grayware-Fund informiert.

3. Wählen Sie im Abschnitt **Erweiterte Malware-Erkennung** eine Option aus und konfigurieren Sie die erforderliche Einstellung.

   - **ActiveAction verwenden**: Wählen Sie diese Option, um eine Reihe vorkonfigurierter Suchaktionen auf erkannte portable ausführbare Dateien anzuwenden. Dies ist die empfohlene Option.

     Weitere Informationen finden Sie unter *ActiveAction auf Seite 10-54*.

   - **Verwenden Sie die gleiche Aktion für alle portablen ausführbaren Dateien mit Bedrohungen**: Wählen Sie, um eine der folgenden Aktionen auf erkannte portable ausführbare Dateien anzuwenden.

     - **Quarantäne**: Das System stellt die erkannten portablen ausführbaren Dateien automatisch unter Quarantäne.
     - **Übergehen**: Das System erstellt ein Erkennungsprotokoll, führt jedoch keine Aktion bei erkannten portablen ausführbaren Dateien aus.

Hinweis

Wenn eine erkannte portable ausführbare Datei in der Suchausschlussliste enthalten ist, führt das System keine Aktion an der Datei aus.

Zeitgesteuerte Suche: Registerkarte "Suchausschluss"

Prozedur

1. Wählen Sie **Suchausschluss aktivieren**.
2. Konfigurieren Sie im Abschnitt **Scan Exclusion List (Directories)** die erforderlichen Einstellungen.
   a. Wählen Sie **Verzeichnisse, in denen Trend Micro Produkte installiert sind, ausschließen**, um Verzeichnisse, die mit anderen Trend Micro-Produkten verbunden sind, automatisch auszuschließen.

      Weitere Informationen finden Sie unter *Trend Micro Produktverzeichnis, Ausschlüsse auf Seite 10-63*.

   b. Geben Sie bei der Konfiguration einer übergeordneten Richtlinie an, wie andere Benutzer untergeordnete Richtlinien konfigurieren können.

      - **Von übergeordnetem Element erben**: Untergeordnete Richtlinien müssen die Einstellungen verwenden, die in der übergeordneten Richtlinie konfiguriert wurden
      - **Von übergeordnetem Element erweitern**: Untergeordnete Richtlinien können zusätzliche Einstellungen an die Einstellungen anhängen, die von der übergeordneten Richtlinie vererbt wurden

Hinweis

Wenn Ihre Kinderrichtlinien **Von übergeordnetem Element erweitern** sind, können Sie **Einschränkungen der Kinderpolitik** konfigurieren, um zu verhindern, dass Kinderrichtlinien bestimmte Regeln zur Liste der Ausnahmeregeln hinzufügen.

c. Geben Sie einen Verzeichnispfad ein, der aus DURCHSUCHEN ausgeschlossen werden soll, und klicken Sie auf die Schaltfläche **+**.

Der Security Agent durchsucht keine Dateien, die sich in dem angegebenen Verzeichnis (und dessen Unterverzeichnissen) befinden.

Hinweis

- Sie können maximal 256 Verzeichnisse angeben, die von der Suche ausgeschlossen werden sollen.
- Verwenden Sie die Schaltflächen **Importieren** und **Exportieren**, um die Liste mit verschiedenen Richtlinien zu teilen.
- Bei Verzeichnisausschlüssen können Platzhalterzeichen verwendet werden.

  Weitere Informationen finden Sie unter *Ausnahmen mit Platzhaltern auf Seite 10-64*.

3. Konfigurieren Sie im Abschnitt **Ausschlussliste für Virensuche (Dateien)** die erforderlichen Einstellungen.

a. Geben Sie bei der Konfiguration einer übergeordneten Richtlinie an, wie andere Benutzer untergeordnete Richtlinien konfigurieren können.

- **Von übergeordnetem Element erben**: Untergeordnete Richtlinien müssen die Einstellungen verwenden, die in der übergeordneten Richtlinie konfiguriert wurden
- **Von übergeordnetem Element erweitern**: Untergeordnete Richtlinien können zusätzliche Einstellungen an die Einstellungen anhängen, die von der übergeordneten Richtlinie vererbt wurden

b. Geben Sie einen Dateinamen oder den Dateinamen mit dem vollständigen Verzeichnispfad für den Ausschluss aus DURCHSUCHEN ein und klicken Sie auf die Schaltfläche **+**.

Hinweis

- Sie können maximal 256 Dateien angeben, die von der Suche ausgeschlossen werden sollen.
- Verwenden Sie die Schaltflächen **Importieren** und **Exportieren**, um die Liste mit verschiedenen Richtlinien zu teilen.
- Bei Dateiausschlüssen können Platzhalterzeichen verwendet werden.

  Weitere Informationen finden Sie unter *Ausnahmen mit Platzhaltern auf Seite 10-64*.

---

4. Konfigurieren Sie im Abschnitt **Ausschlussliste für Virensuche (Dateierweiterungen)** die erforderlichen Einstellungen.

a. Geben Sie bei der Konfiguration einer übergeordneten Richtlinie an, wie andere Benutzer untergeordnete Richtlinien konfigurieren können.

- **Von übergeordnetem Element erben**: Untergeordnete Richtlinien müssen die Einstellungen verwenden, die in der übergeordneten Richtlinie konfiguriert wurden
- **Von übergeordnetem Element erweitern**: Untergeordnete Richtlinien können zusätzliche Einstellungen an die

Einstellungen anhängen, die von der übergeordneten Richtlinie vererbt wurden

b. Geben Sie eine Dateierweiterung ein, die aus Durchsuchvorgängen ausgeschlossen werden soll, oder wählen Sie diese aus und klicken Sie auf die Schaltfläche **Hinzufügen >**.

Hinweis

- Sie können maximal 256 Dateierweiterungen angeben, die von der Suche ausgeschlossen werden sollen.
- Verwenden Sie die Schaltflächen **Importieren** und **Exportieren**, um die Liste mit verschiedenen Richtlinien zu teilen.
- Verwenden Sie bei der manuellen Durchsuchen, der zeitgesteuerten Durchsuchen und der sofortigen Durchsuchen ("Jetzt durchsuchen") als Platzhalter ein Fragezeichen (?), um ein einzelnes Zeichen zu ersetzen, oder ein Sternchen (*), um mehrere Zeichen zu ersetzen. Wenn Sie beispielsweise nicht alle Dateien durchsuchen möchten, deren Erweiterung mit "D" beginnt, wie z. B. `DOC`, `DOT` oder `DAT`, geben Sie `D*` oder `D??` ein.

Manuelle Suche

Bei der manuellen Suche handelt es sich um eine Suche bei Bedarf, die direkt ausgeführt wird, nachdem ein Benutzer die Suche auf der Security Agent-Konsole startet. Die Dauer der Suche hängt von der Anzahl der Dateien und den Hardware-Ressourcen des Security Agent-endpunkts ab.

Sie können die Einstellungen für die manuelle Suche für einen oder mehrere Agents und Domänen bzw. für alle Agents, die vom Server verwaltet werden, konfigurieren und anwenden.

Manuelle Suche: Registerkarte "Ziel"

Prozedur

1. Wählen Sie im Abschnitt **Zu durchsuchende Dateien** eine der folgenden Optionen aus:

   - **Alle durchsuchbaren Dateien**: Alle durchsuchbaren Dateien werden berücksichtigt. Zu den nicht durchsuchbaren Dateien gehören kennwortgeschützte und verschlüsselte Dateien sowie Dateien, die die vom Benutzer festgelegten Suchkriterien nicht erfüllen.

     Hinweis

     Diese Option bietet die höchstmögliche Sicherheit. Das Durchsuchen jeder Datei erfordert allerdings viel Zeit und viele Ressourcen und ist möglicherweise in manchen Fällen gar nicht notwendig. Deshalb können Sie bei Bedarf die Anzahl der durchsuchten Dateien begrenzen.

   - **Von IntelliScan durchsuchte Dateitypen**: Durchsucht Dateien auf Grundlage des ursprünglichen Dateityps.
   - **Dateien mit den folgenden Erweiterungen (mehrere Einträge mit Komma voneinander trennen)**: Legen Sie manuell fest, welche Dateien anhand der Dateierweiterung durchsucht werden sollen. Trennen Sie mehrere Einträge mit Kommas.

Hinweis

Geben Sie bei der Konfiguration einer übergeordneten Richtlinie an, wie andere Benutzer untergeordnete Richtlinien konfigurieren können.

- **Von übergeordnetem Element erben**: Untergeordnete Richtlinien müssen die Einstellungen verwenden, die in der übergeordneten Richtlinie konfiguriert wurden
- **Von übergeordnetem Element erweitern**: Untergeordnete Richtlinien können zusätzliche Einstellungen an die Einstellungen anhängen, die von der übergeordneten Richtlinie vererbt wurden

2. Konfigurieren Sie im Abschnitt **Sucheinstellungen** die erforderlichen Einstellungen.

Einstellung	Beschreibung
Versteckte Ordner	Lässt zu, dass der Security Agent versteckte Ordner auf dem Endpunkt erkennt und anschließend durchsucht.
Netzlaufwerk durchsuchen	Durchsucht Verzeichnisse, die sich physisch auf anderen Endpunkten befinden, aber dem lokalen Endpunkt zugeordnet sind.

Einstellung	Beschreibung
Komprimierte Dateien durchsuchen	Durchsucht die angegebene Anzahl von Komprimierungsebenen innerhalb einer archivierten Datei. **Hinweis** Durch das Durchsuchen mehrerer Ebenen kann Malware erkannt werden, die absichtlich in einem komprimierten Archiv verborgen ist. Die Suche kann jedoch die Systemleistung beeinträchtigen. Wählen Sie diese Option aus und konfigurieren Sie die folgenden Einstellungen: • **Maximale Schichtenanzahl**: Durchsucht die angegebene Anzahl von Komprimierungsebenen innerhalb einer archivierten Datei **Hinweis** Durch das Durchsuchen mehrerer Ebenen kann Malware erkannt werden, die absichtlich in einem komprimierten Archiv verborgen ist. Die Suche kann jedoch die Systemleistung beeinträchtigen. • **Durchsuchen Sie keine Dateien, wenn die komprimierte Dateigröße XX MB überschreitet**: Ermöglicht es Security Agent, die Größe einzelner Dateien in einem komprimierten Archiv zu überprüfen und das Durchsuchen von Dateien zu überspringen, wenn die Größe der einzelnen Dateien den konfigurierten Schwellenwert überschreitet • **Durchsuchen Sie in einer komprimierten Datei nur die ersten XX Dateien**: Verhindert, dass Security Agent alle Dateien in Archiven durchsucht, die mehr Dateien als den konfigurierten Schwellenwert enthalten

Einstellung	Beschreibung
OLE-Objekte durchsuchen	Durchsucht die angegebene Anzahl der OLE-Ebenen (Object Linking and Embedding) in einer Datei. **Exploit-Code in OLE-Dateien erkennen**: Bei der Funktion 'Erkennung von ausgenutzten OLE-Schwachstellen' wird Malware heuristisch gesucht, indem in Dateien von Microsoft Office nach Exploit-Code gesucht wird. **Hinweis** Die angegebene Anzahl Ebenen betrifft die Optionen **OLE-Objekte durchsuchen** und **Exploit-Code in OLE-Dateien erkennen**.
Bootbereich durchsuchen	Durchsucht den Bootsektor der Festplatte auf dem Endpunkt nach Viren/Malware.

3. Wählen Sie im Abschnitt **CPU-Auslastung** unter den folgenden Optionen:
   - **Hoch**: Ohne Pause zwischen den Suchläufen
   - **Mittel**: Pause zwischen den Suchläufen, wenn die CPU-Auslastung über 50 % liegt, sonst keine Pause
   - **Niedrig**: Pause zwischen den Suchläufen, wenn die CPU-Auslastung über 20 % liegt, sonst keine Pause

Manuelle Suche: Registerkarte "Aktion"

Prozedur

1. Konfigurieren Sie im Abschnitt **Virus/Malware** die erforderlichen Einstellungen.
   a. Wählen Sie die Art der Maßnahme aus, die der Security Agent ergreift, nachdem eine Sicherheitsbedrohung erkannt wurde.

- **ActiveAction verwenden**: Wählen Sie diese Option aus, um mehrere vorkonfigurierte Aktionen für die Suche nach Viren/Malware zu verwenden

  Weitere Informationen finden Sie unter *ActiveAction auf Seite 10-54*.

  - **Benutzerdefinierte Aktion bei Viren/Malware-Verdacht**: Wählen Sie die Aktion aus, die der Security Agent bei wahrscheinlichen Malware-Bedrohungen ausführt bzw. geben Sie die Aktion an.

- **Gleiche Aktion für alle Arten von Viren/Malware**: Geben Sie die Aktion an, die der Security Agent bei allen Malware-Bedrohungen ausführt.

- **Bestimmte Aktion für jede Art von Viren/Malware**: Geben Sie die Aktion an, die der Security Agent bei bestimmten Sicherheitsbedrohungen ausführt.

  Weitere Informationen finden Sie unter *Aktionen bei der benutzerdefinierten Suche auf Seite 10-56*.

b. Wählen Sie **Dateien vor dem Säubern sichern** aus, um eine verschlüsselte Kopie der infizierten Datei auf dem Endpunkt im Ordner `<Installationsordner des Agents>\Backup` zu erstellen.

Wenn Sie eine Sicherungskopie der Datei erstellen, können Sie bei Bedarf die ursprüngliche Version der Datei wiederherstellen.

c. Geben Sie den Speicherort des Quarantäne-Ordners an.

- **Quarantäne auf dem Security Agent-Verwaltungsserver**: Der Security Agent sendet eine verschlüsselte Kopie aller unter Quarantäne gestellten Dateien an den verwaltenden Apex One-Server.

- **Quarantäne-Ordner**: Der Security Agent sendet eine verschlüsselte Kopie aller unter Quarantäne gestellten Dateien an den angegebenen Speicherort.

Weitere Informationen finden Sie unter *Quarantäne-Verzeichnis auf Seite 10-57*.

d. Konfigurieren Sie im Abschnitt **Damage Cleanup Services** die folgenden Einstellungen:

- **Säuberungstyp**
  - **Standardsäuberung**: Während einer Standardsäuberung führt der Security Agent die folgenden Aktionen durch:
    - Entdeckt und entfernt aktive Trojaner
    - Beendet durch Trojaner ausgelöste Prozesse
    - Repariert von Trojanern geänderte Systemdateien
    - Löscht von Trojanern hinterlassene Dateien und Anwendungen
  - **Erweiterte Säuberung**: Zusätzlich zu den durchgeführten Standardsäuberungsaktionen beendet der Security Agent Aktivitäten, die von einer bösartigen Sicherheitssoftware (auch als FakeAV bekannt) und bestimmten Rootkit-Varianten ausgeführt werden.
- **Säuberung durchführen, wenn mögliche Viren/Malware erkannt werden**: Führt den konfigurierten Säuberungstyp bei wahrscheinlichen Bedrohungen durch Malware durch.

Hinweis

Sie können diese Option nur auswählen, wenn die Aktion bei Viren-/Malware-Verdacht nicht **übergehen** oder **Zugriff verweigern** ist.

2. Wählen Sie im Abschnitt **Spyware/Grayware** die Aktion aus, die der Security Agent ausführt, nachdem Spyware- oder Grayware-Programme erkannt wurden.

- **Säubern**: Beendet alle zugehörigen Prozesse und löscht zugeordnete Registrierungswerte, Dateien, Cookies und Verknüpfungen.

Hinweis

Nach dem Säubern von Spyware/Grayware sichern die Security Agents Spyware-/Grayware-Daten, die Sie wiederherstellen können, wenn Sie den Zugriff auf die entsprechende Spyware/Grayware für sicher halten.

- **Übergehen**: Protokolliert den Fund, lässt aber die Programmausführung zu.

3. Wählen Sie im Abschnitt **Erweiterte Malware-Erkennung** eine Option aus und konfigurieren Sie die erforderliche Einstellung.

   - **ActiveAction verwenden**: Wählen Sie diese Option, um eine Reihe vorkonfigurierter Suchaktionen auf erkannte portable ausführbare Dateien anzuwenden. Dies ist die empfohlene Option.

     Weitere Informationen finden Sie unter *ActiveAction auf Seite 10-54*.

   - **Verwenden Sie die gleiche Aktion für alle portablen ausführbaren Dateien mit Bedrohungen**: Wählen Sie, um eine der folgenden Aktionen auf erkannte portable ausführbare Dateien anzuwenden.

     - **Quarantäne**: Das System stellt die erkannten portablen ausführbaren Dateien automatisch unter Quarantäne.
     - **Übergehen**: Das System erstellt ein Erkennungsprotokoll, führt jedoch keine Aktion bei erkannten portablen ausführbaren Dateien aus.

   Hinweis

   Wenn eine erkannte portable ausführbare Datei in der Suchausschlussliste enthalten ist, führt das System keine Aktion an der Datei aus.

Manuelle Suche: Registerkarte "Suchausschluss"

Prozedur

1. Wählen Sie **Suchausschluss aktivieren**.
2. Konfigurieren Sie im Abschnitt **Scan Exclusion List (Directories)** die erforderlichen Einstellungen.
   a. Wählen Sie **Verzeichnisse, in denen Trend Micro Produkte installiert sind, ausschließen**, um Verzeichnisse, die mit anderen Trend Micro-Produkten verbunden sind, automatisch auszuschließen.

      Weitere Informationen finden Sie unter *Trend Micro Produktverzeichnis, Ausschlüsse auf Seite 10-63*.

   b. Geben Sie bei der Konfiguration einer übergeordneten Richtlinie an, wie andere Benutzer untergeordnete Richtlinien konfigurieren können.

      - **Von übergeordnetem Element erben**: Untergeordnete Richtlinien müssen die Einstellungen verwenden, die in der übergeordneten Richtlinie konfiguriert wurden
      - **Von übergeordnetem Element erweitern**: Untergeordnete Richtlinien können zusätzliche Einstellungen an die Einstellungen anhängen, die von der übergeordneten Richtlinie vererbt wurden

      Hinweis

      Wenn Ihre Kinderrichtlinien **Von übergeordnetem Element erweitern** sind, können Sie **Einschränkungen der Kinderpolitik** konfigurieren, um zu verhindern, dass Kinderrichtlinien bestimmte Regeln zur Liste der Ausnahmeregeln hinzufügen.

   c. Geben Sie einen Verzeichnispfad ein, der aus DURCHSUCHEN ausgeschlossen werden soll, und klicken Sie auf die Schaltfläche **+**.

Der Security Agent durchsucht keine Dateien, die sich in dem angegebenen Verzeichnis (und dessen Unterverzeichnissen) befinden.

Hinweis

- Sie können maximal 256 Verzeichnisse angeben, die von der Suche ausgeschlossen werden sollen.
- Verwenden Sie die Schaltflächen **Importieren** und **Exportieren**, um die Liste mit verschiedenen Richtlinien zu teilen.
- Bei Verzeichnisausschlüssen können Platzhalterzeichen verwendet werden.

  Weitere Informationen finden Sie unter *Ausnahmen mit Platzhaltern auf Seite 10-64*.

3. Konfigurieren Sie im Abschnitt **Ausschlussliste für Virensuche (Dateien)** die erforderlichen Einstellungen.

   a. Geben Sie bei der Konfiguration einer übergeordneten Richtlinie an, wie andere Benutzer untergeordnete Richtlinien konfigurieren können.

   - **Von übergeordnetem Element erben**: Untergeordnete Richtlinien müssen die Einstellungen verwenden, die in der übergeordneten Richtlinie konfiguriert wurden
   - **Von übergeordnetem Element erweitern**: Untergeordnete Richtlinien können zusätzliche Einstellungen an die Einstellungen anhängen, die von der übergeordneten Richtlinie vererbt wurden

   b. Geben Sie einen Dateinamen oder den Dateinamen mit dem vollständigen Verzeichnispfad für den Ausschluss aus DURCHSUCHEN ein und klicken Sie auf die Schaltfläche **+**.

Hinweis

- Sie können maximal 256 Dateien angeben, die von der Suche ausgeschlossen werden sollen.
- Verwenden Sie die Schaltflächen **Importieren** und **Exportieren**, um die Liste mit verschiedenen Richtlinien zu teilen.
- Bei Dateiausschlüssen können Platzhalterzeichen verwendet werden.

  Weitere Informationen finden Sie unter *Ausnahmen mit Platzhaltern auf Seite 10-64*.

4. Konfigurieren Sie im Abschnitt **Ausschlussliste für Virensuche (Dateierweiterungen)** die erforderlichen Einstellungen.

   a. Geben Sie bei der Konfiguration einer übergeordneten Richtlinie an, wie andere Benutzer untergeordnete Richtlinien konfigurieren können.

      - **Von übergeordnetem Element erben**: Untergeordnete Richtlinien müssen die Einstellungen verwenden, die in der übergeordneten Richtlinie konfiguriert wurden
      - **Von übergeordnetem Element erweitern**: Untergeordnete Richtlinien können zusätzliche Einstellungen an die Einstellungen anhängen, die von der übergeordneten Richtlinie vererbt wurden

   b. Geben Sie eine Dateierweiterung ein, die aus Durchsuchvorgängen ausgeschlossen werden soll, oder wählen Sie diese aus und klicken Sie auf die Schaltfläche **Hinzufügen >**.

Hinweis

- Sie können maximal 256 Dateierweiterungen angeben, die von der Suche ausgeschlossen werden sollen.
- Verwenden Sie die Schaltflächen **Importieren** und **Exportieren**, um die Liste mit verschiedenen Richtlinien zu teilen.
- Verwenden Sie bei der manuellen Durchsuchen, der zeitgesteuerten Durchsuchen und der sofortigen Durchsuchen ("Jetzt durchsuchen") als Platzhalter ein Fragezeichen (?), um ein einzelnes Zeichen zu ersetzen, oder ein Sternchen (*), um mehrere Zeichen zu ersetzen. Wenn Sie beispielsweise nicht alle Dateien durchsuchen möchten, deren Erweiterung mit "D" beginnt, wie z. B. `DOC`, `DOT` oder `DAT`, geben Sie `D*` oder `D??` ein.

Jetzt durchsuchen

Die sofortige Suche ("Jetzt durchsuchen") wird von Administratoren von einem Remote-Standort aus über die Webkonsole gestartet und kann für einen oder mehrere Security Agent-Endpunkte ausgeführt werden.

Sie können die Einstellungen für 'Jetzt durchsuchen' für einen oder mehrere Security Agents und Domänen bzw. für alle Security Agents, die vom Server verwaltet werden, konfigurieren und anwenden.

Einstellungen von Jetzt durchsuchen konfigurieren

Prozedur

1. Wählen Sie die folgenden Optionen:
   - **Suche nach Virus/Malware aktivieren**
   - **Suche nach Spyware/Grayware aktivieren**

Hinweis

Bevor Sie nach Spyware/Grayware suchen können, müssen Sie die Viren-/Malware-Suche aktivieren.

2. Konfigurieren Sie die Einstellungen für **Ziel**.

   Weitere Informationen finden Sie unter *Jetzt durchsuchen: Registerkarte "Ziel" auf Seite 10-44*.

3. Konfigurieren Sie die Einstellungen für **Aktion**.

   Weitere Informationen finden Sie unter *Jetzt durchsuchen: Registerkarte "Aktion" auf Seite 10-47*.

4. Konfigurieren Sie die Einstellungen für **Suchausschluss**.

   Weitere Informationen finden Sie unter *Jetzt durchsuchen: Registerkarte "Suchausschluss" auf Seite 10-51*.

Jetzt durchsuchen: Registerkarte "Ziel"

Prozedur

1. Wählen Sie im Abschnitt **Zu durchsuchende Dateien** eine der folgenden Optionen aus:

   - **Alle durchsuchbaren Dateien**: Alle durchsuchbaren Dateien werden berücksichtigt. Zu den nicht durchsuchbaren Dateien gehören kennwortgeschützte und verschlüsselte Dateien sowie Dateien, die die vom Benutzer festgelegten Suchkriterien nicht erfüllen.

     Hinweis

     Diese Option bietet die höchstmögliche Sicherheit. Das Durchsuchen jeder Datei erfordert allerdings viel Zeit und viele Ressourcen und ist möglicherweise in manchen Fällen gar nicht notwendig. Deshalb können Sie bei Bedarf die Anzahl der durchsuchten Dateien begrenzen.

- **Von IntelliScan durchsuchte Dateitypen**: Durchsucht Dateien auf Grundlage des ursprünglichen Dateityps.
- **Dateien mit den folgenden Erweiterungen (mehrere Einträge mit Komma voneinander trennen)**: Legen Sie manuell fest, welche Dateien anhand der Dateierweiterung durchsucht werden sollen. Trennen Sie mehrere Einträge mit Kommas.

Hinweis

Geben Sie bei der Konfiguration einer übergeordneten Richtlinie an, wie andere Benutzer untergeordnete Richtlinien konfigurieren können.

- **Von übergeordnetem Element erben**: Untergeordnete Richtlinien müssen die Einstellungen verwenden, die in der übergeordneten Richtlinie konfiguriert wurden
- **Von übergeordnetem Element erweitern**: Untergeordnete Richtlinien können zusätzliche Einstellungen an die Einstellungen anhängen, die von der übergeordneten Richtlinie vererbt wurden

2. Konfigurieren Sie im Abschnitt **Sucheinstellungen** die erforderlichen Einstellungen.

Einstellung	Beschreibung
Komprimierte Dateien durchsuchen	Durchsucht die angegebene Anzahl von Komprimierungsebenen innerhalb einer archivierten Datei. **Hinweis** Durch das Durchsuchen mehrerer Ebenen kann Malware erkannt werden, die absichtlich in einem komprimierten Archiv verborgen ist. Die Suche kann jedoch die Systemleistung beeinträchtigen. Wählen Sie diese Option aus und konfigurieren Sie die folgenden Einstellungen: • **Maximale Schichtenanzahl**: Durchsucht die angegebene Anzahl von Komprimierungsebenen innerhalb einer archivierten Datei **Hinweis** Durch das Durchsuchen mehrerer Ebenen kann Malware erkannt werden, die absichtlich in einem komprimierten Archiv verborgen ist. Die Suche kann jedoch die Systemleistung beeinträchtigen. • **Durchsuchen Sie keine Dateien, wenn die komprimierte Dateigröße XX MB überschreitet**: Ermöglicht es Security Agent, die Größe einzelner Dateien in einem komprimierten Archiv zu überprüfen und das Durchsuchen von Dateien zu überspringen, wenn die Größe der einzelnen Dateien den konfigurierten Schwellenwert überschreitet • **Durchsuchen Sie in einer komprimierten Datei nur die ersten XX Dateien**: Verhindert, dass Security Agent alle Dateien in Archiven durchsucht, die mehr Dateien als den konfigurierten Schwellenwert enthalten

Einstellung	Beschreibung
OLE-Objekte durchsuchen	Durchsucht die angegebene Anzahl der OLE-Ebenen (Object Linking and Embedding) in einer Datei. **Exploit-Code in OLE-Dateien erkennen**: Bei der Funktion 'Erkennung von ausgenutzten OLE-Schwachstellen' wird Malware heuristisch gesucht, indem in Dateien von Microsoft Office nach Exploit-Code gesucht wird. **Hinweis** Die angegebene Anzahl Ebenen betrifft die Optionen **OLE-Objekte durchsuchen** und **Exploit-Code in OLE-Dateien erkennen**.
Bootbereich durchsuchen	Durchsucht den Bootsektor der Festplatte auf dem Endpunkt nach Viren/Malware.

3. Wählen Sie im Abschnitt **CPU-Auslastung** unter den folgenden Optionen:
   - **Hoch**: Ohne Pause zwischen den Suchläufen
   - **Mittel**: Pause zwischen den Suchläufen, wenn die CPU-Auslastung über 50 % liegt, sonst keine Pause
   - **Niedrig**: Pause zwischen den Suchläufen, wenn die CPU-Auslastung über 20 % liegt, sonst keine Pause

Jetzt durchsuchen: Registerkarte "Aktion"

Prozedur

1. Konfigurieren Sie im Abschnitt **Virus/Malware** die erforderlichen Einstellungen.
   a. Wählen Sie die Art der Maßnahme aus, die der Security Agent ergreift, nachdem eine Sicherheitsbedrohung erkannt wurde.

- **ActiveAction verwenden**: Wählen Sie diese Option aus, um mehrere vorkonfigurierte Aktionen für die Suche nach Viren/Malware zu verwenden

  Weitere Informationen finden Sie unter *ActiveAction auf Seite 10-54*.

  - **Benutzerdefinierte Aktion bei Viren/Malware-Verdacht**: Wählen Sie die Aktion aus, die der Security Agent bei wahrscheinlichen Malware-Bedrohungen ausführt bzw. geben Sie die Aktion an.

- **Gleiche Aktion für alle Arten von Viren/Malware**: Geben Sie die Aktion an, die der Security Agent bei allen Malware-Bedrohungen ausführt.
- **Bestimmte Aktion für jede Art von Viren/Malware**: Geben Sie die Aktion an, die der Security Agent bei bestimmten Sicherheitsbedrohungen ausführt.

  Weitere Informationen finden Sie unter *Aktionen bei der benutzerdefinierten Suche auf Seite 10-56*.

b. Wählen Sie **Dateien vor dem Säubern sichern** aus, um eine verschlüsselte Kopie der infizierten Datei auf dem Endpunkt im Ordner `<Installationsordner des Agents>\Backup` zu erstellen.

Wenn Sie eine Sicherungskopie der Datei erstellen, können Sie bei Bedarf die ursprüngliche Version der Datei wiederherstellen.

c. Geben Sie den Speicherort des Quarantäne-Ordners an.

- **Quarantäne auf dem Security Agent-Verwaltungsserver**: Der Security Agent sendet eine verschlüsselte Kopie aller unter Quarantäne gestellten Dateien an den verwaltenden Apex One-Server.
- **Quarantäne-Ordner**: Der Security Agent sendet eine verschlüsselte Kopie aller unter Quarantäne gestellten Dateien an den angegebenen Speicherort.

Weitere Informationen finden Sie unter *Quarantäne-Verzeichnis auf Seite 10-57*.

d. Konfigurieren Sie im Abschnitt **Damage Cleanup Services** die folgenden Einstellungen:

- **Säuberungstyp**
  - **Standardsäuberung**: Während einer Standardsäuberung führt der Security Agent die folgenden Aktionen durch:
    - Entdeckt und entfernt aktive Trojaner
    - Beendet durch Trojaner ausgelöste Prozesse
    - Repariert von Trojanern geänderte Systemdateien
    - Löscht von Trojanern hinterlassene Dateien und Anwendungen
  - **Erweiterte Säuberung**: Zusätzlich zu den durchgeführten Standardsäuberungsaktionen beendet der Security Agent Aktivitäten, die von einer bösartigen Sicherheitssoftware (auch als FakeAV bekannt) und bestimmten Rootkit-Varianten ausgeführt werden.
- **Säuberung durchführen, wenn mögliche Viren/Malware erkannt werden**: Führt den konfigurierten Säuberungstyp bei wahrscheinlichen Bedrohungen durch Malware durch.

Hinweis

Sie können diese Option nur auswählen, wenn die Aktion bei Viren-/Malware-Verdacht nicht **übergehen** oder **Zugriff verweigern** ist.

2. Wählen Sie im Abschnitt **Spyware/Grayware** die Aktion aus, die der Security Agent ausführt, nachdem Spyware- oder Grayware-Programme erkannt wurden.

- **Säubern**: Beendet alle zugehörigen Prozesse und löscht zugeordnete Registrierungswerte, Dateien, Cookies und Verknüpfungen.

Hinweis

Nach dem Säubern von Spyware/Grayware sichern die Security Agents Spyware-/Grayware-Daten, die Sie wiederherstellen können, wenn Sie den Zugriff auf die entsprechende Spyware/Grayware für sicher halten.

- **Übergehen**: Protokolliert den Fund, lässt aber die Programmausführung zu.

3. Wählen Sie im Abschnitt **Erweiterte Malware-Erkennung** eine Option aus und konfigurieren Sie die erforderliche Einstellung.

   - **ActiveAction verwenden**: Wählen Sie diese Option, um eine Reihe vorkonfigurierter Suchaktionen auf erkannte portable ausführbare Dateien anzuwenden. Dies ist die empfohlene Option.

     Weitere Informationen finden Sie unter *ActiveAction auf Seite 10-54*.

   - **Verwenden Sie die gleiche Aktion für alle portablen ausführbaren Dateien mit Bedrohungen**: Wählen Sie, um eine der folgenden Aktionen auf erkannte portable ausführbare Dateien anzuwenden.

     - **Quarantäne**: Das System stellt die erkannten portablen ausführbaren Dateien automatisch unter Quarantäne.
     - **Übergehen**: Das System erstellt ein Erkennungsprotokoll, führt jedoch keine Aktion bei erkannten portablen ausführbaren Dateien aus.

Hinweis

Wenn eine erkannte portable ausführbare Datei in der Suchausschlussliste enthalten ist, führt das System keine Aktion an der Datei aus.

Jetzt durchsuchen: Registerkarte "Suchausschluss"

Prozedur

1. Wählen Sie **Suchausschluss aktivieren**.
2. Konfigurieren Sie im Abschnitt **Scan Exclusion List (Directories)** die erforderlichen Einstellungen.
   a. Wählen Sie **Verzeichnisse, in denen Trend Micro Produkte installiert sind, ausschließen**, um Verzeichnisse, die mit anderen Trend Micro-Produkten verbunden sind, automatisch auszuschließen.

      Weitere Informationen finden Sie unter *Trend Micro Produktverzeichnis, Ausschlüsse auf Seite 10-63*.

   b. Geben Sie bei der Konfiguration einer übergeordneten Richtlinie an, wie andere Benutzer untergeordnete Richtlinien konfigurieren können.

      - **Von übergeordnetem Element erben**: Untergeordnete Richtlinien müssen die Einstellungen verwenden, die in der übergeordneten Richtlinie konfiguriert wurden
      - **Von übergeordnetem Element erweitern**: Untergeordnete Richtlinien können zusätzliche Einstellungen an die Einstellungen anhängen, die von der übergeordneten Richtlinie vererbt wurden

      Hinweis

      Wenn Ihre Kinderrichtlinien **Von übergeordnetem Element erweitern** sind, können Sie **Einschränkungen der Kinderpolitik** konfigurieren, um zu verhindern, dass Kinderrichtlinien bestimmte Regeln zur Liste der Ausnahmeregeln hinzufügen.

   c. Geben Sie einen Verzeichnispfad ein, der aus DURCHSUCHEN ausgeschlossen werden soll, und klicken Sie auf die Schaltfläche **+**.

Der Security Agent durchsucht keine Dateien, die sich in dem angegebenen Verzeichnis (und dessen Unterverzeichnissen) befinden.

Hinweis

- Sie können maximal 256 Verzeichnisse angeben, die von der Suche ausgeschlossen werden sollen.
- Verwenden Sie die Schaltflächen **Importieren** und **Exportieren**, um die Liste mit verschiedenen Richtlinien zu teilen.
- Bei Verzeichnisausschlüssen können Platzhalterzeichen verwendet werden.

  Weitere Informationen finden Sie unter *Ausnahmen mit Platzhaltern auf Seite 10-64*.

3. Konfigurieren Sie im Abschnitt **Ausschlussliste für Virensuche (Dateien)** die erforderlichen Einstellungen.

   a. Geben Sie bei der Konfiguration einer übergeordneten Richtlinie an, wie andere Benutzer untergeordnete Richtlinien konfigurieren können.

   - **Von übergeordnetem Element erben**: Untergeordnete Richtlinien müssen die Einstellungen verwenden, die in der übergeordneten Richtlinie konfiguriert wurden
   - **Von übergeordnetem Element erweitern**: Untergeordnete Richtlinien können zusätzliche Einstellungen an die Einstellungen anhängen, die von der übergeordneten Richtlinie vererbt wurden

   b. Geben Sie einen Dateinamen oder den Dateinamen mit dem vollständigen Verzeichnispfad für den Ausschluss aus DURCHSUCHEN ein und klicken Sie auf die Schaltfläche **+**.

Hinweis

- Sie können maximal 256 Dateien angeben, die von der Suche ausgeschlossen werden sollen.
- Verwenden Sie die Schaltflächen **Importieren** und **Exportieren**, um die Liste mit verschiedenen Richtlinien zu teilen.
- Bei Dateiausschlüssen können Platzhalterzeichen verwendet werden.

  Weitere Informationen finden Sie unter *Ausnahmen mit Platzhaltern auf Seite 10-64*.

4. Konfigurieren Sie im Abschnitt **Ausschlussliste für Virensuche (Dateierweiterungen)** die erforderlichen Einstellungen.

   a. Geben Sie bei der Konfiguration einer übergeordneten Richtlinie an, wie andere Benutzer untergeordnete Richtlinien konfigurieren können.

      - **Von übergeordnetem Element erben**: Untergeordnete Richtlinien müssen die Einstellungen verwenden, die in der übergeordneten Richtlinie konfiguriert wurden
      - **Von übergeordnetem Element erweitern**: Untergeordnete Richtlinien können zusätzliche Einstellungen an die Einstellungen anhängen, die von der übergeordneten Richtlinie vererbt wurden

   b. Geben Sie eine Dateierweiterung ein, die aus Durchsuchvorgängen ausgeschlossen werden soll, oder wählen Sie diese aus und klicken Sie auf die Schaltfläche **Hinzufügen >**.

Hinweis

- Sie können maximal 256 Dateierweiterungen angeben, die von der Suche ausgeschlossen werden sollen.
- Verwenden Sie die Schaltflächen **Importieren** und **Exportieren**, um die Liste mit verschiedenen Richtlinien zu teilen.
- Verwenden Sie bei der manuellen Durchsuchen, der zeitgesteuerten Durchsuchen und der sofortigen Durchsuchen ("Jetzt durchsuchen") als Platzhalter ein Fragezeichen (?), um ein einzelnes Zeichen zu ersetzen, oder ein Sternchen (*), um mehrere Zeichen zu ersetzen. Wenn Sie beispielsweise nicht alle Dateien durchsuchen möchten, deren Erweiterung mit "D" beginnt, wie z. B. `DOC`, `DOT` oder `DAT`, geben Sie `D*` oder `D??` ein.

Suchaktionen

Sie können Security Agents für die Verwendung einer Reihe von vordefinierten Suchaktionen oder benutzerdefinierten Aktionen basierend auf dem erkannten Malware-Typ konfigurieren.

Wichtig

Einige Dateien können nicht gesäubert werden.

Weitere Informationen finden Sie unter:

ActiveAction

Unterschiedliche Viren-/Malware-Typen erfordern unterschiedliche Suchaktionen. Unterschiedliche Suchaktionen benutzerdefiniert festzulegen, setzt jedoch grundlegendes Wissen über Viren/Malware voraus und kann äußerst zeitaufwendig sein. Der Security Agent verwendet ActiveAction, um diesen Problemen entgegenzuwirken.

In ActiveAction sind mehrere bereits vorkonfigurierte Aktionen für die Suche nach Viren/Malware zusammengefasst. ActiveAction sollten Sie verwenden, wenn Sie mit der Konfiguration von Suchaktionen nicht vertraut sind oder nicht genau wissen, welche Suchaktion sich für einen bestimmten Viren-/Malware-Typ am besten eignet.

Welche Vorteile bietet die Verwendung von ActiveAction?

- ActiveAction verwendet von Trend Micro empfohlene Suchaktionen. Der zeitliche Aufwand für die Konfiguration der Suchaktionen entfällt dadurch.
- Die Angriffsstrategien der Viren/Malware gegen Endpunkte ändern sich permanent. Die ActiveAction Einstellungen werden aktualisiert, um vor den neuesten Bedrohungen und Methoden von Viren-/Malware-Angriffen zu schützen.

Die folgende Tabelle zeigt, wie ActiveAction mit den jeweiligen Viren-/Malware-Typen verfährt.

Tabelle 10-2. Von Trend Micro empfohlene Suchaktionen gegen Viren und Malware

Viren-/Malware-Typ	Echtzeitsuche		Manuelle Suche/ Zeitgesteuerte Suche	
	Erste Aktion	Zweite Aktion	Erste Aktion	Zweite Aktion
CVE-Schwachstelle	Bestanden	n. v.	n. v.	n. v.
Scherzprogramm	Quarantäne	n. v.	Quarantäne	n. v.
Trojaner	Quarantäne	n. v.	Quarantäne	n. v.
Virus	Säubern	Quarantäne	Säubern	Quarantäne
Testviren	Zugriff verweigern	n. v.	Übergehen	n. v.
Packer	Quarantäne	n. v.	Quarantäne	n. v.
Andere	Säubern	Quarantäne	Säubern	Quarantäne

Viren-/Malware-Typ	Echtzeitsuche		Manuelle Suche/ Zeitgesteuerte Suche	
	Erste Aktion	Zweite Aktion	Erste Aktion	Zweite Aktion
Mögliche Malware	Bestanden	n. v.	Übergehen oder vom Benutzer konfigurierte Aktion	n. v.

Hinweis

- Die Standardaktion bei Viren-/Malware-Verdacht ist „Zugriff verweigern“ während einer Echtzeitsuche und „Übergehen“ während einer manuellen Suche und einer zeitgesteuerten Suche. Sind das nicht Ihre bevorzugten Aktionen, können Sie sie ändern in „Quarantäne“, „Löschen“ oder „Umbenennen“.
- Einige Dateien können nicht gesäubert werden.
- ActiveAction ist nicht für die Suche nach Spyware/Grayware verfügbar.

Aktionen bei der benutzerdefinierten Suche

Aktion	Beschreibung
Löschen	Die infizierte Datei wird gelöscht.
Quarantäne	Die infizierte Datei wird umbenannt und anschließend in den temporären Quarantäne-Ordner auf dem Endpunkt verschoben. Der Security Agent sendet unter Quarantäne gestellte Dateien anschließend an den festgelegten Quarantäne-Ordner, der sich standardmäßig auf dem Verwaltungsserver befindet. Der Security Agent verschlüsselt unter Quarantäne gestellte Dateien, die an dieses Verzeichnis gesendet werden. Weitere Informationen finden Sie unter *Quarantäne-Verzeichnis auf Seite 10-57*.

Aktion	Beschreibung
Säubern	Die infizierte Datei wird gesäubert, bevor der vollständige Zugriff möglich ist. Lässt sich die Datei nicht säubern, führt der Security Agent eine zweite Aktion durch, bei der es sich um eine der folgenden Aktionen handeln kann: „Quarantäne“, „Löschen“, „Umbenennen“ und „Übergehen“. Diese Aktion kann auf alle Arten von Sicherheitsbedrohungen angewendet werden, außer auf wahrscheinliche Viren/Malware. **Hinweis** Einige Dateien lassen sich nicht säubern. Weitere Informationen finden Sie unter *Dateien, die nicht gesäubert werden können auf Seite 10-59*
Umbenennen	Die Erweiterung der infizierten Datei wird in `vir` geändert. Der Benutzer kann die umbenannte Datei erst öffnen, wenn sie mit einer bestimmten Anwendung verknüpft wird. Beim Öffnen der umbenannten, infizierten Datei wird der Virus/die Malware möglicherweise ausgeführt.
Bestanden	Führt keine Aktion für die erkannten Bedrohungen aus. Das erkannte Risiko wird jedoch in den Protokolldateien verzeichnet.
Zugriff verweigern	Entdeckt der Security Agent einen Versuch, eine infizierte Datei zu öffnen oder auszuführen, wird dieser Vorgang umgehend gesperrt. Die infizierte Datei kann manuell gelöscht werden.

Quarantäne-Verzeichnis

Wenn es sich bei der Aktion für eine infizierte Datei um "Quarantäne" handelt, wird die Datei vom Security Agent verschlüsselt und in den temporären Quarantäne-Ordner verschoben, der sich im Ordner <Installationsordner des Agents>\SUSPECT befindet. Anschließend wird die Datei in das vorgesehene Quarantäne-Verzeichnis verschoben.

Hinweis

Sie können die verschlüsselten Dateien in der Quarantäne wiederherstellen, falls Sie zu einem späteren Zeitpunkt darauf zugreifen möchten.

Übernehmen Sie den Quarantäne-Ordner, der sich standardmäßig auf dem Apex One Server-Computer befindet. Das Verzeichnis ist im URL-Format angegeben und enthält den Hostnamen oder die IP-Adresse des Servers.

- Verwaltet der Server sowohl IPv4- als auch IPv6-Agents verwenden Sie den Hostnamen, damit alle Security Agents in Quarantäne verschobene Dateien an den Server senden können.
- Hat der Server nur eine IPv4-Adresse oder wird über sie identifiziert, können nur reine IPv4- und Dual-Stack-Security Agents Quarantäne-Dateien an den Server senden.
- Hat der Server nur eine IPv6-Adresse oder wird über sie identifiziert, können nur reine IPv6- und Dual-Stack-Security Agents Quarantäne-Dateien an den Server senden.

Sie können auch einen alternativen Quarantäne-Ordner festlegen, indem Sie den Speicherort als URL, UNC-Pfad oder absoluten Dateipfad eingeben. Security Agents sollten eine Verbindung zu diesem alternativen Verzeichnis aufbauen können. Das alternative Verzeichnis sollte beispielsweise eine IPv6-Adresse haben, wenn es Quarantäne-Dateien von den Dual-Stack-Agents und den reinen IPv6-Security Agents empfangen soll. Trend Micro empfiehlt die Benennung eines alternativen Dual-Stack-Verzeichnisses, die Identifizierung des Verzeichnisses nach seinem Host-Namen und die Verwendung eines UNC-Pfads bei Eingabe des Verzeichnisses.

In der folgenden Tabelle finden Sie eine Anleitung zur Verwendung von URLs, UNC-Pfaden oder absoluten Dateipfaden:

TABELLE 10-3. Quarantäne-Ordner

QUARANTÄNE-ORDNER	KOMPATIBLES FORMAT	BEISPIEL	HINWEISE
Ein Verzeichnis auf dem Verwaltungsserver-Computer	URL	`http://<osceserver>`	Dabei handelt es sich um das Standardverzeichnis. Sie können die Einstellungen für dieses Verzeichnis konfigurieren, z. B. die Größe des Quarantäne-Ordners.
	UNC-Pfad	`\\<osceserver>\ofcscan\Virus`	
Ein Verzeichnis auf einem anderen Apex One Server-Computer (falls sich in Ihrem Netzwerk andere Apex One Server befinden)	URL	`http://<osceserver2>`	Vergewissern Sie sich, dass Security Agents eine Verbindung zu diesem Verzeichnis aufbauen können. Bei Angabe eines ungültigen Verzeichnisses behält der Security Agent die unter Quarantäne gestellten Dateien im Ordner "SUSPECT", bis ein gültiger Quarantäne-Ordner angegeben wird. Im Viren-/Malware-Protokoll des Servers lautet das Suchergebnis "Die Datei konnte nicht in den festgelegten Quarantäne-Ordner verschoben werden". Wenn Sie einen UNC-Pfad verwenden, stellen Sie sicher, dass der Quarantäne-Ordner für die Gruppe "Alle" freigegeben ist und dass Sie dieser Gruppe Lese- und Schreibberechtigungen zugewiesen haben.
	UNC-Pfad	`\\<osceserver2>\ofcscan\Virus`	
Ein anderer Endpunkt im Netzwerk	UNC-Pfad	`\\<computer_name>\temp`	
Ein anderes Verzeichnis auf dem Security Agent	Absoluter Pfad	`C:\temp`	

Dateien, die nicht gesäubert werden können

Die Viren-Scan-Engine kann folgende Dateien nicht säubern:

Tabelle 10-4. Lösungen bei nicht zu säubernden Dateien

Nicht zu säubernde Datei	Erklärung und Lösung
Mit Trojanern infizierte Dateien	Trojaner sind Programme, die unerwartete oder unberechtigte, in der Regel aber schädliche Aktionen durchführen. Es werden beispielsweise Meldungen angezeigt, Dateien gelöscht oder Festplatten formatiert. Da Trojaner keine Dateien infizieren, ist kein Säubern erforderlich. Lösung: Die Damage Cleanup Engine und die Damage Cleanup Template entfernen Trojaner.
Mit Würmern infizierte Dateien	Ein Wurm ist ein eigenständiges Programm (oder eine Gruppe von Programmen), das funktionsfähige Kopien von sich selbst oder seinen Segmenten an andere Endpunktsysteme verteilen kann. Würmer verbreiten sich normalerweise über Netzwerkverbindungen oder E-Mail-Anhänge. Würmer sind eigenständige Programme und können deshalb nicht gesäubert werden. Lösung: Trend Micro empfiehlt, Würmer zu löschen.
Infizierte, schreibgeschützte Dateien	Lösung: Heben Sie den Schreibschutz auf, damit die Datei gesäubert werden kann.
Kennwortgeschützte Dateien	Kennwortgeschützte Dateien umfassen kennwortgeschützte, komprimierte Dateien oder kennwortgeschützte Microsoft Office-Dateien. Lösung: Heben Sie den Kennwortschutz auf, damit die Datei gesäubert werden kann.
Sicherungsdateien	Bei Dateien mit den Erweiterungen RB0~RB9 handelt es sich um Sicherungskopien infizierter Dateien. Beim Säuberungsprozess werden diese Kopien für den Fall erstellt, dass der Virus/die Malware die infizierte Datei beim Säubern beschädigt. Lösung: Wenn die Datei gesäubert werden konnte, müssen Sie die Sicherungskopie der infizierten Datei nicht aufbewahren. Wenn der Endpunkt fehlerfrei funktioniert, können Sie die Sicherungskopie löschen.
Infizierte Dateien im Papierkorb	Infizierte Dateien im Papierkorb des Systems können möglicherweise nicht entfernt werden, wenn das System aktiv ist.

Nicht zu säubernde Datei	Erklärung und Lösung
	1. Melden Sie sich bei dem Endpunkt als Administrator an. 2. Schließen Sie alle aktiven Anwendungen, damit die Datei nicht gesperrt wird. Windows könnte sie sonst nicht löschen. 3. Öffnen Sie ein Eingabeaufforderungsfenster. 4. Geben Sie zum Löschen der Dateien folgende Befehle ein: `del /s \$Recycle.Bin\*` 5. Überprüfen Sie, ob die Dateien entfernt wurden.
Infizierte Dateien im Windows Ordner "Temp" oder im Internet Explorer-Ordner "Temporary Internet Files"	Infizierte Dateien in diesen Ordnern können möglicherweise nicht gesäubert werden, da sie vom Endpunkt verwendet werden. Möglicherweise handelt es sich bei den Dateien, die gesäubert werden sollen, um temporäre Dateien, die für den Betrieb von Windows benötigt werden.
	1. Melden Sie sich bei dem Endpunkt als Administrator an. 2. Schließen Sie alle aktiven Anwendungen, damit die Datei nicht gesperrt wird. Windows könnte sie sonst nicht löschen. 3. Wenn sich die infizierte Datei im Windows Ordner "Temp" befindet: a. Öffnen Sie ein Eingabeaufforderungsfenster. b. Geben Sie zum Löschen der Dateien folgende Befehle ein: `del /s \Windows\Temp\*` c. Starten Sie den Endpunkt im Normalmodus neu. 4. Wenn sich die infizierte Datei im tempoären Ordner von Internet Explorer befindet: a. Öffnen Sie eine Eingabeaufforderung und navigieren Sie zum Internet Explorer-Ordner "Temp". • Windows 7: `%LocalAppData%\Microsoft\Windows\Temporary Internet Files` • Windows 8/8.1: `%LocalAppData%\Microsoft\Windows\INetCache`

Nicht zu säubernde Datei	Erklärung und Lösung
	• Windows 10: `%LocalAppData%\Microsoft\Windows\INetCache\IE` b. Geben Sie zum Löschen der Dateien folgende Befehle ein: `del /s .\*` Mit dem letzten Befehl werden alle Dateien im temporären Ordner des Internet Explorers gelöscht. c. Starten Sie den Endpunkt im Normalmodus neu.
Dateien, die mit einem unbekannten Komprimierungs-Tool bearbeitet wurden.	Lösung: Dekomprimieren Sie die Dateien.
Gesperrte Dateien oder Dateien, die gerade ausgeführt werden.	Lösung: Entsperren Sie die Dateien oder warten Sie, bis die Dateien ausgeführt wurden.
Beschädigte Dateien.	Lösung: Löschen Sie die Dateien.

Mit Trojanern infizierte Dateien

Trojaner sind Programme, die unerwartete oder unberechtigte, in der Regel aber schädliche Aktionen durchführen. Es werden beispielsweise Meldungen angezeigt, Dateien gelöscht oder Festplatten formatiert. Da Trojaner keine Dateien infizieren, ist kein Säubern erforderlich.

Lösung: Der Security Agent entfernt Trojaner mit Hilfe der Damage Cleanup Engine und der Damage Cleanup Template.

Mit Würmern infizierte Dateien

Ein Wurm ist ein eigenständiges Programm (oder eine Gruppe von Programmen), das funktionsfähige Kopien von sich selbst oder seinen Segmenten an andere endpunkt-Systeme verteilen kann. Würmer verbreiten sich normalerweise über Netzwerkverbindungen oder E-Mail-Anhänge.

Würmer sind eigenständige Programme und können deshalb nicht gesäubert werden.

Lösung: Trend Micro empfiehlt, Würmer zu löschen.

Infizierte, schreibgeschützte Dateien

Lösung: Heben Sie den Schreibschutz auf, damit der Security Agent die Datei säubern kann.

Kennwortgeschützte Dateien

Umfasst kennwortgeschützte komprimierte Dateien oder kennwortgeschützte Microsoft Office Dateien.

Lösung: Heben Sie den Kennwortschutz auf, damit Security Agent diese Dateien säubern kann.

Sicherungsdateien

Bei Dateien mit den Erweiterungen RB0~RB9 handelt es sich um Sicherungskopien infizierter Dateien. Der Security Agent erstellt eine Sicherungskopie der infizierten Datei, für den Fall, dass der Virus bzw. die Malware die Datei während des Säuberungsvorgangs beschädigt hat.

Lösung: Wenn die infizierte Datei von Security Agent gesäubert werden konnte, muss die Sicherungskopie nicht aufbewahrt werden. Wenn der Endpunkt fehlerfrei funktioniert, können Sie die Sicherungskopie löschen.

Unterstützung der Suchausschlüsse

Informationen zum Ausschließen von Verzeichnissen und Dateien aus der Anti-Malware-Suche finden Sie in folgendem Referenzmaterial:

Trend Micro Produktverzeichnis, Ausschlüsse

Wenn Sie **Installationsverzeichnisse von Trend Micro Produkten ausschließen** im Abschnitt **Ausschlussliste für Virensuche (Verzeichnisse)** auswählen, schließt der Security Agent automatisch die folgenden Produktverzeichnisse aus:

- <Installationsordner des Servers>
- IM Security
- InterScan eManager 3.5x
- InterScan Web Security Suite
- InterScan Web Protect
- InterScan FTP VirusWall
- InterScan Web VirusWall
- InterScan NSAPI Plug-in
- InterScan E-mail VirusWall
- ScanMail eManager™ 3.11, 5.1, 5.11, 5.12
- ScanMail for Lotus Notes™ eManager NT
- ScanMail™ für Microsoft Exchange

Ausnahmen mit Platzhaltern

Die Suchausschlusslisten für Dateien und Verzeichnisse unterstützen die Verwendung von Platzhalterzeichen. Verwenden Sie als Platzhalterzeichen das "?", um ein Zeichen zu ersetzen, und das "*", um mehrere Zeichen zu ersetzen.

Setzen Sie Platzhalterzeichen mit Bedacht ein. Bei der Verwendung des falschen Zeichens können Dateien und Verzeichnisse ausgeschlossen werden, die eigentlich eingeschlossen werden sollten. Beispielsweise wird durch Hinzufügen von `C:\*` zur Ausschlussliste für Virensuche (Dateien) das gesamte Laufwerk `C:\` ausgeschlossen.

TABELLE 10-5. Ausschlüsse von der Suche mit Platzhalterzeichen

WERT	AUSGESCHLOSSEN	NICHT AUSGESCHLOSSEN

`c:\director*\fil\*.txt`	`c:\directory\fil\doc.txt`
	`c:\directories\fil\files\document.txt`
		`c:\directory\file\`
		`c:\directories\files\`
		`c:\directory\file\doc.txt`
		`c:\directories\files\document.txt`

`c:\director?\file\*.txt`	`c:\directory\file\doc.txt`	`c:\directories\file\document.txt`
`c:\director?\file\?.txt`	`c:\directory\file\1.txt`	`c:\directory\file\doc.txt` `c:\directories\file\document.txt`
`c:\*.txt`	Alle `.txt`-Dateien im `C:\`-Verzeichnis	Alle anderen Dateitypen im `C:\`-Verzeichnis
`[]`	Nicht unterstützt	Nicht unterstützt

Kapitel 11

Einstellungen der Web-Reputation-Richtlinie

In diesem Abschnitt wird beschrieben, wie Web-Reputation-Richtlinien für Security Agents konfiguriert werden.

Es werden folgende Themen behandelt:

- *Web Reputation auf Seite 11-2*
- *Eine Web-Reputation-Richtlinie konfigurieren auf Seite 11-2*

Web Reputation

Die Web-Reputation-Technologie bewertet die Glaubwürdigkeit von Webdomänen nach einem Scoring-Verfahren, indem Informationen wie das Alter einer Website, historische Änderungen des Speicherorts und Anzeichen von verdächtigen Aktivitäten zurückverfolgt werden, die durch die Malware-Verhaltensanalyse entdeckt wurden. Trend Micro analysiert ständig Websites und aktualisiert Web-Reputation-Bewertungen, um zu verhindern, dass Benutzer auf potenziell bösartige Inhalte zugreifen.

Wenn ein Benutzer versucht, auf eine Website zuzugreifen, fragt der Security Agent eine Smart Protection Quelle ab, um die Risikostufe des Inhalts zu ermitteln. Die konfigurierte Web-Reputation-Richtlinie für den Security Agent bestimmt, ob der Zugriff auf die Website zulässig ist.

Web Reputation ermöglicht Ihnen das Hinzufügen von Websites zu Listen zulässiger oder gesperrter Websites, die Sie als sicher oder gefährlich erachten. Der Security Agent fragt keine Web-Reputation-Bewertungen für Websites ab, die den Listen hinzugefügt wurden, sondern sperrt stattdessen den Zugriff automatisch oder lässt ihn zu.

Eine Web-Reputation-Richtlinie konfigurieren

Legen Sie die Anmeldedaten zur Proxy-Server-Authentifizierung fest, wenn die HTTP-Kommunikation in Ihrem Unternehmen über den Proxy-Server erfolgt und eine Authentifizierung vor dem Internet-Zugriff erforderlich ist.

Prozedur

1. Klicken Sie auf die Registerkarte **Externe Agents**, um eine Richtlinie für externe Agents zu konfigurieren, oder auf die Registerkarte **Interne Agents**, um eine Richtlinie für interne Agents zu konfigurieren.
2. Wählen Sie unter **Web Reputation unter den folgenden Betriebssystemen aktivieren** die Arten der zu schützenden Windows-Plattformen aus (**Windows Desktop-Plattformen** und **Windows Server-Plattformen**).

Tipp

Trend Micro empfiehlt, Web Reputation für interne Agents zu deaktivieren, wenn Sie bereits ein Trend Micro Produkt mit einer Web Reputation-Funktion (z. B. InterScan Web Security Virtual Appliance) verwenden.

3. Wählen Sie **Bewertungsmodus aktivieren** aus.

Hinweis

Gestatten Sie Security Agents den Zugriff auf alle Websites, wenn Sie sich im Bewertungsmodus befinden. Für alle besuchten Websites, die gegen die konfigurierte Einstellung für die **Sicherheitsstufe** verstoßen, protokolliert der Security Agent das Ereignis. Im Bewertungsmodus können Sie den Websitezugriff überwachen und die Sicherheit von Websites bewerten, bevor Sie den Benutzerzugriff aktiv sperren. Anhand der Bewertung in den Zugriffsprotokollen können Sie vertrauenswürdige Websites zur Liste der zulässigen URLs hinzufügen, bevor Sie den Bewertungsmodus deaktivieren.

4. Wählen Sie **HTTPS-URLs prüfen** aus.

Wichtig

- Die HTTPS-URL-Suchfunktion unterstützt auch das HTTP/2-Protokoll. Bevor Web Reputation HTTPS- oder HTTP/2-URLs prüfen kann, müssen Sie als Voraussetzung einige Einstellungen für verschiedene Browser konfigurieren.

  Weitere Informationen finden Sie unter *Unterstützung der HTTPS-URL-Suche auf Seite 11-8*.

- Ab Trend Micro Apex One Security Agent14.0.20315 und später wird durch Aktivieren der Option **HTTPS-URLs prüfen** die Trend Micro Toolbar für die Enterprise-Browser-Erweiterung auf Endpunkten mit Google Chrome und Microsoft Edge heruntergeladen und installiert. Die Browser-Erweiterung hilft, Sicherheitsfunktionen zu verbessern, wie das Blockieren von URLs und URLs, die Ihrer Liste verdächtiger Objekte hinzugefügt wurden.

  Die Trend Micro Toolbar für Unternehmen unterstützt nur Google Chrome und Microsoft Edge auf Windows 64-Bit-Endpunkten. Die Browser-Erweiterung unterstützt Windows Server 2008 R2 (64-Bit) nicht.

  Die Browser-Erweiterung verwendet die folgenden Dienste, um mit dem Security Agent zu kommunizieren:

  - Trend Micro Netzwerkdienst (tm_netsrv.exe)
  - Trend Micro Web Reputation App (dsa-wrs-app.exe)

5. Wählen Sie **Nur gängige HTTP-Ports durchsuchen**, um die Web Reputation-Suche auf die Ports 80, 81 und 8080 zu beschränken. Standardmäßig durchsucht Web Reputation den gesamten Datenverkehr auf allen Ports.

Hinweis

Nicht unterstützt unter Windows 7, 8, 8.1, 10 oder Windows Server 2008 R2, 2012 oder höheren Plattformen.

6. Wählen Sie für interne Security Agents die Option **Abfragen an Smart Protection Server senden** aus, wenn Security Agents Web Reputation-Abfragen an Smart Protection Server senden sollen.

   - Wenn Sie diese Option aktivieren:
     - Agents ermitteln anhand der Liste der Smart Protection Quelle den Smart Protection Server, an den sie ihre Abfragen senden.
     - Vergewissern Sie sich, dass die Smart Protection Server verfügbar sind. Wenn keiner der Smart Protection Server verfügbar ist, senden die Agents Abfragen an das Smart Protection Network und verweisen auf genehmigte und gesperrte URL-Listen.
     - Nicht getestete Websites werden von den Agents nicht gesperrt. Die Smart Protection Server speichern keine Web Reputation-Daten für diese Websites.
   - Wenn Sie diese Option deaktivieren:
     - Agents senden Web Reputation-Abfragen an das Smart Protection Network. Endpunkte benötigen eine Internetverbindung für den erfolgreichen Versand von Abfragen.
     - Nicht getestete Websites werden von Agents gesperrt, wenn Sie **Seiten sperren, die nicht von Trend Micro getestet wurden** auswählen.

Hinweis

Sie können nur interne lokale Security Agents konfigurieren, um Web Reputation-Abfragen an lokale Smart Protection Server zu senden.

7. Wählen Sie unter den vorhandenen Web Reputation-Sicherheitsstufen aus: **Hoch**, **Mittel** oder **Niedrig**

Hinweis

Die Sicherheitsstufen legen fest, ob Web Reputation den Zugriff auf eine URL zulässt oder sperrt. Wenn zum Beispiel die Sicherheitsstufe auf "Niedrig" festgelegt ist, sperrt Web Reputation nur URLs, die als Internetbedrohung bekannt sind. Bei einer Erhöhung der Sicherheitsstufe verbessert sich die Erkennungsrate von Internet-Bedrohungen, doch gleichzeitig steigt auch die Wahrscheinlichkeit von Fehlalarmen.

8. Wenn Sie die Option **Abfragen an Smart Protection Server senden** deaktiviert haben, können Sie **Seiten sperren, die nicht von Trend Micro getestet wurden** auswählen.

Hinweis

Obwohl Trend Micro Websites aktiv auf deren Sicherheit testet, ist es möglich, dass Benutzer auf ungetestete Websites treffen, wenn diese neu sind oder seltener besucht werden. Das Sperren ungetesteter Sites kann die Sicherheit erhöhen, doch es kann auch dazu führen, dass der Zugriff auf sichere Sites gesperrt wird.

9. Wählen Sie **Seiten mit bösartigem Skript sperren**, um Webbrowser-Schwachstellen und bösartige Skripts zu identifizieren und die Gefährdung des Webbrowsers durch diese Bedrohungen zu verhindern.

   Web Reputation verwendet sowohl das Pattern zur Erkennung von Browser-Schwachstellen als auch das Pattern der Skriptanalyse, um Webseiten zu identifizieren und zu sperren, bevor das System gefährdet wird.

Wichtig

- Die Funktion Browser-Exploit-Schutz unterstützt nur die Analyse des HTTP-Datenverkehrs für die Browser Microsoft Edge Legacy, Microsoft Edge Chromium, Mozilla Firefox und Chrome.
- Für die Funktion zur Verhinderung von Browser-Schwachstellen müssen Sie den erweiterten Schutzdienst aktivieren.

10. Konfigurieren Sie die Liste der zulässigen und gesperrten Absender.

Hinweis

Die Liste der zulässigen URLs hat Vorrang vor der Liste der gesperrten URLs. Wenn eine URL einem Eintrag in der Liste der zulässigen URLs entspricht, gewähren die Agents stets Zugriff, selbst wenn sie sich in der Liste der gesperrten URLs befindet.

a. Wählen Sie **Liste 'Zulässig/Gesperrt' aktivieren** aus.

b. Geben Sie einen URL ein.

   Sie können an jeder Stelle im Link ein Platzhalterzeichen (*) verwenden.

   Beispiel:

   - Wenn Sie `www.trendmicro.com/*` eingeben, bedeutet das, dass Web Reputation alle Seiten der Website von Trend Micro zulässt.
   - Wenn Sie `*.trendmicro.com/*` eingeben, bedeutet das, dass Web Reputation alle Seiten in jeder Unterdomäne von `trendmicro.com` zulässt.

   Sie können URLs eingeben, die IP-Adressen enthalten. Wenn Sie einen URL eingeben, der eine IPv6-Adresse enthält, setzen Sie die Adresse in Klammern.

c. Klicken Sie auf **Zur Liste der zulässigen URLs hinzufügen** oder **Zur Liste der gesperrten URLs hinzufügen**.

Wichtig

Web Reputation durchsucht keine Adressen in der Liste der zulässigen und gesperrten URLs.

11. Um einen Kommentar zu Web Reputation abzugeben, klicken Sie auf den entsprechenden Link unter **Neubewertung URL**. Das Trend Micro Web Reputation Hilfesystem wird in einem Browser-Fenster geöffnet.
12. Wählen Sie, ob der Security Agent Web Reputation-Protokolle an den Server senden darf. Gestatten Sie Agents das Senden von Protokollen, wenn Sie die von Web Reputation gesperrten URLs analysieren und bei als sicher eingestuften URLs eine entsprechende Aktion durchführen möchten.

Unterstützung der HTTPS-URL-Suche

HTTPS-Kommunikation verwendet Zertifikate zum Identifizieren von Webservern. Sie verschlüsselt Daten, um Datendiebstahl und Abhörvorgänge zu verhindern. Obwohl HTTPS beim Zugriff auf Websites mehr Schutz bietet, verbleiben bei der Nutzung Risiken. Sites, die von Hackern übernommen wurden, können trotz gültiger Zertifikate Malware anbieten und persönliche Daten stehlen. Außerdem sind Zertifikate relativ einfach zu beschaffen, wodurch sich das Einrichten bösartiger Webserver, die HTTPS nutzen, einfach gestaltet.

Aktivieren Sie das Prüfen von HTTPS-URLs, um die Gefährdung durch infizierte und bösartige Websites, die HTTPS verwenden, zu verringern. Web Reputation kann HTTPS-Datenverkehr auf den folgenden Browsern überwachen:

TABELLE 11-1. Browser, die den HTTPS-Datenverkehr unterstützen

BROWSER	VERSION	VORAUSSETZUNGEN
Mozilla Firefox	3.5 oder höher	Keiner
Chrome	Aktuelle Version	
Microsoft Edge	• Legacy	

Browser	Version	Voraussetzungen
	• Chromium	

Kapitel 12

Schutz vor unbekannten Bedrohungen

In diesem Abschnitt wird beschrieben, wie Sie Security Agents konfigurieren können, um zuvor unerkannte, gezielte oder selten vorkommende Bedrohungen zu erkennen und davor zu schützen.

Es werden folgende Themen behandelt:

- *Vorausschauendes Maschinenlernen auf Seite 12-2*
- *Konfigurieren der Einstellungen für die Exemplar Zusendung auf Seite 12-8*
- *Verdächtige Verbindungseinstellungen konfigurieren auf Seite 12-8*

Vorausschauendes Maschinenlernen

Das Trend Micro Vorausschauendes Maschinenlernen setzt moderne Technologien ein, um Bedrohungsinformationen zu korrelieren und ausführliche Dateianalysen durchzuführen und so unbekannte neue Sicherheitsrisiken durch digitale DNS-Fingerabdrücke, API-Zuordnung und weitere Funktionen zu erkennen. Beim 'Vorausschauendes Maschinenlernen' wird außerdem eine Verhaltensanalyse für unbekannte Prozesse oder Prozesse mit geringer Prävalenz durchgeführt, um zu ermitteln, ob eine neue oder unbekannte Bedrohung versucht, das Netzwerk zu infizieren.

Beim 'Vorausschauendes Maschinenlernen' handelt es sich um ein leistungsstarkes Tool, mit dem Ihre Umgebung vor unbekannten und Zero-Day-Angriffen geschützt wird.

Das Überwachungsniveau ist der Grad der Wachsamkeit und Strenge, der bei der Erkennung und Reaktion auf mögliche Bedrohungen angewendet wird. Eine Erhöhung des Niveaus steigert die Empfindlichkeit des Sensors, was die Anzahl der Erkennungen und Warnungen erhöht. Höhere Niveaus ermöglichen eine strengere Überwachung, um bei Situationen wie laufenden Bedrohungsuntersuchungen zu helfen, können jedoch eine große Anzahl nicht wesentlicher Protokolle erzeugen und die Leistung des Endpunkts beeinträchtigen. Trend Micro empfiehlt, das Überwachungsniveau auf 2 - Moderat einzustellen, um relevantere Daten mit minimaler Auswirkung auf Ihre Endpunkte auszugleichen. Einige Komponenten, die von höheren Überwachungsniveaus verwendet werden, sind nicht auf allen Plattformen verfügbar.

Fundtyp	Beschreibung
Datei	Nach der Erkennung einer unbekannten oder selten vorkommenden Datei durchsucht der Security Agent die Datei mit Hilfe der Funktion "Fortgeschrittene Bedrohungssuchmaschine", um Dateifunktionen zu extrahieren, und sendet den Bericht an das Modul "Vorausschauendes Maschinenlernen", das im Trend Micro Smart Protection Network gehostet wird. Durch die Verwendung von Malware-Modellen wird beim 'Vorausschauendes Maschinenlernen' das Beispiel mit dem Malware-Modell verglichen, ein Wahrscheinlichkeitswert zugewiesen und der mögliche Malware-Typ ermittelt, der in der Datei enthalten ist. Falls keine funktionierende Internetverbindung verfügbar ist, wechselt die Funktion "Vorausschauendes Maschinenlernen" automatisch zum lokalen Modell, um bei Bedrohungen durch portable ausführbare Dateien dauerhaften Schutz vor unbekannten Bedrohungen zu bieten. Je nach Konfiguration der Funktion "Vorausschauendes Maschinenlernen" kann der Security Agent versuchen, die betroffene Datei unter „Quarantäne“ zu stellen, um zu verhindern, dass sich die Bedrohung im Netzwerk verbreitet.

Fundtyp	Beschreibung
Prozess	Nach der Erkennung eines unbekannten oder selten vorkommenden Prozesses überwacht der Security Agent diesen Prozess mit Hilfe der Funktion "Maschine für kontextbezogene Intelligenz" und sendet den Verhaltensbericht an das Modul "Vorausschauendes Maschinenlernen". Durch die Verwendung von verhaltensbezogenen Malware-Modellen wird beim 'Vorausschauendes Maschinenlernen' das Prozessverhalten mit dem Modell verglichen, ein Wahrscheinlichkeitswert zugewiesen und der mögliche Malware-Typ ermittelt, der vom Prozess ausgeführt wird. Die Prozesserkennung überwacht auch die Ausführung des Skripts. Wenn die "Maschine für kontextbezogene Intelligenz" die Ausführung eines verdächtigen Skripts erkennt, führt die Funktion "Vorausschauendes Maschinenlernen" die konfigurierte Aktion durch. Die Funktion "Vorausschauendes Maschinenlernen" führt die Sperrung von Skripts für die folgenden Arten von Skripts durch: • Cscript • JAR • PowerShell • VBS • WScript Je nach Konfiguration der Funktion "Vorausschauendes Maschinenlernen" kann Security Agent den betroffenen Prozess oder das Skript „beenden“ und die Datei bereinigen, die den Prozess oder das Skript ausgeführt hat.

Konfigurieren der Einstellungen für das Vorrausschaunde Maschinenlernen

Hinweis

Folgende Dienste müssen für "Vorausschauendes Maschinenlernen" aktiviert werden:

- Schutz vor unbefugten Änderungen
- Erweiterter Schutzdienst

Prozedur

1. Wählen Sie **Vorausschauendes Maschinenlernen aktivieren** aus.
2. Konfigurieren Sie die **Überwachungsstufe**-Einstellungen für **Erkennung** und **Prävention**.

Wichtig

- Höhere Überwachungsstufen bieten eine größere Sensibilität, können jedoch eine große Anzahl nicht wesentlicher Protokolle erzeugen und die Leistung des Endpunkts beeinträchtigen. Trend Micro empfiehlt, **2 - Mäßig** auszuwählen, um relevantere Daten mit minimalen Auswirkungen auf Ihre Endpunkte zu erhalten.
- Die **Prävention**-Stufe muss gleich oder niedriger als **Erkennung** sein.

3. Wählen Sie unter **Erkennungseinstellungen** den Erkennungstyp und die zugehörige Aktion aus, die von "Vorausschauendes Maschinenlernen" durchgeführt wird.

Erkennungstyp	Aktionen
Datei	• **Quarantäne**: Wählen Sie diese Option aus, um Dateien automatisch unter Quarantäne zu stellen, die basierend auf der Analyse von "Vorausschauendes Maschinenlernen" mit Malware in Verbindung stehende Funktionen aufweisen. • **Nur protokollieren**: Wählen Sie diese Option aus, um unbekannte Dateien zu durchsuchen und die Analyse von "Vorausschauendes Maschinenlernen" zur weiteren internen Überprüfung der Bedrohung zu protokollieren.
Prozess	• **Beenden**: Wählen Sie diese Option aus, um Prozesse oder Skripts automatisch zu beenden, die basierend auf der Analyse von "Vorausschauendes Maschinenlernen" mit Malware in Verbindung stehendes Verhalten aufweisen. **Wichtig** Mit Hilfe der Funktion "Vorausschauendes Maschinenlernen" wird versucht, die Dateien zu bereinigen, die böswillige Prozesse oder Skripts ausgeführt haben. Wenn die Bereinigungsaktion nicht erfolgreich ist, verschiebt "Vorausschauendes Maschinenlernen" die betroffenen Dateien in die Quarantäne. • **Nur protokollieren**: Wählen Sie diese Option aus, um nach unbekannten Prozessen oder Skripts zu suchen und die Analyse von "Vorausschauendes Maschinenlernen" zur weiteren internen Überprüfung der Bedrohung zu protokollieren.

4. Konfigurieren Sie unter **Ausnahmen** die globalen Dateiausnahmen für "Vorausschauendes Maschinenlernen", um alle Agents daran zu hindern, eine Datei als böswillig zu erkennen.

   a. Geben Sie bei der Konfiguration einer übergeordneten Richtlinie an, wie andere Benutzer untergeordnete Richtlinien konfigurieren können.

- **Von übergeordnetem Element erben**: Untergeordnete Richtlinien müssen die Einstellungen verwenden, die in der übergeordneten Richtlinie konfiguriert wurden
- **Von übergeordnetem Element erweitern**: Untergeordnete Richtlinien können zusätzliche Einstellungen an die Einstellungen anhängen, die von der übergeordneten Richtlinie vererbt wurden

Hinweis

Wenn Ihre Kinderrichtlinien **Von übergeordnetem Element erweitern** sind, können Sie **Einschränkungen der Kinderpolitik** konfigurieren, um zu verhindern, dass Kinderrichtlinien bestimmte Regeln zur Liste der Ausnahmeregeln hinzufügen.

b. Klicken Sie auf **Datei-Hash hinzufügen**.

Das Fenster **Datei zur Ausnahmeliste hinzufügen** wird angezeigt.

Hinweis

Verwenden Sie die Schaltflächen **Importieren** und **Exportieren**, um die Liste mit verschiedenen Richtlinien zu teilen.

c. Geben Sie den Datei-Hash SHA-1 an, um ihn vom Suchvorgang auszuschließen.

d. Stellen Sie optional eine Anmerkung mit dem Grund für die Ausnahme bereit oder beschreiben Sie die dem Hash-Wert zugeordneten Dateinamen.

e. Klicken Sie auf **Hinzufügen**.

Die Funktion "Vorausschauendes Maschinenlernen" fügt den Dateihash zur Ausnahmeliste hinzu.

Konfigurieren der Einstellungen für die Exemplar Zusendung

Sie können Security Agents so konfigurieren, dass Dateiobjekte, die unter Umständen zuvor nicht erkannte Bedrohungen enthalten, zur weiteren Analyse an Virtual Analyzer weitergeleitet werden. Nach der Bewertung der Objekte fügt Virtual Analyzer alle Objekte, in denen unbekannte Bedrohungen gefunden wurden, zu den Virtual Analyzer-Listen mit verdächtigen Objekten hinzu und verteilt die Listen über das Netzwerk an andere Security Agents.

Zu den verdächtigen Dateien gehören die folgenden:

- Programme, die Trend Micro nicht bekannt sind (heruntergeladen über unterstützte Webbrowser oder E-Mail-Kanäle)
- Heuristische Erkennung von Prozessen (heruntergeladen über unterstützte Webbrowser oder E-Mail-Kanäle)
- Autorun-Programme mit geringer Verbreitung auf Wechselmedien

Wichtig

Die Größe der Beispieldateien, die die Security Agents übermitteln können, ändert sich basierend auf dem verwendeten Typ von Virtual Analyzer. Beim Deep Discovery Analyzer-Server können Beispieldateien bis zu 50 MB groß sein. Beim Deep Discovery Analyzer als Dienst-Add-On können Beispieldateien bis zu 60 MB groß sein.

Prozedur

1. Wählen Sie **Weiterleitung verdächtiger Dateien an Virtual Analyzer aktivieren**.

Verdächtige Verbindungseinstellungen konfigurieren

Security Agents kann alle Verbindungen zwischen Endpunkten und Adressen in der globalen C&C-IP-Liste protokollieren und sperren. Sie können IP-

Adressen protokollieren, die in der benutzerdefinierten Liste mit gesperrten IP-Adressen konfiguriert sind, aber dennoch den Zugriff auf diese IP-Adressen erlauben.

Security Agents kann außerdem Verbindungen überwachen, die das Ergebnis einer Botnet- oder sonstigen Malware-Bedrohung sind. Wenn eine Malware-Bedrohung erkannt wurde, kann Security Agents versuchen, die Infektion zu beseitigen.

Prozedur

1. Aktivieren Sie die Einstellung **Detect network connections made to addresses in the Global C&C IP list**, um Verbindungen zu von Trend Micro bestätigten C&C-Servern zu überwachen, und wählen Sie, ob Verbindungen **Nur protokollieren** oder **Sperren** werden sollen.

   - Um Agenten die Verbindung zu Adressen in der Benutzerdefinierten Liste mit gesperrten IP-Adressen zu ermöglichen, aktivieren Sie die Einstellung **Zugriff auf benutzerdefinierte Liste mit gesperrten IP-Adressen zulassen und protokollieren**.

   Hinweis

   Sie müssen die Protokollierung von Netzwerkverbindungen aktivieren, damit Security Agents den Zugriff auf Adressen in der benutzerdefinierten Liste mit gesperrten IP-Adressen zulassen kann.

2. Wählen Sie **Erkennen von Verbindungen mithilfe des Fingerabdrucks für Netzwerk von Malware**, um die Funktion zu aktivieren.

3. Konfigurieren Sie die **Überwachungsstufe**-Einstellungen für **Erkennung** und **Prävention**.

Wichtig

- Höhere Überwachungsstufen bieten eine größere Sensibilität, können jedoch eine große Anzahl nicht wesentlicher Protokolle erzeugen und die Leistung des Endpunkts beeinträchtigen. Trend Micro empfiehlt, **2 - Mäßig** auszuwählen, um relevantere Daten mit minimalen Auswirkungen auf Ihre Endpunkte zu erhalten.
- Die **Prävention**-Stufe muss gleich oder niedriger als **Erkennung** sein.
- Die Auswahl von **Bedrohungen zum Sperren** kann die Präventionsmaßnahmen für das ausgewählte Präventionsniveau beeinflussen.

4. Wählen Sie den **Zu ergreifende Maßnahmen** aus.
   - **Nur protokollieren**: Ereignis protokollieren und keine Aktion ausführen.
   - **Sperren**: Die Verbindung sperren.
5. Um Security Agents zu ermöglichen, Verbindungen zu C&C-Servern zu bereinigen, aktivieren Sie die Einstellung **Verdächtige Verbindungen säubern, wenn ein C&C-Callback erkannt wird**.

   Security Agents verwenden Sie GeneriClean, um die Malware-Bedrohung zu bereinigen und die Verbindung zum C&C-Server zu beenden.

   Wichtig

   Sie müssen **Log connections using malware network fingerprinting** aktivieren, damit Security Agents versuchen kann, die Verbindungen zu C&C-Servern zu säubern, die vom Paketstrukturabgleich erkannt wurden.

Kapitel 13

Einstellungen der Gerätesteuerungsrichtlinien

In diesem Abschnitt wird beschrieben, wie die Gerätesteuerungsrichtlinien für Security Agents konfiguriert werden.

Es werden folgende Themen behandelt:

- *Gerätesteuerung auf Seite 13-2*
- *Einstellungen der Gerätesteuerung konfigurieren auf Seite 13-2*

Gerätesteuerung

Die Gerätesteuerung reguliert den Zugriff auf externe Speichergeräte und Netzwerkressourcen, die an Computer angeschlossen sind. Die Gerätesteuerung trägt dazu bei, Datenverluste und Datenlecks zu verhindern und bietet, gemeinsam mit der Virensuche, Schutz vor Sicherheitsrisiken.

Sie können Gerätesteuerungsrichtlinien für interne und externe Agents konfigurieren. In der Regel konfigurieren Administratoren eine strengere Richtlinie für externe Agents.

Trend Micro Apex Central bietet sowohl eine endpunktbasierte als auch eine benutzerbasierte Konfiguration der Gerätesteuerungsrichtlinie.

Einstellungen der Gerätesteuerung konfigurieren

Prozedur

1. Wählen Sie **Gerätesteuerung aktivieren**.
   - Wenn Sie sich auf der **Externe Agents**-Registerkarte befinden, können Sie Einstellungen für interne Agents anwenden, indem Sie **Alle Einstellungen für interne Agents übernehmen** auswählen.
   - Wenn Sie sich auf der **Interne Agents**-Registerkarte befinden, können Sie Einstellungen für externe Agenten anwenden, indem Sie **Alle Einstellungen für externe Agents übernehmen** auswählen.
2. Fügen Sie eine Regel für die Gerätesteuerung hinzu oder bearbeiten Sie diese:
   - Für benutzerbasierte Regeln:
     - Um eine Regel basierend auf Active Directory-Benutzer- oder -Gruppenkonten zu erstellen, klicken Sie auf **Hinzufügen**.
     - Um eine Regel basierend auf Active Directory-Benutzer- oder -Gruppenkonten zu bearbeiten, klicken Sie auf den Link in der Spalte **Benutzerkonten**.

Wichtig

Benutzerbasierte Gerätesteuerungsregeln sind nur verfügbar, nachdem Active Directory in Trend Micro Apex Central integriert wurde.

- So bearbeiten Sie die standardmäßige endpunktbasierte Regel:
  - Klicken Sie auf den Link **Alle Benutzer (Standard)** in der Spalte **Benutzerkonten**.

Hinweis

Die standardmäßige endpunktbasierte Regel kann nicht gelöscht werden.

Das Fenster **Gerätesteuerungsregel** wird angezeigt.

3. Geben Sie im Abschnitt **Benutzerkonten** die Anzeigenamen der Active Directory-Benutzer- oder -Gruppenkonten ein, für die die Regel gilt, bzw. wählen Sie sie aus.

Hinweis

Sie können keine Benutzer- oder Gruppenkonten angeben, wenn Sie die standardmäßige endpunktbasierte Regel **Alle Benutzer (Standard)** bearbeiten.

4. Gehen Sie im Abschnitt **Speichergeräte** wie folgt vor:
   a. Wählen Sie eine Berechtigung für jedes Speichergerät aus.

Wichtig

- Nur Security Agents mit Schutz aktiviert können die Aktion „Sperren“ ausführen. Wenn Sie eine Richtlinie auf Security Agents anwenden, die keinen Schutz aktiviert haben, wendet Apex One die im Dropdown-Menü konfigurierte Aktion an.
- Apex One wendet automatisch die Zugriffsberechtigung an, die für jedes USB-Gerät in der Liste **Zulässige USB-Liste** konfiguriert wurde, selbst wenn Datenschutz nicht aktiviert wurde.

Weitere Informationen zu Berechtigungen finden Sie unter *Berechtigungen für Geräte auf Seite 13-6*.

Wenn Sie den Zugriff auf Speichergeräte beschränkt haben, wird die Schaltfläche **Zulässige Programme** angezeigt. Für **USB-Speichergeräte** gilt: Wenn Sie **Sperren (Datenschutz)** ausgewählt haben, wird die Schaltfläche **Zulässige USB-Geräte** angezeigt.

b. (Optional) Klicken Sie auf **Zulässige Programme**, um eine Liste der Programme zu konfigurieren, für die die Gerätesteuerung den Zugriff auf keinem Gerätetyp einschränkt.

Das Fenster **Zulässige Programme** wird angezeigt.

1. Geben Sie den vollständigen Pfad oder den vertrauenswürdigen Anbieter der digitalen Signatur der Programme ein, auf die Benutzer gemäß der Gerätesteuerung zugreifen dürfen.

Hinweis

- Wird ein Anbieter der digitalen Signatur angegeben, lässt die Gerätesteuerung nur die Ausführung von Programmen zu, die vom Herausgeber signiert wurden.

  Weitere Informationen finden Sie unter *Anbieter der digitalen Signatur festlegen auf Seite 13-10*.

- Wenn Sie den vollständigen Pfad eines Programms angeben, unterstützt die Liste der zulässigen Programme der Gerätesteuerung die Verwendung von Platzhalterzeichen.

  Weitere Informationen finden Sie unter *Unterstützung von Platzhalterzeichen für die Liste zulässiger Programme der Gerätesteuerung auf Seite 13-9*.

2. Klicken Sie auf **Hinzufügen**.

   Der vollständige Pfad des Programms oder der vertrauenswürdige Anbieter der digitalen Signatur wird in der Liste angezeigt.

3. Wählen Sie, ob für das Programm die Berechtigungen **Ausführen** oder **Lesen/Schreiben** zulässig sein sollen.

4. Klicken Sie auf **OK**.

c. (Optional) Klicken Sie auf **Zulässige USB-Geräte**, um eine Liste der USB-Geräte zu konfigurieren, die von der Gerätesteuerung nicht gesperrt werden.

Das Fenster **Zulässige USB-Geräte** wird angezeigt.

1. Geben Sie den Gerätehersteller, das Modell und die Seriennummer in die Liste ein.

2. Um weitere Geräte hinzuzufügen, klicken Sie auf das Plus-Symbol (+).

3. Geben Sie im Listenfeld **Berechtigungen** die Zugriffsebene an, die die Gerätesteuerung Benutzern gewährt, die auf die angegebenen USB-Geräte zugreifen.
4. Klicken Sie auf **OK**.

d. Wählen Sie **AutoAusführen-Funktion auf USB-Speichergeräten sperren** aus, um zu verhindern, dass auf USB-Geräten gespeicherte Programme automatisch ausgeführt werden.

e. Wählen Sie **Zeigen Sie eine Benachrichtigung auf dem Endpunkt an, wenn Apex One einen unbefugten Gerätezugriff erkennt**, um Endbenutzer darüber zu informieren, dass die Gerätesteuerung den Zugriff auf ein Gerät eingeschränkt hat.

5. Wählen Sie für Security Agents mit installierter Datenschutzfunktion für den Zugriff auf die Geräte, die unter **Mobilgeräte** und **Nicht-Speichergeräte** aufgeführt sind, entweder **Zulassen** oder **Sperren** aus.

6. Klicken Sie auf **OK**.

Hinweis

Die Gerätesteuerung weist automatisch allen benutzerbasierten Regeln eine höhere Priorität als der standardmäßigen endpunktbasierten Regel (**Alle Benutzer (Standard)**) zu.

7. (Optional) Verwalten Sie die Regelliste der Gerätesteuerung.

- **Priorität**: Klicken Sie auf die Pfeile, um die Priorität der benutzerbasierten Regeln zu ändern.
- **Kopieren**: Wählen Sie eine Regel aus, klicken Sie auf **Kopieren** und ändern Sie die Inhalte der Regel.
- **Löschen**: Wählen Sie eine Regel aus und klicken Sie auf **Löschen**, um die Regel dauerhaft aus der Liste zu löschen.

Berechtigungen für Geräte

Gerätesteuerung-Berechtigungen für Speichergeräte werden verwendet, wenn Sie:

- Erlauben Sie den Zugriff aus USB-Speichergeräte, CD/DVD, Disketten und Netzwerklaufwerke. Sie können den Zugriff auf diese Geräte entweder uneingeschränkt zulassen oder die Zugriffsstufe einschränken.
- Konfigurieren Sie die Liste der zulässigen USB-Speichergeräte. Mit der Gerätesteuerung können Sie den Zugriff auf alle USB-Speichergeräte sperren, mit Ausnahme der Geräte, die Sie in der Liste zulässiger Geräte hinzugefügt haben. Sie können den Zugriff auf die zulässigen Geräte entweder uneingeschränkt zulassen oder die Zugriffsstufe einschränken.

Die folgende Tabelle enthält eine Liste der Berechtigungen für Speichergeräte.

Tabelle 13-1. Gerätesteuerungsberechtigungen für Speichergeräte

Berechtigungen	Dateien auf dem Gerät	Eingehende Dateien
Vollständiger Zugriff	Zulässige Aktionen: Kopieren, Verschieben, öffnen, Speichern, Löschen, Ausführen	Zulässige Aktionen: Speichern, Verschieben, Kopieren Das bedeutet, dass eine Datei kann auf dem Gerät gespeichert, verschoben und kopiert werden kann.
Ändern	Zulässige Aktionen: Kopieren, Verschieben, öffnen, Speichern, Löschen Unzulässige Aktionen: Ausführen	Zulässige Aktionen: Speichern, Verschieben, Kopieren
Lesen und ausführen	Zulässige Aktionen: Kopieren, öffnen, Ausführen Unzulässige Aktionen: Speichern, Verschieben, Löschen	Unzulässige Aktionen: Speichern, Verschieben, Kopieren
Lesen	Zulässige Aktionen: Kopieren, öffnen Unzulässige Aktionen: Speichern, Verschieben, Löschen, Ausführen	Unzulässige Aktionen: Speichern, Verschieben, Kopieren

Berechtigungen	Dateien auf dem Gerät	Eingehende Dateien
Nur Geräteinhalt auflisten	Unzulässige Aktionen: Alle Aktionen Die enthaltenen Geräte und Dateien werden dem Benutzer angezeigt (beispielsweise in Windows Explorer).	Unzulässige Aktionen: Speichern, Verschieben, Kopieren
Sperren (nach der Installation der Funktion "Datenschutz" verfügbar)	Unzulässige Aktionen: Alle Aktionen Die enthaltenen Geräte und Dateien werden dem Benutzer nicht angezeigt (beispielsweise in Windows Explorer).	Unzulässige Aktionen: Speichern, Verschieben, Kopieren

Die dateibasierte Suche wird durch Geräteberechtigungen ergänzt und kann die Geräteberechtigungen überschreiben. Wenn die Berechtigung z. B. zulässt, dass eine Datei geöffnet werden kann, der Security Agent jedoch erkennt, dass die Datei mit Malware infiziert ist, wird eine bestimmte Suchaktion auf die Datei angewendet, um die Malware zu entfernen. Wenn als Suchaktion "Säubern" ausgewählt wird, wird die Datei nach dem Säubern geöffnet. Wird jedoch als Suchaktion "Löschen" ausgewählt, wird die Datei gelöscht.

Die folgende Tabelle enthält eine Liste der Berechtigungen für mobile Geräte und Nicht-Speichergeräte, die vom Datenschutzdienst verwaltet werden.

Tabelle 13-2. Gerätesteuerungsberechtigungen für mobile Geräte und Nicht-Speichergeräte

Berechtigungen	Dateien auf dem Gerät	Eingehende Dateien
Zulassen	Zulässige Aktionen: Kopieren, Verschieben, öffnen, Speichern, Löschen, Ausführen	Zulässige Aktionen: Speichern, Verschieben, Kopieren Das bedeutet, dass eine Datei kann auf dem Gerät gespeichert, verschoben und kopiert werden kann.

Berechtigungen	Dateien auf dem Gerät	Eingehende Dateien
Sperren	Unzulässige Aktionen: Alle Aktionen Die enthaltenen Geräte und Dateien werden dem Benutzer nicht angezeigt (beispielsweise in Windows Explorer).	Unzulässige Aktionen: Speichern, Verschieben, Kopieren

Tipp

Die Gerätesteuerung für den Datenschutz unterstützt alle 64-Bit-Plattformen. Legen Sie für die Überwachung durch Unauthorized Change Prevention auf Systemen, die der Security Agent nicht unterstützt, die Geräteberechtigung auf **Sperren** fest, um den Zugriff auf diese Geräte einzuschränken.

Unterstützung von Platzhalterzeichen für die Liste zulässiger Programme der Gerätesteuerung

Ein Programmpfad und -name darf maximal 259 Zeichen umfassen und nur alphanumerische Zeichen (A-Z, a-z, 0-9) enthalten. Es ist nicht möglich, nur den Programmnamen anzugeben.

Als Ersatz für Laufwerksbuchstaben und Programmnamen können Platzhalterzeichen verwendet werden. Verwenden Sie ein Fragezeichen (?), um ein einzelnes Zeichen darzustellen, z. B. einen Laufwerksbuchstaben. Verwenden Sie einen Stern (*), um mehrere Zeichen darzustellen, z. B. einen Programmnamen.

Hinweis

Platzhalter können nicht für Ordnernamen verwendet werden. Sie müssen den exakten Namen eines Ordners angeben.

In den folgenden Beispielen wurden die Platzhalter richtig verwendet:

Tabelle 13-3. Richtige Verwendung von Platzhaltern

Beispiel	Übereinstimmende Daten
?:\Password.exe	Die Datei "Password.exe", die sich direkt auf einem beliebigen Laufwerk befindet
C:\Programme\Microsoft*****.exe	Eine beliebige Datei unter C:\Programme mit einer Dateierweiterung
C:\Programme*****.*****	Eine beliebige Datei unter C:\Programme mit einer Dateierweiterung
C:\Programme\a**?**c.exe	Eine beliebige .exe-Datei unter C:\Programme mit 3 Buchstaben, die mit dem Buchstaben "a" beginnt und mit dem Buchstaben "c" endet
C:*****	Alle Dateien, die sich direkt auf dem Laufwerk C:\ befinden, und zwar mit oder ohne Dateierweiterung

In den folgenden Beispielen wurden die Platzhalter falsch verwendet:

Tabelle 13-4. Falsche Verwendung von Platzhaltern

Beispiel	Grund
??:\Buffalo\Password.exe	?? stellt zwei Zeichen dar, und Laufwerksbuchstaben bestehen nur aus einem alphabetischen Zeichen.
*****:\Buffalo\Password.exe	* stellt mehrere Zeichen dar, und Laufwerksbuchstaben bestehen nur aus einem alphabetischen Zeichen.
C:*****\Password.exe	Platzhalter können nicht für Ordnernamen verwendet werden. Sie müssen den exakten Namen eines Ordners angeben.
C:**?**\Password.exe	

Anbieter der digitalen Signatur festlegen

Legen Sie einen Anbieter der digitalen Signatur fest, wenn Sie Programmen von diesem Anbieter vertrauen. Geben Sie beispielsweise Microsoft Corporation oder Trend Micro, Inc. ein. Sie können den Anbieter der digitalen Signatur über die Eigenschaften eines Programms abrufen (indem Sie beispielsweise mit der rechten Maustaste auf das Programm klicken und **Eigenschaften** auswählen).

Kapitel 14

Ausnahmen

In diesem Abschnitt wird beschrieben, wie Sie Suchausschlusslisten konfigurieren, die auf mehrere Suchfunktionen angewendet werden.

Es werden folgende Themen behandelt:

- *Liste der vertrauenswürdigen Programme auf Seite 14-2*
- *Liste der zulässigen Spyware/Grayware auf Seite 14-5*
- *Regelausnahmen auf Seite 14-3*

Liste der vertrauenswürdigen Programme

Sie können Security Agents so konfigurieren, dass die Suche für vertrauenswürdige Prozesse bei der Application Control, der Verhaltensüberwachung, der Gerätesteuerung, dem Endpoint Sensor und der Echtzeitsuche übersprungen wird. Nach dem Hinzufügen eines Programms zur Liste der vertrauenswürdigen Programme führt der Security Agent keine Echtzeitsuche für das Programm oder für vom Programm ausgeführte Prozesse aus. Fügen Sie vertrauenswürdige Programme zur Liste der vertrauenswürdigen Programme hinzu, um die Suchleistung auf Endpunkten zu verbessern.

Hinweis

Sie können eine Datei zur Liste der Vertrauenswürdigen Programme hinzufügen, wenn die Datei eine gültige digitale Signatur hat.

Nachdem Sie ein Programm zur Liste der vertrauenswürdigen Programme hinzugefügt haben, schließt der Security Agent das Programm automatisch von den folgenden Suchvorgängen aus:

- Application Control (konfigurierbar nur auf der Trend Micro Apex Central-Konsole)
- Verhaltensüberwachung
- Gerätesteuerung
- Endpoint Sensor (konfigurierbar nur auf der Trend Micro Apex Central-Konsole)
- Echtzeitsuche: Dateiüberprüfung und Durchsuchen von Prozessen

Liste der vertrauenswürdigen Programme konfigurieren

Die Liste der vertrauenswürdigen Programme schließt Programme und alle untergeordneten Prozesse aus, die über Application Control, Verhaltensüberwachung, Gerätesteuerung, Endpoint Sensor und Echtzeitsuche vom Programm aufgerufen werden.

Prozedur

1. Geben Sie bei der Konfiguration einer übergeordneten Richtlinie an, wie andere Benutzer untergeordnete Richtlinien konfigurieren können.

   - **Von übergeordnetem Element erben**: Untergeordnete Richtlinien müssen die Einstellungen verwenden, die in der übergeordneten Richtlinie konfiguriert wurden
   - **Von übergeordnetem Element erweitern**: Untergeordnete Richtlinien können zusätzliche Einstellungen an die Einstellungen anhängen, die von der übergeordneten Richtlinie vererbt wurden

   Hinweis

   Wenn Ihre Kinderrichtlinien **Von übergeordnetem Element erweitern** sind, können Sie **Einschränkungen der Kinderpolitik** konfigurieren, um zu verhindern, dass Kinderrichtlinien bestimmte Regeln zur Liste der Ausnahmeregeln hinzufügen.

2. Geben Sie den vollständigen Programmpfad für das Programm an, das von der Liste ausgeschlossen werden soll.
3. Klicken Sie auf **Zur Liste vertrauenswürdiger Programme hinzufügen**.
4. Um ein Programm aus der Liste zu entfernen, klicken Sie auf das Symbol **Delete**.

Regelausnahmen

Sie können die Liste der Ausnahmeregeln in Security Agents-Richtlinien konfigurieren, um Erkennungen basierend auf Regel-IDs von den folgenden DURCHSUCHEN-Funktionen auszuschließen:

- Anti-Malware-Scans
- Verhaltensüberwachung
- Verdächtige Verbindung

Konfigurieren Sie Ausnahmeregeln in Security Agents-Richtlinien, um die Richtlinienverwaltung zu verbessern und die DURCHSUCHEN-Leistung zu steigern.

Konfigurieren von Ausnahmeregeln

Fügen Sie Regel-IDs zur Liste der Regelausnahmen hinzu, um DURCHSUCHEN-Erkennungen basierend auf Regel-IDs auszuschließen.

Prozedur

1. Geben Sie bei der Konfiguration einer übergeordneten Richtlinie an, wie andere Benutzer untergeordnete Richtlinien konfigurieren können.
   - **Von übergeordnetem Element erben**: Untergeordnete Richtlinien müssen die Einstellungen verwenden, die in der übergeordneten Richtlinie konfiguriert wurden
   - **Von übergeordnetem Element erweitern**: Untergeordnete Richtlinien können zusätzliche Einstellungen an die Einstellungen anhängen, die von der übergeordneten Richtlinie vererbt wurden

   Hinweis

   Wenn Ihre Kinderrichtlinien **Von übergeordnetem Element erweitern** sind, können Sie **Einschränkungen der Kinderpolitik** konfigurieren, um zu verhindern, dass Kinderrichtlinien bestimmte Regeln zur Liste der Ausnahmeregeln hinzufügen.
2. Geben Sie eine gültige Regel-ID ein.

   Sie können Regel-IDs auf dem Bildschirm **Protokollabfrage** finden.
3. Klicken Sie auf **Hinzufügen**.

   Das System zeigt einen neuen Eintrag in der Tabelle an.
4. Um einen Eintrag aus der Liste zu entfernen, klicken Sie auf das **Löschen**-Symbol.

Liste der zulässigen Spyware/Grayware

Der Security Agent stellt eine Liste der "zulässigen" Spyware/Grayware bereit, die Dateien oder Anwendungen enthält, die nicht als Spyware oder Grayware behandelt werden sollen. Wenn während der Suche eine bestimmte Spyware/Grayware erkannt wird, überprüft der Security Agent die Liste der zulässigen Software und führt bei einer Übereinstimmung keine Aktion aus.

Sie können die Liste der zulässigen Software auf einen oder mehrere Security Agents und Domänen bzw. auf alle Security Agents, die vom Server verwaltet werden, verteilen. Die Liste der zulässigen Software gilt für alle Suchtypen, d. h. dieselbe Liste der zulässigen Software wird während der manuellen Suche, der Echtzeitsuche, der zeitgesteuerten Suche und der Funktion "Jetzt durchsuchen" verwendet.

Die Liste der zulässigen Spyware/Grayware verwalten

Prozedur

1. Wählen Sie in der **Spyware/Grayware names**-Tabelle einen Spyware/Grayware-Namen aus. Um mehrere Namen auszuwählen, halten Sie die CTRL-Taste gedrückt, während Sie auswählen.

   - Sie können auch ein Schlüsselwort in das Feld **Suchen** eingeben und auf **Suchen** klicken. Die Tabelle wird mit den Namen aktualisiert, die dem Schlüsselwort entsprechen.

2. Klicken Sie auf **Hinzufügen**.

   Die Namen werden in die Tabelle **Zulässige Liste** verschoben.

3. Wählen Sie die Namen aus, und klicken Sie auf **Entfernen**, um die Namen aus der Liste zu löschen. Um mehrere Namen auszuwählen, halten Sie die CTRL-Taste bei der Auswahl gedrückt.

Kapitel 15

Richtlinieneinstellungen für Endpoint Sensor

In diesem Abschnitt wird beschrieben, wie die Endpoint Sensor-Richtlinien für Security Agents konfiguriert werden.

Es werden folgende Themen behandelt:

Endpoint Sensor

Endpoint Sensor ist ein leistungsstarkes Überwachungs- und Untersuchungswerkzeug, mit dem das Vorhandensein, der Standort und der Eintrittspunkt von Bedrohungen identifiziert werden können. Mittels detaillierter Systemereignisaufzeichnung und Verlaufsanalyse können Sie historische Untersuchungen durchführen, um in Ihrem Netzwerk verborgene Bedrohungen und alle betroffenen Endpoints zu ermitteln. Erstellen Sie Berichte zur Fehlerursachenanalyse, um die Art und Aktivität der Malware seit Auftreten der Bedrohung am Endpoint zu verstehen.

Sie können mit Hilfe von freigegebenen IOC-Dateien und YARA-Regeln auch Live-Untersuchungen durchführen. Während Live-Untersuchungen werden ausführliche Suchläufe in Endpoints durchgeführt, um zuvor nicht erkannte Bedrohungen und mögliche Advanced Persistent Threat-Angriffe zu finden.

Konfigurieren von Einstellungen für Endpoint Sensor

Wichtig

Die Endpoint Sensor-Funktion erfordert eine spezielle Lizenzierung und zusätzliche Systemvoraussetzungen. Stellen Sie sicher, dass Sie die richtige Lizenz haben, bevor Sie Endpoint Sensor-Richtlinien auf Endpunkten bereitstellen. Für weitere Informationen zum Erwerb von Lizenzen wenden Sie sich an Ihren Support-Anbieter.

Wenn Ihre Umgebung sowohl Apex One On-Premises als auch Apex One as a Service Security Agents verwaltet, können einige Funktionen im Vergleich zu Apex One as a Service unterschiedlich sein. Apex One as a Service Security Agents senden weiterhin Daten an Trend Micro Server, aber die Untersuchungskapazitäten können sich von der Apex Central as a Service-Konsole unterscheiden.

Prozedur

1. Wählen Sie **Endpoint Sensor aktivieren**.
2. Wählen Sie **Ereignisaufzeichnung aktivieren**, um mit der Erfassung von Systemereignisprotokollen auf dem Agent-Endpunkt zu beginnen. (nur vor Ort)

   Endpoint Sensor verwendet die Echtzeit-Ereignisprotokolle, um gefährdete Endpunkte bei Untersuchungen zu identifizieren. Nachdem betroffene Windows-Endpunkte identifiziert wurden, können Sie eine gründliche Grundursachenanalyse durchführen, um mögliche Angriffsvektoren besser zu verstehen.

Optionen	Beschreibung
Maximale Datenbankgröße (nur vor Ort)	Geben Sie die maximale Datenbankgröße an, die der Endpoint Sensor verwenden kann, um Ereignisprotokolle auf dem Endpunkt zu speichern. Sobald die Agentendatenbank die maximale Größenbeschränkung erreicht, löscht der Endpoint Sensor die ältesten Protokolle, um Platz für neue Ereigniseinträge zu schaffen.

Optionen	Beschreibung
Senden Sie einen Teil der Protokolldaten, um historische Untersuchungen durchzuführen (nur vor Ort)	Die an den Server gesendeten Informationen bestehen aus Metadaten, wie Domain, Dateien oder Prozessen auf dem Endpunkt. Endpoint Sensor nutzt die Daten während historischer Untersuchungen, um betroffene Endpunkte zu identifizieren. • **Upload-Häufigkeit**: Geben Sie an, wie oft der Agent die Metadaten an den Server hochlädt. **Hinweis** Je nach Ihrem Netzwerk können häufigere Uploads die Netzwerkleistung beeinträchtigen. • **Zusätzliche Hash-Typen**: Geben Sie an, ob der Endpoint Sensor auch SHA-256- und MD5-Hashes berechnet und an den Server sendet. Standardmäßig sendet der Endpoint Sensor nur SHA1-Hashes. **Hinweis** Die Auswahl zusätzlicher Hash-Typen beansprucht mehr Datenbankplatz.
Aktivieren Sie die Angriffserkennung, um bekannte Angriffsindikatoren auf Endpunkten zu erkennen	Attack Discovery verwendet die Bedrohungsinformationen von Trend Micro, die auf Verhaltensweisen von Angriffsanzeichen (Indicators of Attack, IoA) basieren. Nach der Erkennung eines bekannten IoA protokolliert Attack Discovery die Erkennung.

Kapitel 16

Vulnerability Protection – Policy-Einstellungen

In diesem Abschnitt wird beschrieben, wie Vulnerability Protection-Richtlinien für Security Agents konfiguriert werden.

Es werden folgende Themen behandelt:

- *Vulnerability Protection auf Seite 16-2*
- *Konfigurieren der Einstellungen für den Vulnerability Protection auf Seite 16-2*

Vulnerability Protection

Durch die Integration von Vulnerability Protection werden Apex One-Benutzer geschützt, indem die Anwendung virtueller Patches automatisiert wird, bevor offizielle Patches verfügbar sind. Trend Micro stellt geschützte Endpunkte mit empfohlenen Eindringschutzregeln basierend auf der Leistung Ihres Netzwerks und den Sicherheitsprioritäten zur Verfügung.

Konfigurieren der Einstellungen für den Vulnerability Protection

Prozedur

1. Wählen Sie **Vulnerability Protection aktivieren**.
2. Einstellungen zur Eindringungsprävention konfigurieren:
   a. Klicken Sie auf die Registerkarte **Regeln zum Eindringschutz**.
   b. Wählen Sie eines der folgenden Scanprofile aus:
      - **(Empfohlen)**: Gewährleistet Schutz vor bekannten Sicherheitslücken, bietet relevantere Daten und reduziert die Leistungseinbußen auf Endpunkten
      - **Aggressiv**: Wendet zusätzliche Regeln zum Eindringschutz für verdächtige Netzwerkaktivitäten auf das **(Empfohlen)**-Scanprofil an

      Wichtig

      Aggressives Durchsuchen kann eine große Anzahl nicht wesentlicher Protokolle erzeugen und die Leistung des Endpunkts beeinträchtigen. Trend Micro empfiehlt dringend die Verwendung des **(Empfohlen)**-Profils.

   c. (Optional) Wählen Sie eine Ansicht, um die Liste der Regeln zum Eindringschutz nach Status zu filtern.

Anzeigen	Beschreibung
Alle	Zeigt alle Regeln zum Eindringschutz an
Standard (Aktiviert)	Zeigt nur die Regeln zum Eindringschutz an, die das ausgewählte Scanprofil standardmäßig aktiviert
Standard (Deaktiviert)	Zeigt nur die Regeln zum Eindringschutz an, die das ausgewählte Scanprofil standardmäßig deaktiviert
Benutzerdefiniert (Aktiviert)	Zeigt nur die vom Benutzer aktivierten Regeln zum Eindringschutz an
Benutzerdefiniert (Deaktiviert)	Zeigt nur die vom Benutzer deaktivierten Regeln zum Eindringschutz an

d. Ändern Sie den Status einer Regel, indem Sie aus der **Status**-Dropdown-Steuerung auswählen.

- **Standard (Aktiviert)**: Das ausgewählte Scanprofil aktiviert die entsprechende Regel standardmäßig. Wählen Sie, um den Regelstatus anzuwenden, der durch das Scanprofil definiert ist.
- **Standard (Deaktiviert)**: Das ausgewählte Scanprofil deaktiviert die entsprechende Regel standardmäßig. Wählen Sie, um den durch das Scanprofil definierten Regelstatus anzuwenden.
- **Benutzerdefiniert (Aktiviert)**: Wählen, um die Regel zu aktivieren.
- **Benutzerdefiniert (Deaktiviert)**: Wählen Sie, um die Regel zu deaktivieren.

3. Einstellungen der Netzwerk-Engine konfigurieren:

a. Klicken Sie auf die Registerkarte **Einstellungen der Netzwerk-Engine**.

b. Wählen Sie den **Erkennungsmodus der Netzwerkanalyse-Engine*** aus.

Hinweis

Sie können auch den ausgewählten Netzwerk-Engine-Erkennungsmodus verwenden, um die erweiterte Protokollierungsrichtlinie zu konfigurieren.

- **Inline**: Live-Paketströme passieren direkt die Vulnerability Protection-Netzwerk-Engine. Alle Regeln werden auf den Netzwerkverkehr angewendet, bevor die Pakete den Protokollstapel hinaufgehen.
- **Tippen (Nur Erkennung)**: Live-Paketströme werden repliziert und vom Hauptstrom abgeleitet.

c. Konfigurieren Sie die folgenden Einstellungen:

Einstellung	Beschreibung
ESTABLISHED Timeout	Wie lange im ESTABLISHED-Zustand bleiben, bevor die Verbindung geschlossen wird
LAST_ACK-Zeitüberschreitung	Wie lange im LAST-ACK-Zustand bleiben, bevor die Verbindung geschlossen wird
Kaltstart-Zeitüberschreitung	Die Zeitspanne, die nicht-SYN-Paketen erlaubt wird, die zu einer Verbindung gehören könnten, die vor dem Start des zustandsbehafteten Mechanismus hergestellt wurde
UDP-Zeitüberschreitung	Die maximale Dauer einer UDP-Verbindung
Maximale TCP-Verbindungen	Die maximale Anzahl gleichzeitiger TCP-Verbindungen
Maximale UDP-Verbindungen	Die maximale Anzahl gleichzeitiger UDP-Verbindungen
Statuscode ignorieren	Wählen Sie bis zu 3 Arten von Ereignissen zum Ignorieren aus

Einstellung	Beschreibung
Erweiterte Protokollierungsrichtlinie	Wählen Sie unter folgenden Einstellungen: • **Umgehen**: Keine Filterung von Ereignissen. Überschreibt die **Statuscode ignorieren**-Einstellungen (oben) und andere erweiterte Einstellungen, überschreibt jedoch nicht die auf dem Apex One-Server definierten Protokollierungseinstellungen • **Erkennungsmodus der Netzwerkanalyse-Engine***: Verwendet **Tippen-Modus**, wenn **Tippen (Nur Erkennung)** für den Netzwerk-Engine-Erkennungsmodus ausgewählt ist, oder **Normal**, wenn **Inline** für den Netzwerk-Engine-Erkennungsmodus ausgewählt ist • **Normal**: Alle Ereignisse werden protokolliert, außer verworfene Übertragungswiederholungen • **Rückwärtskompatibilitätsmodus**: Nur für Support verwenden • **Ausführlicher Modus**: Gleich wie **Normal**, jedoch einschließlich verworfener Neuübertragungen • **Statusbehaftete und Normalisierungsunterdrückung**: Ignoriert verworfene Übertragungen, außerhalb der Verbindung, ungültige Flags, ungültige Sequenz, ungültige Bestätigung, unaufgeforderte UDP, unaufgeforderte ICMP, außerhalb der erlaubten Richtlinie • **Zustandsbehaftet, Normalisierung und Frag-Unterdrückung**: Ignoriert alles, was **Statusbehaftete und Normalisierungsunterdrückung** ignoriert, sowie Ereignisse im Zusammenhang mit Fragmentierung • **Statusbehaftete, Frag- und Verifizierungsunterdrückung**: Ignoriert alles, was **Zustandsbehaftet, Normalisierung und Frag-Unterdrückung** ignoriert, sowie verifizierungsbezogene Ereignisse

Einstellung	Beschreibung
	• **Tippen-Modus**: Ignoriert verworfene Übertragungen, außerhalb der Verbindung, ungültige Flags, ungültige Sequenz, ungültige Bestätigung, maximale Bestätigungsübertragung, Paket auf geschlossener Verbindung Eine umfassendere Liste der Ereignisse, die für **Statusbehaftete und Normalisierungsunterdrückung**, **Zustandsbehaftet, Normalisierung und Frag-Unterdrückung**, **Statusbehaftete, Frag- und Verifizierungsunterdrückung** und **Tippen-Modus** ignoriert werden, finden Sie unter *Erweiterte Protokollierungsrichtlinienmodi auf Seite 16-6*.

4. Klicken Sie auf **Speichern**, um die Einstellungen zu übernehmen.

Erweiterte Protokollierungsrichtlinienmodi

Die folgende Tabelle listet die Arten von Ereignissen auf, die in vier der komplexeren Modi der erweiterten Protokollierungsrichtlinie ignoriert werden.

Modus	Ignorierte Ereignisse
Statusbehaftete und Normalisierungsunterdrückung	Keine Verbindung
	Ungültige Flags
	Ungültige Sequenz
	Ungültige ACK
	Unaufgeforderte UDP
	Unaufgeforderte ICMP
	Außerhalb der erlaubten Richtlinie
	Verworfenes Wiederübertragen

Modus	Ignorierte Ereignisse
Zustandsbehaftet, Normalisierung und Fragmentunterdrückung	Keine Verbindung
	Ungültige Flags
	Ungültige Sequenz
	Ungültige ACK
	Unaufgeforderte UDP
	Unaufgeforderte ICMP
	Außerhalb der erlaubten Richtlinie
	CE-Flags
	Ungültige IP
	Ungültige IP-Datagrammlänge
	Fragmentiert
	Ungültiger Fragmentversatz
	Erstes Fragment zu klein
	Fragment außerhalb des Bereichs
	Fragmentversatz zu klein
	IPv6-Paket
	Maximale eingehende Verbindungen
	Maximale ausgehende Verbindungen
	Max SYN gesendet
	Lizenz abgelaufen
	IP-Version unbekannt
	Ungültige Paketinformationen
	Maximale ACK-Wiederübertragung

Modus	Ignorierte Ereignisse
	Paket auf geschlossener Verbindung
	Verworfenes Wiederübertragen
Statusbehaftete, Frag- und Verifizierer-Unterdrückung	Keine Verbindung
	Ungültige Flags
	Ungültige Sequenz
	Ungültige ACK
	Unaufgeforderte UDP
	Unaufgeforderte ICMP
	Außerhalb der erlaubten Richtlinie
	CE-Flags
	Ungültige IP
	Ungültige IP-Datagrammlänge
	Fragmentiert
	Ungültiger Fragmentversatz
	Erstes Fragment zu klein
	Fragment außerhalb des Bereichs
	Fragmentversatz zu klein
	IPv6-Paket
	Maximale eingehende Verbindungen
	Maximale ausgehende Verbindungen
	Max SYN gesendet
	Lizenz abgelaufen
	IP-Version unbekannt

Modus	Ignorierte Ereignisse
	Ungültige Paketinformationen
	Ungültiger Datenversatz
	Kein IP-Header
	Nicht lesbare Ethernet-Header
	Nicht definiert
	Gleiche Quell- und Ziel-IP
	Ungültige TCP-Headerlänge
	Unlesbarer Protokollkopf
	Nicht lesbare IPv4-Header
	Unbekannte IP-Version
	Maximale ACK-Wiederübertragung
	Paket auf geschlossener Verbindung
	Verworfenes Wiederübertragen
Tippen-Modus	Keine Verbindung
	Ungültige Flags
	Ungültige Sequenz
	Ungültige ACK
	Maximale ACK-Wiederübertragung
	Paket auf geschlossener Verbindung
	Verworfenes Wiederübertragen

Teil VI

Apex One-Richtlinien für die Prävention vor Datenverlust

Kapitel 17

Apex One Data Discovery Dashboard-Widgets

Dieser Abschnitt enthält Hilfethemen für die Apex One Data Discovery Dashboard-Widgets, die in Trend Micro Apex Central unterstützt werden.

Es werden folgende Themen behandelt:

- *Wichtigste Richtlinienfunde für vertrauliche Dateien – Widget auf Seite 17-2*
- *Die wichtigsten Endpunkte mit vertraulichen Dateien – Widget auf Seite 17-4*
- *Häufigste Übereinstimmungen für Data Discovery-Vorlagen – Widget auf Seite 17-6*
- *Häufigste Dateien mit vertraulichen Dateien – Widget auf Seite 17-7*

Wichtigste Richtlinienfunde für vertrauliche Dateien – Widget

Diese Widget zeigt Informationen über erkannte Data Discovery-Richtlinienverstöße sowie die vertraulichen Dateien an, die die Regeln ausgelöst haben.

Hinweis

Standardmäßig zeigt das Widget Daten aller verwalteten Produkte an, für die ein Benutzerkonto über Anzeigeberechtigungen verfügt.

Verwenden Sie die Dropdown-Liste **Bereich**, um den Zeitraum für die angezeigten Daten auszuwählen.

- Um einen benutzerdefinierten Zeitraum oder ein Zeitintervall festzulegen, klicken Sie auf das Einstellungssymbol (>) und wählen Sie **Benutzerdefiniert** für den **Bereich** aus.

Geben Sie mit Hilfe der Dropdown-Liste **Regel** an, welche Regel die Erkennung ausgelöst hat.

- Um die Anzahl der angezeigten Regeln festzulegen, klicken Sie auf das Einstellungssymbol (>) und wählen Sie aus dem Dropdown-Menü **Regeln zum Anzeigen** aus.
- Um die verbleibenden Daten zu aggregieren, klicken Sie auf das Einstellungssymbol (>) und wählen Sie **Die verbleibenden Daten als "Andere" anzeigen** aus.

Sie können die Daten in einer Tabelle, einem Balkendiagramm, einem Tortendiagramm oder einem Liniendiagramm anzeigen, indem Sie auf die Anzeigesymbole ( ) klicken.

Die Standardansicht enthält die folgenden Informationen in einer Tabelle.

Name der Spalte	Beschreibung
Regelname	Zeigt die Regeln an, die von vertraulichen Dateien ausgelöst wurden.

Name der Spalte	Beschreibung
Funde	Zeigt an, wie oft die Regel ausgelöst wird Klicken Sie auf den Spaltennamen **Funde**, um die Tabelle nach der Anzahl der Funde zu sortieren. Klicken Sie auf die Zahl, um detaillierte Informationen über den Fund anzuzeigen (wenn der Fund stattfindet, werden die vertraulichen Dateien erkannt).
Prozentsatz	Zeigt an, wie oft die Regel ausgelöst wird – als Prozentsatz der Gesamtzahl der Funde

Klicken Sie auf eine Zahl in der Spalte **Funde** oder klicken Sie auf einen Diagrammbereich, um detaillierte Informationen anzuzeigen.

Daten	Beschreibung
Empfangen	Datum und Uhrzeit des Empfangs der Daten durch Apex Central
Erstellt	Datum und Uhrzeit der Erkennung
Regel	Ausgelöste Regel
Endpunkt	Endpunkt, der die Regel ausgelöst hat
Domäne	Domäne, die die Regel ausgelöst hat
Benutzer	Benutzer, der die Regel ausgelöst hat
Benutzerdomäne	Domäne, zu der der Benutzer gehört
Dateipfad	Dateipfad der vertraulichen Datei
Datei	Name der vertraulichen Datei
Vorlage	Vorlage, zu der die Regel gehört
Aktion	An der vertraulichen Datei durchgeführte Aktion

Die wichtigsten Endpunkte mit vertraulichen Dateien – Widget

Dieses Widget zeigt Informationen über Endpunkte mit vertraulichen Dateien an, die erkannte Data Discovery-Richtlinienverstöße ausgelöst haben.

Hinweis

Standardmäßig zeigt das Widget Daten aller verwalteten Produkte an, für die ein Benutzerkonto über Anzeigeberechtigungen verfügt.

Verwenden Sie die Dropdown-Liste **Bereich**, um den Zeitraum für die angezeigten Daten auszuwählen.

- Um einen benutzerdefinierten Zeitraum oder ein Zeitintervall festzulegen, klicken Sie auf das Einstellungssymbol (>) und wählen Sie **Benutzerdefiniert** für den **Bereich** aus.

Geben Sie mit Hilfe der Dropdown-Liste **Regel** an, welche Regel die Erkennung ausgelöst hat.

- Um die Anzahl der angezeigten Vorlagen festzulegen, klicken Sie auf das Einstellungssymbol (>) und wählen Sie aus dem Dropdown-Menü **Anzuzeigende Endpunkte** aus.
- Um die verbleibenden Daten zu aggregieren, klicken Sie auf das Einstellungssymbol (>) und wählen Sie **Die verbleibenden Daten als "Andere" anzeigen** aus.

Sie können die Daten in einer Tabelle, einem Balkendiagramm oder einem Tortendiagramm anzeigen, indem Sie auf die Anzeigesymbole ( ) klicken.

Die Standardansicht enthält die folgenden Informationen in einer Tabelle.

Name der Spalte	Beschreibung
Endpunkte	Zeigt den Endpunkt mit vertraulichen Dateien an, die die Regel ausgelöst haben
Funde	Zeigt an, wie oft die Regel ausgelöst wird Klicken Sie auf den Spaltennamen **Funde**, um die Tabelle nach der Anzahl der Funde zu sortieren.
Prozentsatz	Zeigt an, wie oft die Regel ausgelöst wird – als Prozentsatz der Gesamtzahl der Funde

Klicken Sie auf eine Zahl in der Spalte **Funde** oder klicken Sie auf einen Diagrammbereich, um detaillierte Informationen anzuzeigen.

Daten	Beschreibung
Empfangen	Datum und Uhrzeit des Empfangs der Daten durch Apex Central
Erstellt	Datum und Uhrzeit der Erkennung
Regel	Ausgelöste Regel
Endpunkt	Endpunkt, der die Regel ausgelöst hat
Domäne	Domäne, die die Regel ausgelöst hat
Benutzer	Benutzer, der die Regel ausgelöst hat
Benutzerdomäne	Domäne, zu der der Benutzer gehört
Dateipfad	Dateipfad der vertraulichen Datei
Datei	Name der vertraulichen Datei
Vorlage	Vorlage, zu der die Regel gehört
Aktion	An der vertraulichen Datei durchgeführte Aktion

Häufigste Übereinstimmungen für Data Discovery-Vorlagen – Widget

Dieses Widget zeigt Informationen über die häufigsten Richtlinienverstöße in Data Discovery-Vorlagen im Zeitverlauf an.

Hinweis

Standardmäßig zeigt das Widget Daten aller verwalteten Produkte an, für die ein Benutzerkonto über Anzeigeberechtigungen verfügt.

Verwenden Sie die Dropdown-Liste **Bereich**, um den Zeitraum für die angezeigten Daten auszuwählen.

- Um einen benutzerdefinierten Zeitraum oder ein Zeitintervall festzulegen, klicken Sie auf das Einstellungssymbol (>) und wählen Sie **Benutzerdefiniert** für den **Bereich** aus.

Geben Sie mit Hilfe der Dropdown-Liste **Regel** an, welche Regel die Erkennung ausgelöst hat.

- Um die Anzahl der angezeigten Vorlagen festzulegen, klicken Sie auf das Einstellungssymbol (>) und wählen Sie aus dem Dropdown-Menü **Vorlagen zum Anzeigen** aus.
- Um die verbleibenden Daten zu aggregieren, klicken Sie auf das Einstellungssymbol (>) und wählen Sie **Die verbleibenden Daten als "Andere" anzeigen** aus.

Sie können die Daten in einer Tabelle, einem Balkendiagramm oder einem Tortendiagramm anzeigen, indem Sie auf die Anzeigesymbole ( ) klicken.

Die Standardansicht enthält die folgenden Informationen in einer Tabelle.

Name der Spalte	Beschreibung
Vorlagen	Zeigt die Vorlage an, die von vertraulichen Dateien ausgelöst wird

Name der Spalte	Beschreibung
Funde	Zeigt an, wie häufig die Vorlage ausgelöst wird Klicken Sie auf den Spaltennamen **Funde**, um die Tabelle nach der Anzahl der Funde zu sortieren.
Prozentsatz	Zeigt als Prozentsatz der Gesamtzahl der Funde an, wie häufig die Vorlage ausgelöst wird

Klicken Sie auf eine Zahl in der Spalte **Funde** oder klicken Sie auf einen Diagrammbereich, um detaillierte Informationen anzuzeigen.

Daten	Beschreibung
Empfangen	Datum und Uhrzeit des Empfangs der Daten durch Apex Central
Erstellt	Datum und Uhrzeit der Erkennung
Regel	Ausgelöste Regel
Endpunkt	Endpunkt, der die Regel ausgelöst hat
Domäne	Domäne, die die Regel ausgelöst hat
Benutzer	Benutzer, der die Regel ausgelöst hat
Benutzerdomäne	Domäne, zu der der Benutzer gehört
Dateipfad	Dateipfad der vertraulichen Datei
Datei	Name der vertraulichen Datei
Vorlage	Vorlage, zu der die Regel gehört
Aktion	An der vertraulichen Datei durchgeführte Aktion

Häufigste Dateien mit vertraulichen Dateien – Widget

Dieses Widget zeigt Informationen über die häufigsten vertraulichen Dateien an, die im Zeitverlauf Data Discovery-Richtlinienverstöße ausgelöst haben.

Hinweis

Standardmäßig zeigt das Widget Daten aller verwalteten Produkte an, für die ein Benutzerkonto über Anzeigeberechtigungen verfügt.

Verwenden Sie die Dropdown-Liste **Bereich**, um den Zeitraum für die angezeigten Daten auszuwählen.

- Um einen benutzerdefinierten Zeitraum oder ein Zeitintervall festzulegen, klicken Sie auf das Einstellungssymbol (>) und wählen Sie **Benutzerdefiniert** für den **Bereich** aus.

Geben Sie mit Hilfe der Dropdown-Liste **Regel** an, welche Regel die Erkennung ausgelöst hat.

- Um die Anzahl der angezeigten Erkennungen festzulegen, klicken Sie auf das Einstellungssymbol (>) und wählen Sie aus dem Dropdown-Menü **Anzuzeigende sensible Dateien** aus.
- Um die verbleibenden Daten zu aggregieren, klicken Sie auf das Einstellungssymbol (>) und wählen Sie **Die verbleibenden Daten als "Andere" anzeigen** aus.

Sie können die Daten in einer Tabelle, einem Balkendiagramm oder einem Tortendiagramm anzeigen, indem Sie auf die Anzeigesymbole ( ) klicken.

Die Standardansicht enthält die folgenden Informationen in einer Tabelle.

Name der Spalte	Beschreibung
Datei	Zeigt die vertraulichen Dateien an, die potenziell weitergegeben wurden
Funde	Zeigt an, wie häufig die vertrauliche Datei potenziell weitergegeben wurde Klicken Sie auf den Spaltennamen **Funde**, um die Tabelle nach der Anzahl der Funde zu sortieren.

Name der Spalte	Beschreibung
Prozentsatz	Zeigt als Prozentsatz der Gesamtzahl der Funde an, wie häufig die vertrauliche Datei potenziell weitergegeben wurde

Klicken Sie auf eine Zahl in der Spalte **Funde** oder klicken Sie auf einen Diagrammbereich, um detaillierte Informationen anzuzeigen.

Daten	Beschreibung
Empfangen	Datum und Uhrzeit des Empfangs der Daten durch Apex Central
Erstellt	Datum und Uhrzeit der Erkennung
Regel	Ausgelöste Regel
Endpunkt	Endpunkt, der die Regel ausgelöst hat
Domäne	Domäne, die die Regel ausgelöst hat
Benutzer	Benutzer, der die Regel ausgelöst hat
Benutzerdomäne	Domäne, zu der der Benutzer gehört
Dateipfad	Dateipfad der vertraulichen Datei
Datei	Name der vertraulichen Datei
Vorlage	Vorlage, zu der die Regel gehört
Aktion	An der vertraulichen Datei durchgeführte Aktion

Kapitel 18

Apex One Einstellungen für die Datenerkennungsrichtlinie

In diesem Abschnitt wird die Konfiguration von Apex One Einstellungen für die Datenerkennungsrichtlinie in Apex Central erläutert.

Es werden folgende Themen behandelt:

- *Data Discovery-Richtlinien erstellen auf Seite 18-2*

Data Discovery-Richtlinien erstellen

Data Discovery durchsucht Datenbanken, Endpunkte und Dokumentverwaltungssysteme auf das Vorhandensein von vertraulichen Daten. Data Discovery-Widgets zeigen die Einhaltung der Richtlinien für 'Prävention vor Datenverlust' im Hinblick auf eine Unternehmensrichtlinie an. Mit Hilfe von Data Discovery-Richtlinien und -Widgets können Administratoren Wartungsaktionen in ihrem Netzwerk durchführen.

Hinweis

Das vollständige Durchsuchen eines Endpunktlaufwerks oder -verzeichnisses kann zu einer erheblichen Systemverlangsamung für Endbenutzer führen.

Prozedur

1. Wählen Sie **Datenerkennung aktivieren** aus.
2. Klicken Sie auf **Hinzufügen**.

   Das Fenster **Data Discovery-Richtlinieneinstellungen** wird angezeigt.
3. Wählen Sie **Diese Regel aktivieren**.
4. Geben Sie einen Namen für diese Regel an.
5. Konfigurieren Sie die Einstellungen für den Zielordner:
   a. Klicken Sie auf die Registerkarte **Zielordner**.

      Hinweis

      Der Stammordner darf kein freigegebener Windows-Ordner bzw. kein Wechselmedium (USB-Gerät oder DVD) sein.

   b. Geben Sie im Abschnitt **Dateipfad** den Speicherort der Dateien für die Suche an.

Hinweis

Data Discovery durchsucht keine Dateien vom Typ `autoexec.bat` in den folgenden Verzeichnissen:

- `\Dokumente und Einstellungen\*\Anwendungsdaten\`
- `\Dokumente und Einstellungen\*\Lokale Einstellungen\`
- `\Dokumente und Einstellungen\*\Cookies\`
- `\Programme\`
- `\Windows\`
- `\Winnt\`
- `\Benutzer\*\AppData\`
- `\ProgramData\`

c. Geben Sie im Abschnitt **Ausnahmen beim Dateityp** Ausnahmen für die Suche an.

- **Suche**: Geben Sie bestimmte zu durchsuchende Dateien oder Dateitypen an.
- **Nicht durchsuchen**: Geben Sie bestimmte Dateien, Dateitypen und/oder Ordner an, die Data Discovery nicht durchsucht.

Hinweis

- Data Discovery unterstützt die folgenden Platzhalterzeichen:
  - *: Als Ersatz für ein einzelnes Zeichen oder für alle Zeichen vor oder nach dem *
  - ?: Als Ersatz für ein einzelnes Zeichen oder ein einzelnes Doppelbyte-Zeichen
- Trennen Sie mehrere Einträge durch Pipe-Zeichen (|) und verwenden Sie das folgende Format:
  - Für Dateien: *.<Dateierweiterung> (z. B.: *.exe|*.doc)
  - Für Ordner: Geben Sie einen Dateipfad an (z. B.: *\Test*|C:\My-Docs\)

Konfigurieren Sie die Vorlageneinstellungen:

6. Konfigurieren Sie die Vorlageneinstellungen:

   a. Klicken Sie auf die Registerkarte **Vorlage**.

   b. Wählen Sie Vorlagen aus der Liste **Verfügbare Vorlagen**, und klicken Sie dann auf **Hinzufügen**.

   Zur Auswahl von Vorlagen:

   - Durch Klicken auf die Vorlagennamen können Sie mehrere Einträge auswählen. Der Name wird hervorgehoben.
   - Verwenden Sie die Suchfunktion, wenn Sie nach einer bestimmten Vorlage suchen. Sie können den Namen der Vorlage vollständig oder teilweise eingeben.

Hinweis

- Jede Regel darf maximal 500 Vorlagen enthalten.
- Wenn Ihre bevorzugte Vorlage in der Liste **Verfügbare Vorlagen** nicht gefunden wurde, navigieren Sie zu **Richtlinien** > **Richtlinienressourcen** > **DLP-Vorlagen** und erstellen Sie eine neue Vorlage.

7. Konfigurieren Sie die Aktionseinstellungen:
   a. Klicken Sie auf die Registerkarte **Aktion**.
   b. Wählen Sie **Überwachen** aus, um Funde zur Analyse zu erfassen.
   c. (Optional) Wählen Sie **Verschlüsseln** aus, um vertrauliche Dateien mit einem der beiden folgenden Verfahren zu verschlüsseln:
      - **Benutzerschlüssel**
      - **Gruppenschlüssel**
      - **Verschlüsselungspasswort**: Das Verschlüsselungskennwort ist ein globales Kennwort für alle Apex One-Server. Klicken Sie auf **Verschlüsselungspasswort erstellen**, um ein Kennwort zu konfigurieren.

Wichtig

Die Dateiverschlüsselungsfunktion in Endpoint Encryption ist veraltet und möglicherweise nicht für neue Installationsinstanzen verfügbar.

8. Konfigurieren Sie den Zeitplan für die Suche:
   a. Klicken Sie auf die Registerkarte **Zeitplan**.
   b. Geben Sie das Zeitintervall für die Suche an.
   c. Geben Sie die Uhrzeit an, zu der die Suche beginnt.
9. Klicken Sie auf **Speichern**, um die Einstellungen zu übernehmen.

Kapitel 19

Apex One Einstellungen der Richtlinien für 'Prävention vor Datenverlust'

In diesem Abschnitt wird beschrieben, wie die Richtlinien für die "Prävention vor Datenverlust" für Security Agents konfiguriert werden.

Es werden folgende Themen behandelt:

- *Prävention vor Datenverlust (Data Loss Prevention, DLP) auf Seite 19-2*
- *Richtlinie für die Prävention vor Datenverlust konfigurieren auf Seite 19-3*

Prävention vor Datenverlust (Data Loss Prevention, DLP)

Der Schwerpunkt herkömmlicher Sicherheitslösungen liegt darin, zu verhindern, dass externe Sicherheitsbedrohungen in das Netzwerk eindringen. In der heutigen Sicherheitsumgebung deckt dies nur einen Teil der erforderlichen Aufgaben ab. Datenschutzverletzungen, die vertrauliche und sensitive Daten (digitale Assets) einer Organisation an außenstehende unbefugte Dritte weitergeben, sind heute gang und gäbe. Gründe für eine Datenschutzverletzung können Fehler oder Sorglosigkeit interner Mitarbeiter, Datenauslagerung, gestohlene oder verlegte Computer oder bösartige Angriffe sein.

Datenschutzverletzungen können:

- Das Markenimage schädigen
- Das Vertrauen der Kunden in das Unternehmen schwächen
- Unnötige Kosten für Schadenswiedergutmachung und Strafen wegen Richtlinienverstößen verursachen
- Zum Verlust von Geschäftschancen und zu Umsatzeinbußen durch entwendetes geistiges Eigentum führen

Auf Grund der Zunahme der schädlichen Auswirkungen durch Datenschutzverletzungen sehen Unternehmen mittlerweile den Schutz ihrer digitalen Assets als eine kritische Komponente in ihrer Sicherheitsinfrastruktur.

Die Funktion "Prävention vor Datenverlust" schützt die vertraulichen Daten eines Unternehmens vor versehentlichen oder beabsichtigten Lecks. Die Funktion "Prävention vor Datenverlust" ermöglicht Folgendes:

- Vertrauliche Informationen, die geschützt werden müssen, mit Hilfe von Datenbezeichnern identifizieren
- Richtlinien erstellen, die die übertragung von digitalen Assets über gemeinsam genutzte übertragungskanäle wie E-Mail und externe Geräte einschränken oder verhindern

- Die Einhaltung bewährter Datenschutzstandards durchsetzen

Um vertrauliche Informationen hinsichtlich eines potentiellen Verlusts überwachen zu können, müssen Sie die folgenden Fragen beantworten können:

- Welche Daten müssen vor unberechtigten Benutzern geschützt werden?
- Wo befinden sich die sensiblen Daten?
- Wie werden die sensiblen Daten übertragen?
- Welche Benutzer sind berechtigt, auf die sensiblen Daten zuzugreifen oder diese zu übertragen?
- Welche Maßnahmen sollten ergriffen werden, wenn eine Sicherheitsverletzung auftritt?

Diese wichtige Überprüfung betrifft in der Regel mehrere Abteilungen und Mitarbeiter, die mit den sensiblen Informationen in Ihrer Organisation vertraut sind.

Wenn Sie Ihre vertraulichen Informationen und Sicherheitsrichtlinien bereits definiert haben, können Sie damit beginnen, Datenbezeichner und Unternehmensrichtlinien zu definieren.

Richtlinie für die Prävention vor Datenverlust konfigurieren

Prozedur

1. Klicken Sie auf die Registerkarte **Externe Agents**, um eine Richtlinie für externe Agents zu konfigurieren, oder auf die Registerkarte **Interne Agents**, um eine Richtlinie für interne Agents zu konfigurieren.

   Hinweis

   Konfigurieren Sie die Einstellungen zum Agent-Standort, wenn dies noch nicht vorgenommen wurde. Agents verwenden diese Standorteinstellungen, um die richtige Richtlinie für die Funktion "Prävention vor Datenverlust" festzulegen.

2. Wählen Sie**'Prävention vor Datenverlust' aktivieren**.
3. Wählen Sie eine der folgenden Optionen aus:
   - Auf der Registerkarte **Externe Agents** können Sie alle Einstellungen für die Funktion "Prävention vor Datenverlust" auf interne Agents anwenden, indem Sie die Option **Alle Einstellungen für interne Agents übernehmen** auswählen.
   - Auf der Registerkarte **Interne Agents** können Sie alle Einstellungen für die Funktion "Prävention vor Datenverlust" auf externe Agents anwenden, indem Sie die Option **Alle Einstellungen für externe Agents übernehmen** auswählen.
4. Die Regeln, die von der Funktion "Prävention vor Datenverlust" auf die Richtlinie angewendet werden, werden auf der Registerkarte **Regeln** verwaltet.

Aufgabe	Beschreibung
Neue Regel hinzufügen	Klicken Sie auf **Hinzufügen**, um eine Regel zu erstellen, die auf die Richtlinie angewendet wird. Weitere Informationen finden Sie unter *Regeln für die Funktion "Prävention vor Datenverlust" konfigurieren auf Seite 19-5*.
Vorhandene Regeleinstellungen kopieren	Wählen Sie eine vorhandene Regel aus und klicken Sie auf **Kopieren**, um das Fenster **Einstellungen der Richtlinien für 'Prävention vor Datenverlust'** zu öffnen. Ändern Sie die Regeleinstellungen nach Bedarf.
Vorhandene Regeln löschen	Wählen Sie eine vorhandene Regel aus und klicken Sie auf **Löschen**, um die Regel aus der Liste zu entfernen.
Vorhandene Regeln ändern	Klicken Sie auf den Namen einer vorhandenen **Regel**, um die Einstellungen zu ändern.
Vorhandene Regeln aktivieren/ deaktivieren	Klicken Sie auf die Schaltfläche unter der Spalte **Aktivieren**, um eine Regel für die Richtlinie zu aktivieren oder zu deaktivieren.

Hinweis

Eine Richtlinie darf maximal 40 Regeln enthalten.

5. Klicken Sie auf die Registerkarte **Ausnahmen**, und konfigurieren Sie die erforderlichen Ausnahmeeinstellungen.

   Weitere Informationen finden Sie unter *Ausnahmen für Prävention vor Datenverlust auf Seite 19-15*.

Regeln für die Funktion "Prävention vor Datenverlust" konfigurieren

Hinweis

Die Prävention vor Datenverlust verarbeitet Regeln und Vorlagen anhand der Priorität. Wenn für eine Regel „Übergehen“ festgelegt ist, wird von der Prävention vor Datenverlust die nächste Regel in der Liste verarbeitet. Wenn für eine Regel „Sperren“ oder „Benutzerrechtfertigung“ festgelegt ist, wird die Benutzeraktion von der Prävention vor Datenverlust gesperrt oder akzeptiert, und diese Regel/Vorlage wird nicht weiter verarbeitet.

Prozedur

1. Wählen Sie **Diese Regel aktivieren**.
2. Geben Sie einen Namen für diese Regel an.

   Konfigurieren Sie die Vorlageneinstellungen:

3. Klicken Sie auf die Registerkarte **Vorlage**.
4. Wählen Sie Vorlagen aus der Liste **Verfügbare Vorlagen**, und klicken Sie dann auf **Hinzufügen**.

   Zur Auswahl von Vorlagen:

   - Durch Klicken auf die Vorlagennamen können Sie mehrere Einträge auswählen. Der Name wird hervorgehoben.

- Verwenden Sie die Suchfunktion, wenn Sie nach einer bestimmten Vorlage suchen. Sie können den Namen der Vorlage vollständig oder teilweise eingeben.

Hinweis

Jede Regel darf maximal 200 Vorlagen enthalten.

Konfigurieren Sie die Kanaleinstellungen:

5. Klicken Sie auf die Registerkarte **Kanal**.
6. Wählen Sie die Kanäle für die Richtlinie aus.

   Weitere Informationen über Kanäle finden Sie unter *Netzwerkkanäle auf Seite 19-8* und *System- und Anwendungskanäle auf Seite 19-10*.
7. Wenn Sie einen der Netzwerkkanäle ausgewählt haben, wählen Sie den Übertragungsbereich:
   - **Alle Übertragungen**
   - **Nur Übertragungen außerhalb des lokalen Netzwerks**

   Unter *Übertragungsumfang und -ziele für Netzwerkkanäle auf Seite 19-7* finden Sie weitere Informationen über den übertragungsumfang, wie Ziele abhängig vom übertragungsumfang funktionieren und wie Ziele korrekt definiert werden.
8. Wenn Sie **E-Mail-Clients** ausgewählt haben:
   a. Klicken Sie auf **Ausnahmen**.
   b. Geben Sie überwachte und nicht-überwachte interne E-Mail-Domänen an.

      Informationen über überwachte und nicht-überwachte E-Mail-Domänen finden Sie unter *E-Mail-Clients auf Seite 19-8*.
9. Wenn Sie **Wechseldatenträger** ausgewählt haben:
   a. Klicken Sie auf **Ausnahmen**.

b. Fügen Sie nicht-überwachte Wechseldatenträger hinzu, indem Sie sie anhand der jeweiligen Hersteller ermitteln. Die Modellbezeichnung und die serielle ID des Geräts sind optional.

Die Liste der zulässigen USB-Geräte unterstützt die Verwendung des Sterns (*) als Platzhalter. Verwenden Sie den Stern (*) in beliebigen Feldern, um alle Geräte einzuschließen, die den Kriterien der übrigen Felder entsprechen.

Beispiel: [Hersteller]-[Modell]-* platziert alle Geräte des angegebenen Herstellers und Modells in die Liste der zulässigen Geräte, unabhängig von der Seriennummer.

c. Um weitere Geräte hinzuzufügen, klicken Sie auf das Plus-Symbol (+).

Konfigurieren Sie die Aktionseinstellungen:

10. Klicken Sie auf die Registerkarte **Aktion**.

11. Wählen Sie eine primäre Aktion und weitere zusätzliche Aktionen. Weitere Informationen über Aktionen finden Sie unter *Aktionen der Funktion "Prävention vor Datenverlust" auf Seite 19-11*.

12. Nach der Konfiguration der Einstellungen für **Vorlage**, **Kanal** und **Aktion** klicken Sie auf **Speichern**.

Übertragungsumfang und -ziele für Netzwerkkanäle

Mit dem Übertragungsumfang und den Übertragungszielen werden die Datenübertragungen in Netzwerkkanälen definiert, die die Funktion "Prävention vor Datenverlust" überwachen muss. Bei zu überwachenden Übertragungen überprüft die Funktion "Prävention vor Datenverlust", ob Datenbezeichner vorhanden sind, bevor die Übertragung zugelassen oder gesperrt wird. Bei nicht zu überwachenden Übertragungen überprüft die Funktion "Prävention vor Datenverlust" nicht, ob Datenbezeichner vorhanden sind, und lässt die Übertragung sofort zu.

Netzwerkkanäle

Prävention vor Datenverlust kann die Datenübertragung durch die folgenden Netzwerkkanäle überwachen:

- E-Mail-Clients
- FTP
- HTTP und HTTPS
- IM-Anwendungen
- SMB-Protokoll
- Webmail

Um festzulegen, welche Datenübertragungen überwacht werden sollen, überprüft die Funktion "Prävention vor Datenverlust" den Übertragungsumfang, den Sie konfigurieren müssen. Abhängig vom ausgewählten Umfang überwacht die Funktion "Prävention vor Datenverlust" alle Datenübertragungen oder nur Übertragungen außerhalb des lokalen Netzwerks (LAN).

E-Mail-Clients

Prävention vor Datenverlust überwacht E-Mails, die über verschiedene E-Mail-Clients gesendet werden. Prävention vor Datenverlust überprüft den Betreff, den Inhalt und die Anhänge der E-Mail auf Datenbezeichner. Eine Liste der unterstützten E-Mail-Clients finden Sie im Dokument *Datenschutzlisten* unter:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Die überwachung findet dann statt, wenn der Benutzer versucht, eine E-Mail zu versenden. Enthält die E-Mail Datenbezeichner, wird das Versenden der E-Mail von der Funktion "Prävention vor Datenverlust" zugelassen oder gesperrt.

Sie können nicht überwachte interne E-Mail-Domänen und überwachte Subdomänen festlegen.

- **Non-monitored email domains**: Prävention vor Datenverlust ermöglicht sofort die Übertragung von E-Mails, die an nicht überwachte Domains gesendet werden.

  Hinweis

  Datenübertragungen an nicht überwachte E-Mail-Domänen und an überwachte E-Mail-Subdomänen, bei denen die Aktion "überwachen" gilt, sind insofern vergleichbar, als die übertragung zulässig ist. Der einzige Unterschied besteht darin, dass die Funktion "Prävention vor Datenverlust" bei nicht überwachten E-Mail-Domänen die Übertragung nicht protokolliert, während die Übertragung bei überwachten E-Mail-Subdomänen immer protokolliert wird.

- **Monitored email subdomains**: Wenn die Funktion "Prävention vor Datenverlust" die Übertragung einer E-Mail an eine überwachte Subdomäne erkennt, wird die Aktion hinsichtlich der Richtlinie überprüft. Je nach Aktion wird die Übertragung zugelassen oder gesperrt.

  Hinweis

  Wenn Sie E-Mail-Clients als überwachten Kanal auswählen, muss eine E-Mail mit einer Richtlinie übereinstimmen, damit sie überwacht wird. Im Gegensatz dazu wird eine E-Mail, die an überwachte E-Mail-Subdomänen gesendet wird, selbst dann automatisch überwacht, wenn sie nicht mit einer Richtlinie übereinstimmt.

Geben Sie Domänen in einem der folgenden Formate an. Trennen Sie mehrere Domänen durch Kommas:

- X400-Format, z. B. /O=Trend/OU=USA, /O=Trend/OU=China
- E-Mail-Domänen, z. B. `example.com`

Bei E-Mail-Nachrichten, die über das SMTP-Protokoll gesendet werden, überprüft die Funktion "Prävention vor Datenverlust", ob der Ziel-SMTP-Server in den folgenden Listen enthalten ist:

1. überwachte Ziele
2. Nicht überwachte Ziele
3. Nicht überwachte E-Mail-Domänen
4. überwachte E-Mail-Subdomänen

Wenn also eine E-Mail an einen SMTP-Server auf der Liste der überwachten Ziele gesendet wird, wird die E-Mail überwacht. Wenn sich der SMTP-Server nicht auf der Liste überwachter Ziele befindet, überprüft die Funktion "Prävention vor Datenverlust" die anderen Listen.

Bei E-Mails, die über andere Protokolle gesendet werden, überprüft die Funktion "Prävention vor Datenverlust" nur die folgenden Listen:

1. Nicht überwachte E-Mail-Domänen
2. überwachte E-Mail-Subdomänen

System- und Anwendungskanäle

Die Funktion "Prävention vor Datenverlust" kann folgende System- und Anwendungskanäle überwachen:

- Cloud Storage Services
- Datenspeicher (CD/DVD)
- Peer-to-Peer-Anwendungen
- PGP-Verschlüsselung
- Drucker
- Wechseldatenträger
- Synchronisierungssoftware (ActiveSync)
- Windows-Zwischenablage

Gerätelisten-Tool

Führen Sie Device List an jedem Endpunkt lokal aus, um externe Geräte abzufragen, die mit dem Endpunkt verbunden sind. Das Tool überprüft

einen Endpunkt nach externen Geräten und zeigt die entdeckten Geräte dann in einem Browser-Fenster an. Diese Informationen können Sie zur Konfiguration von Geräteeinstellungen bei der Funktion "Prävention vor Datenverlust" und der Gerätesteuerung verwenden.

Das Gerätelisten-Tool ausführen

Prozedur

1. Gerätelisten-Tool lokalisieren.
   - Gehen Sie auf dem Zielendpunkt, auf dem Security Agent installiert ist, zu `C:\Windows\System32\dgagent\listDeviceInfo.exe`.
   - Holen Sie `listDeviceInfo.zip` vom Support-Portal und extrahieren Sie das Paket auf dem Zielendpunkt.

     https://success.trendmicro.com/en-US/solution/KA-0008546
2. Führen Sie auf dem Endpunkt `listDeviceInfo.exe` aus.
3. Es öffnet sich ein Browser-Fenster mit Informationen zu den Geräten. Die Funktion 'Prävention vor Datenverlust' und die Gerätesteuerung verwenden folgende Informationen:
   - Hersteller (erforderlich)
   - Modell (optional)
   - Seriennummer (optional)

Aktionen der Funktion "Prävention vor Datenverlust"

Wenn die Prävention vor Datenverlust die Übertragung von Datenbezeichnern entdeckt, überprüft es, ob die entsprechenden Richtlinien eingehalten werden, und führt dann den Vorgang richtliniengemäß durch.

Die folgende Tabelle listet die Aktionen zur Prävention vor Datenverlust auf.

TABELLE 19-1. Aktionen der Funktion "Prävention vor Datenverlust"

AKTION	BESCHREIBUNG
Aktionen	
Übergehen	Die Prävention vor Datenverlust erlaubt und protokolliert die Übertragung.
Sperren	Die Prävention vor Datenverlust sperrt und protokolliert die Übertragung.
Zusätzliche Aktionen	
Agent-Benutzer benachrichtigen	Die Prävention vor Datenverlust benachrichtigt den Benutzer, ob die Datenübertragung stattgefunden hat oder gesperrt wurde.
Daten aufzeichnen	Unabhängig von der primären Aktion zeichnet die Prävention vor Datenverlust die vertraulichen Informationen im Ordner `<Security Agent installation folder>\DLPLite\Forensic` auf. Wählen Sie diese Aktion, um vertrauliche Informationen zu überprüfen, die von der Funktion "Prävention vor Datenverlust" gekennzeichnet werden. Aufgezeichnete vertrauliche Informationen können zu viel Festplattenspeicherplatz verbrauchen. Daher empfiehlt Trend Micro dringend, dass Sie diese Option nur für hochsensible Informationen wählen.
Verschlüsselt unterstützte Kanäle mit dem angegebenen Schlüssel/Kennwort (nur verfügbar, wenn Endpoint Encryption installiert ist)	Wenn Trend Micro Endpoint Encryption neben dem Security Agents installiert ist, kann Prävention vor Datenverlust Dateien automatisch verschlüsseln, bevor diese von einem Benutzer an einen anderen Speicherort weitergegeben werden können. Wenn Endpoint Encryption nicht installiert ist, führt Prävention vor Datenverlust eine Aktion zum Sperren der Dateien durch. Wählen Sie einen der folgenden Verschlüsselungsschlüssel oder ein festes Kennwort aus: • **Benutzerschlüssel**: Dieser auch als **lokaler Schlüssel** bezeichneter Schlüssel ist eindeutig für jeden Benutzer und beschränkt den Zugriff auf die verschlüsselte Datei für den Benutzer, der die Datei erstellt hat.

Aktion	Beschreibung
Hinweis Diese Option ist nur für Wechseldatenträger- und Cloud-Speicher-Kanäle und bei Auswahl der Aktion **übergehen** verfügbar. **Wichtig** Die Dateiverschlüsselungsfunktion in Endpoint Encryption ist veraltet und möglicherweise nicht für neue Installationsinstanzen verfügbar.	• **Gemeinsamer Schlüssel**: Dieser Schlüssel bezieht sich auf den **Gruppenschlüssel** oder **Unternehmensschlüssel** und der Endpoint Encryption Administrator konfiguriert den Typ unter Verwendung der PolicyServer MMC. • **Festgelegtes Kennwort**: Benutzer geben manuell ein festes Kennwort an, wenn Sie auf dem Bildschirm dazu aufgefordert werden. Endpoint Encryption erstellt ein selbstextrahierendes Paket, auf das Benutzer nach Eingabe des Verschlüsselungskennworts von allen Endpunkten aus zugreifen können.

Aktion	Beschreibung
	Wichtig • Auf dem Ziel-Endpunkt muss Endpoint Encryption installiert sein und der Benutzer muss sich bei Endpoint Encryption anmelden, um die Daten zu verschlüsseln. • Verschlüsselte Dateien auf USB-Geräten werden auf die Prävention vor Datenverlust hin durchsucht, wenn Benutzer die Dateien zu entschlüsseln versuchen. Wenn Sie auf einem USB-Gerät Dateien entschlüsseln, die vertrauliche Daten enthalten, wird das USB-Verschlüsselungsprotokoll ausgelöst. Die vertraulichen Daten müssen dann (erneut) verschlüsselt werden. Um zu verhindern, dass die Daten durch die Funktion zur Prävention vor Datenverlust erneut verschlüsselt werden, verschieben Sie die verschlüsselten Dateien auf ein lokales Laufwerk, bevor Sie versuchen, auf die Daten zuzugreifen. • Bei Verwendung eines Web-Clients blockiert Prävention vor Datenverlust Versuche, Dateien in den Cloud Storage hochzuladen. Verschlüsseln Sie die Dateien manuell, bevor Sie den Upload mit einem Web-Client durchführen.
Benutzerrechtfertigung **Hinweis** Diese Option steht nur nach der Auswahl der Aktion **Sperren** zur Verfügung.	Die Prävention vor Datenverlust fordert den Benutzer zur Bestätigung auf, bevor die Aktion „Sperren“ ausgeführt wird. Der Benutzer kann die Aktion „Sperren“ überschreiben, indem er erläutert, weshalb die vertraulichen Daten sicher sind. Es gibt die folgenden Rechtfertigungsgründe: • **Dies ist Bestandteil eines etablierten Geschäftsvorgangs.**

Aktion	Beschreibung
	• **Mein Vorgesetzter hat die Datenübertragung genehmigt.** • **Die Daten in dieser Datei sind nicht vertraulich.** • **Andere**: Die Benutzer geben in das entsprechende Textfeld eine andere Erklärung ein.

Ausnahmen für Prävention vor Datenverlust

Ausnahmen für die Prävention vor Datenverlust gelten für die gesamte Richtlinie, einschließlich aller in der Richtlinie definierten Regeln. Die Prävention vor Datenverlust wendet die Ausnahme-Einstellungen auf alle Übertragungen an, bevor nach digitalen Assets gesucht wird. Wenn eine Übertragung einer der Ausnahmeregeln entspricht, wird sie umgehend von der Prävention vor Datenverlust zugelassen oder durchsucht (je nach Ausnahmetyp).

Nicht überwachte und überwachte Ziele definieren

Definieren Sie die nicht überwachten und die überwachten Ziele anhand des Übertragungsbereichs, der auf der Registerkarte **Kanal** konfiguriert ist. Details zur Definition nicht überwachter und überwachter Ziele für **Alle Übertragungen** finden Sie unter *übertragungsumfang: Alle übertragungen auf Seite 19-16*. Details zur Definition nicht überwachter und überwachter Ziele für **Nur Übertragungen an Ziele außerhalb des lokalen Netzwerks** finden Sie unter *übertragungsumfang: Nur übertragungen außerhalb des lokalen Netzwerks auf Seite 19-18*.

Befolgen Sie diese Richtlinien beim Definieren von überwachten und nicht überwachten Zielen:

1. Definieren Sie jedes Ziel nach:
    - IP-Adresse
    - Host-Name
    - FQDN

- Netzwerkadresse und Subnetzmaske, z. B. 10.1.1.1/32

Hinweis

Bei der Subnetzmaske unterstützt die Prävention vor Datenverlust nur einen Port vom Typ klassenloses Inter-Domänen-Routing (CIDR). Das heißt, Sie können nur eine Zahl wie 32 anstelle von 255.255.255.0 eingeben.

2. Um bestimmte Kanäle anzusteuern, geben Sie die Standard- oder die vom Benutzer bzw. Unternehmen festgelegten Portnummern für diese Kanäle an. Port 21 ist z. B. typischerweise für FTP-, Port 80 für HTTP- und Port 443 für HTTPS-Datenverkehr bestimmt. Verwenden Sie einen Doppelpunkt, um das Ziel von den Portnummern zu trennen.
3. Sie können auch Portbereiche angeben. Um alle Ports einzubeziehen, ignorieren Sie den Portbereich.

   Nachstehend finden Sie einige Beispiele für Zieladressen mit Portnummern und Portbereichen:

   - 10.1.1.1:80
   - host:5-20
   - host.domain.com:20
   - 10.1.1.1/32:20
4. Fügen Sie zwischen den einzelnen Zielen jeweils ein Komma ein.

übertragungsumfang: Alle übertragungen

Prävention vor Datenverlust überwacht Daten, die außerhalb des Host-Computers übertragen werden.

Hinweis

Trend Micro empfiehlt die Wahl dieses Bereichs für externe Agents

Wenn Datenübertragungen zu bestimmten Zielen außerhalb des Host-Computers nicht überwacht werden sollen, definieren Sie folgende Punkte:

- **Non-monitored targets**: Prävention vor Datenverlust überwacht keine Daten, die an diese Ziele übertragen werden.

  Hinweis

  Datenübertragungen an nicht überwachte Ziele und an überwachte Ziele, bei denen die Aktion "überwachen" gilt, sind insofern vergleichbar, als die übertragung zulässig ist. Der einzige Unterschied besteht darin, dass die Funktion "Prävention vor Datenverlust" die Übertragung nicht protokolliert, während die Übertragung bei überwachten Zielen immer protokolliert wird.

- **Monitored targets**: Dies sind spezifische Ziele innerhalb der nicht überwachten Ziele, die überwacht werden sollten. Überwachte Ziele sind:
  - Optional, wenn Sie nicht überwachte Ziele definiert haben.
  - Nicht konfigurierbar, wenn Sie keine nicht überwachten Ziele festgelegt haben.

Beispiel:

Die folgenden IP-Adressen wurden der Rechtsabteilung Ihrer Firma zugewiesen:

- `10.201.168.1` zu `10.201.168.25`

Sie erstellen eine Richtlinie, mit der die Übertragung von Beschäftigungszertifikaten an alle Mitarbeiter mit Ausnahme der Vollzeitmitarbeiter der Rechtsabteilung überwacht wird. Wählen Sie hierzu als Übertragungsumfang **Alle Übertragungen** aus, und gehen Sie anschließend wie folgt vor:

Optionen	Schritte
Möglichkeit 1	1. Fügen Sie `10.201.168.1-10.201.168.25` zu den nicht überwachten Zielen hinzu. 2. Fügen Sie die IP-Adressen der Teilzeitmitarbeiter der Rechtsabteilung zu den überwachten Zielen hinzu. Angenommen, es gibt 3 IP-Adressen, `10.201.168.21-10.201.168.23`.
Möglichkeit 2	Fügen Sie die IP-Adressen der Vollzeitmitarbeiter der Rechtsabteilung zu den nicht überwachten Zielen hinzu: • `10.201.168.1-10.201.168.20` • `10.201.168.24-10.201.168.25`

Richtlinien zur Definition überwachter und nicht überwachter Ziele finden Sie unter *Nicht überwachte und überwachte Ziele definieren auf Seite 19-15*.

übertragungsumfang: Nur übertragungen außerhalb des lokalen Netzwerks

Prävention vor Datenverlust überwacht Daten, die an ein Ziel außerhalb des lokalen Netzwerks (LAN) übertragen werden.

Hinweis

Trend Micro empfiehlt die Wahl dieses Bereichs für interne Agents.

"Netzwerk" bezieht sich auf das Unternehmens- oder lokale Netzwerk. Dazu gehören das aktuelle Netzwerk (IP-Adresse des Endpunkts und Netzmaske) und die folgenden standardmäßigen privaten IP-Adressen:

- Klasse A: `10.0.0.0` bis `10.255.255.255`
- Klasse B: `172.16.0.0` bis `172.31.255.255`
- Klasse C: `192.168.0.0` bis `192.168.255.255`

Wenn Sie diesen übertragungsumfang auswählen, können Sie folgende Elemente definieren:

- **Non-monitored targets**: Definieren Sie Ziele außerhalb des LAN, die Sie als sicher betrachten und daher nicht überwacht werden sollten.

Hinweis

Datenübertragungen an nicht überwachte Ziele und an überwachte Ziele, bei denen die Aktion "überwachen" gilt, sind insofern vergleichbar, als die übertragung zulässig ist. Der einzige Unterschied besteht darin, dass die Funktion "Prävention vor Datenverlust" die Übertragung nicht protokolliert, während die Übertragung bei überwachten Zielen immer protokolliert wird.

- **Monitored targets**: Definieren Sie Ziele innerhalb des LAN, die Sie überwachen möchten.

Richtlinien zur Definition überwachter und nicht überwachter Ziele finden Sie unter *Nicht überwachte und überwachte Ziele definieren auf Seite 19-15*.

Dekomprimierungsregeln

Dateien, die komprimierte Dateien enthalten, können nach digitalen Assets durchsucht werden. Um die zu durchsuchenden Dateien zu ermitteln, wendet die Prävention vor Datenverlust folgende Regeln auf eine komprimierte Datei an:

- **Size of a decompressed file exceeds: __ MB (1-10240 MB)**
- **Komprimierungsebenen überschritten: __ (1–20)**
- **Number of files to scan exceeds: __ (1-2000)**

Teil VII

Apex One (Mac)-Widgets und Richtlinien

Kapitel 20

Apex One (Mac) Dashboard-Widgets

Dieser Abschnitt enthält Hilfethemen für die Apex One (Mac) Dashboard-Widgets, die in Trend Micro Apex Central unterstützt werden.

Es werden folgende Themen behandelt:

- *Leistungsindikatoren-Widget auf Seite 20-2*

Leistungsindikatoren-Widget

Verwenden Sie dieses Widget im Trend Micro Apex Central **Dashboard**-Fenster, um basierend auf ausgewählten Kriterien Leistungsindikatoren (KPI) für Apex One (Mac) anzuzeigen.

Informationen dazu, wie Sie ein Widget zum **Dashboard**-Fenster hinzufügen, finden Sie in der Dokumentation zu Trend Micro Apex Central oder Control Manager.

Tipp

Standardmäßig markiert das Widget bei 15 Vorkommnissen von Ereignissen diese als „Wichtig“ ( ) und bei 30 Vorkommnissen als „Kritisch“ ( ).

Optional können Sie durch das Konfigurieren von Ereignisschwellenwerten Ereignisse als 'Wichtig' oder 'Kritisch' markieren.

Leistungsindikatoren konfigurieren

Greifen Sie in Trend Micro Apex Central oder Control Manager auf das Widget **Wichtigste Leistungsindikatoren für Apex One (Mac)** auf dem **Dashboard** zu, um die folgenden indikatorbezogenen Tasks durchzuführen.

TABELLE 20-1. KPI-Widget-Indikator-Tasks

AUFGABE	SCHRITTE
Neuen Indikator hinzufügen	1. Klicken Sie auf **Add Indicator**. Das Fenster **Add Indicator** wird angezeigt. 2. Wählen Sie eine Option aus dem Listenfeld **Name** und passen Sie ggfs. die Einstellungen an. 3. Klicken Sie auf **Save**.
Indikator bearbeiten	1. Klicken Sie auf den Indikator in der Liste. Das Fenster **Edit Indicator** wird angezeigt. 2. Passen Sie die Einstellungen an. 3. Klicken Sie auf **Save**.

Aufgabe	Schritte
Indikator löschen	1. Klicken Sie auf den Indikator in der Liste. Das Fenster **Edit Indicator** wird angezeigt. 2. Klicken Sie auf **Löschen**. 3. Klicken Sie auf **OK**.
Einstellungen für den Ereignisschwellenwert konfigurieren	1. Wählen Sie im Fenster **Add Indicator** oder **Edit Indicator** die Option **Enable alerts at the following thresholds** aus. 2. Geben Sie die Mindestanzahl an Ereignisvorkommen für jeden Ereignistyp ein. 3. Klicken Sie auf **Save**. **Hinweis** Das Symbol 'Wichtig' oder 'Kritisch' wird in der Spalte **Vorkommen** angezeigt, wenn beide der folgenden Aussagen wahr sind: • Die Anzahl der Ereignisvorkommen, die diesem Indikator entsprechen, ist gleich oder größer als der Schwellenwert. • **Warnungen bei folgendem Schwellenwert aktivieren** ist ausgewählt.

Widget-Einstellungen konfigurieren

Wählen Sie auf dem Trend Micro Apex Central oder im Control Manager **Dashboard** Bildschirm **Widget-Einstellungen** im Menü im oberen rechten Bereich des Widgets, um die folgenden Tasks durchzuführen.

Tabelle 20-2. KPI-Widget-Einstellungen

Aufgabe	Schritte
Widget-Titel bearbeiten	Geben Sie den Widget-Titel in das Textfeld ein.

AUFGABE	SCHRITTE
Tägliche Update-Zeit konfigurieren	Wählen Sie im Listenfeld die Stunde aus, zu der die Widget-Daten täglich erzeugt werden sollen. **Tipp** Klicken Sie auf das Aktualisierungssymbol ( ), um die Widget-Daten manuell zu aktualisieren.

Kapitel 21

Apex One (Mac)-Richtlinieneinstellungen

In diesem Abschnitt wird die Konfiguration von Richtlinieneinstellungen für Trend Micro Apex One (Mac) in Apex Central beschrieben.

Es werden folgende Themen behandelt:

Anti-Malware-Suchen

In diesem Abschnitt wird beschrieben, wie die Anti-Malware-Suche auf macOS Security Agents konfiguriert wird.

Verwenden Sie die Bildschirme in diesem Abschnitt, um die Suchmethode, die Überwachungsstufe und den Suchtyp zu konfigurieren.

Apex One (Mac) stellt die folgenden Suchtypen bereit, um Endpunkte vor Sicherheitsrisiken zu schützen:

Suchtyp	Beschreibung
Echtzeitsuche	Beim Empfangen, Öffnen, Herunterladen, Kopieren oder Ändern einer Datei wird diese automatisch durchsucht. Weitere Informationen finden Sie unter *Echtzeitsuche auf Seite 21-8*.
Manuelle Suche	Eine vom Benutzer eingeleitete Suche, bei der eine vom Benutzer angeforderte Datei oder ein Dateisatz durchsucht wird. Weitere Informationen finden Sie unter *Manuelle Suche auf Seite 21-14*.
Zeitgesteuerte Suche	Dateien auf dem Endpunkt werden automatisch gemäß dem vom Administrator festgelegten Zeitplan durchsucht. Weitere Informationen finden Sie unter *Zeitgesteuerte Suche auf Seite 21-20*.
Jetzt durchsuchen	Eine vom Administrator gestartete Suche, bei der Dateien auf einem oder mehreren Zielendpunkten durchsucht werden.

Allgemeine Einstellungen

Der Bildschirm für Allgemeine Einstellungen ist der Ort, an dem Sie die **Suchmethoden** und **Überwachungsstufe** für Ihre macOS-Agenten konfigurieren können.

Bei der Suche nach Sicherheitsrisiken können Security Agents eine von zwei Suchmethoden anwenden: Die Suchmethoden sind intelligente Suche und herkömmliche Suche.

- **Intelligente Suche**

Security Agents, die die intelligente Suche anwenden, werden in diesem Dokument als „Smart Scan Agents“ bezeichnet. Smart Scan Agents nutzen die lokale Suche und webbasierte Abfragen, die von File Reputation-Diensten bereitgestellt werden.

Dies ist der standardmäßige Suchmethodentyp.

- **Herkömmliche Suche**

  Agents, die keinen Smart Scan durchführen, werden als „Herkömmliche Suchagenten“ bezeichnet. Ein Agent der herkömmlichen Suche speichert alle Komponenten von Apex One (Mac) auf dem Agent-Endpunkt und durchsucht alle Dateien lokal.

Das Überwachungsniveau ist der Grad der Wachsamkeit und Strenge, der bei der Erkennung und Reaktion auf mögliche Bedrohungen angewendet wird. Eine Erhöhung des Niveaus steigert die Empfindlichkeit des Sensors, was die Anzahl der Erkennungen und Warnungen erhöht. Höhere Niveaus ermöglichen eine strengere Überwachung, um bei Situationen wie laufenden Bedrohungsuntersuchungen zu helfen, können jedoch eine große Anzahl nicht wesentlicher Protokolle erzeugen und die Leistung des Endpunkts beeinträchtigen. Trend Micro empfiehlt, das Überwachungsniveau auf 2 - Moderat einzustellen, um relevantere Daten mit minimaler Auswirkung auf Ihre Endpunkte auszugleichen. Einige Komponenten, die von höheren Überwachungsniveaus verwendet werden, sind nicht auf allen Plattformen verfügbar.

Suchmethoden im Vergleich

Die folgende Tabelle beinhaltet einen Vergleich zwischen den beiden Suchmethoden:

Tabelle 21-1. Vergleich zwischen herkömmlicher Suche und intelligenter Suche

Vergleichsgrundlage	Herkömmliche Suche	Intelligente Suche
Suchverhalten	Die herkömmliche Suche agent durchsucht den lokalen endpoint.	• Der intelligente Suchagent durchsucht den lokalen Endpunkt. • Wenn der Security Agent das Risiko der Datei während der Suche nicht ermitteln kann, überprüft Security Agent dies, indem er eine Suchabfrage an eine Smart Protection-Quelle sendet. • Der Security Agent legt die Ergebnisse der Suchabfrage zur Verbesserung der Suchleistung in einem Zwischenspeicher ab.
Verwendete und aktualisierte Komponenten	Alle unter der Update-Adresse verfügbaren Komponenten, außer dem Mac-Heuristik-Pattern und dem Agent-Pattern der intelligenten Suche.	Alle unter der Update-Adresse verfügbaren Komponenten, außer dem Viren-Pattern und dem Spyware-Aktivmonitor-Pattern.
Typische Update-Adresse	Apex One (Mac) Server	Apex One (Mac) Server

Wechsel von der intelligenten Suche zur herkömmlichen Suche

Die folgende Tabelle enthält weitere Überlegungen zur Umstellung von Agents auf die herkömmliche Suche:

Tabelle 21-2. Überlegungen bei der Umstellung auf die herkömmliche Suche

Überlegung	Details
Anzahl der umzuschaltenden Security Agents	Wenn Sie eine relativ kleine Anzahl von Security Agents gleichzeitig umschalten, werden die Ressourcen von Apex One (Mac) Server und Smart Protection Server effizient genutzt. Diese Server können andere wichtige Aufgaben ausführen, während Security Agents ihre Suchmethoden ändern.

Überlegung	Details
Timing	Wenn Sie wieder zur herkömmlichen Suche wechseln, wird Security Agents wahrscheinlich die vollständige Version des Viren-Patterns und des Spyware-Aktivmonitor-Patterns vom Server mit Apex One (Mac) herunterladen. Diese Pattern-Dateien werden nur von den Agents der herkömmlichen Suche verwendet. Die Umschaltung sollte bei geringem Netzaufkommen durchgeführt werden, um sicherzustellen, dass der Download-Prozess in kurzer Zeit beendet wird. Außerdem sollten Sie dann umschalten, wenn keine Aktualisierung eines Security Agent über den Server geplant ist.
Einstellungen der Agent-Hierarchie	Die Suchmethode ist eine granuläre Einstellung, die auf Stamm- oder Domänenebene oder für einzelne Agents festgelegt werden kann. Bei der Umschaltung zur herkömmlichen Suche können Sie Folgendes tun: • Erstellen Sie eine neue Gruppe und ordnen Sie die herkömmliche Suche als Suchmethode zu. Alle Security Agent, die Sie in diese Gruppe verschieben, werden die herkömmliche Suche verwenden. Wenn Sie den Security Agent verschieben, aktivieren Sie die Einstellung **Einstellungen der neuen Gruppe auf ausgewählte Agenten anwenden**. • Wählen Sie eine Gruppe aus, und konfigurieren Sie diese zur Verwendung der herkömmlichen Suche. Agents der intelligenten Suche, die der Gruppe angehören, werden auf die herkömmliche Suche umgestellt. • Wählen Sie einen oder mehrere Agents der herkömmlichen Suche aus einer Gruppe aus, und stellen Sie diese dann auf die intelligente Suche um. **Hinweis** Alle Änderungen an der Suchmethode der Gruppe überschreiben die Suchmethode, die Sie für individuelle Security Agents konfiguriert haben.

Wechsel von der herkömmlichen Suche zur intelligenten Suche

Wenn Sie Security Agents von der herkömmlichen Suche auf die intelligente Suche umstellen, stellen Sie sicher, dass Smart Protection-Dienste auf dem Apex One-Server eingerichtet sind. Weitere Informationen finden Sie in der Apex One-Dokumentation.

Die folgende Tabelle bietet weitere Überlegungen beim Wechsel von Security Agent zur intelligenten Suche.

TABELLE 21-3. Überlegungen bei der Umstellung auf die intelligente Suche

ÜBERLEGUNG	DETAILS
Produktlizenz	Um die intelligente Suche zu verwenden, vergewissern Sie sich, dass Sie die Lizenzen für die folgenden Dienste auf dem Apex One Server aktiviert haben und die Lizenzen nicht abgelaufen sind: • Virenschutz • Web Reputation und Anti-Spyware
Apex One (Mac) Server	Stellen Sie sicher, dass Security Agents eine Verbindung zum Apex One (Mac)-Server herstellen kann. Nur online Security Agents werden benachrichtigt, um auf intelligente Suche umzuschalten. Offline Security Agents werden benachrichtigt, wenn sie online gehen. Roaming Security Agents werden benachrichtigt, wenn sie online gehen oder, falls der Security Agent Berechtigungen für zeitgesteuerte Updates hat, wenn das zeitgesteuerte Update ausgeführt wird.
Anzahl der umzuschaltenden Security Agents	Wenn Sie eine relativ kleine Anzahl von Security Agents gleichzeitig umschalten, werden die Ressourcen des Apex One (Mac) Servers effizient genutzt. Der Apex One (Mac) Server kann andere wichtige Aufgaben ausführen, während Security Agents ihre Suchmethoden ändern.

Überlegung	Details
Timing	Wenn Sie zum ersten Mal zu Smart Scan wechseln, müssen Security Agents die Vollversion des Mac Heuristic Pattern und des Smart Scan Agent Pattern vom Server mit Apex One (Mac) herunterladen. Das Smart Scan Pattern wird nur von Smart Scan-Agents verwendet. Die Umschaltung sollte bei geringem Netzaufkommen durchgeführt werden, um sicherzustellen, dass der Download-Prozess in kurzer Zeit beendet wird. Außerdem sollten Sie dann umschalten, wenn keine Aktualisierung eines Security Agent über den Server geplant ist.
Einstellungen der Agent-Hierarchie	Die Suchmethode ist eine granuläre Einstellung, die auf Stamm- oder Gruppenebene oder für einzelne Agents festgelegt werden kann. Bei der Umschaltung zur intelligenten Suche können Sie Folgendes tun: • Erstellen Sie eine neue Gruppe und ordnen Sie die intelligente Suche als Suchmethode zu. Alle Security Agent, die Sie in diese Gruppe verschieben, werden die intelligente Suche verwenden. Wenn Sie den Security Agent verschieben, aktivieren Sie die Einstellung **Einstellungen der neuen Gruppe auf ausgewählte Agenten anwenden**. • Wählen Sie eine Gruppe aus, und konfigurieren Sie diese zur Verwendung der intelligenten Suche. Agents der herkömmlichen Suche, die der Gruppe angehören, werden auf die intelligente Suche umgestellt. • Wählen Sie einen oder mehrere Agents der herkömmlichen Suche aus einer Gruppe aus, und stellen Sie diese dann auf die intelligente Suche um. **Hinweis** Alle Änderungen an der Suchmethode der Gruppe überschreiben die Suchmethode, die Sie für individuelle Security Agents konfiguriert haben.

Überlegung	Details
IPv6-Unterstützung	Die Agents der intelligenten Suche senden Suchabfragen an Smart Protection Quellen. Ein reiner IPv6-Agent der intelligenten Suche kann Abfragen nicht direkt an IPv4-Quellen senden wie zum Beispiel: • Smart Protection Server 3.0 (integriert oder eigenständig) • Trend Micro Smart Protection Network Entsprechend kann ein reiner IPv4-Agent der intelligenten Suche ebenfalls keine Abfragen an reine IPv6 Smart Protection Server senden. Ein Dual-Stack-Proxy-Server wie beispielsweise DeleGate, der IP-Adressen konvertieren kann, muss ermöglichen, dass Agents der intelligenten Suche eine Verbindung zu den Quellen herstellen können.

Echtzeitsuche

Die Echtzeitsuche wird kontinuierlich und dauerhaft ausgeführt. Bei jedem Empfang, Öffnen, Herunterladen, Kopieren oder Ändern einer Datei wird diese durch die Echtzeitsuche nach Sicherheitsrisiken durchsucht. Wenn Apex One (Mac) kein Sicherheitsrisiko erkennt, verbleibt die Datei an ihrem Speicherort und Benutzer können darauf zugreifen. Wenn Apex One (Mac) ein Sicherheitsrisiko entdeckt, wird eine Nachricht mit dem Namen der infizierten Datei und dem jeweiligen Sicherheitsrisiko angezeigt.

Sie können die Einstellungen für Echtzeitsuche für einen oder mehrere Agents und Gruppen bzw. für alle Security Agents, die vom Server verwaltet werden, konfigurieren und anwenden.

Einstellungen der Echtzeitsuche konfigurieren

Prozedur

1. Aktivieren Sie das Kontrollkästchen, um die Echtzeitsuche zu aktivieren.
2. Klicken Sie auf die Registerkarte **Ziel**, um die Dateiaktivitäten und die Sucheinstellungen zu konfigurieren.

Weitere Informationen finden Sie unter *Echtzeitsuche: Registerkarte "Ziel" auf Seite 21-9*.

3. Klicken Sie auf die Registerkarte **Aktion**, um die Suchaktionen zu konfigurieren, die Apex One (Mac) bei entdeckten Sicherheitsbedrohungen durchführen soll.

   Weitere Informationen finden Sie unter *Echtzeitsuche: Registerkarte "Aktion" auf Seite 21-10*.

Echtzeitsuche: Registerkarte "Ziel"

Prozedur

1. Unter **Benutzerdefinierte Aktionen für Dateien** wählen Sie Aktivitäten für Dateien aus, die die Echtzeitsuche auslösen. Wählen Sie unter folgenden Optionen:

   - **Dateien beim Erstellen/Ändern DURCHSUCHEN**: Durchsucht Dateien, die dem Endpunkt neu hinzugefügt werden (z. B. nach dem Herunterladen einer Datei) oder gerade verändert werden
   - **Dateien beim Abrufen/Ausführen DURCHSUCHEN**: Durchsucht Dateien, wenn sie geöffnet werden
   - **Dateien durchsuchen, die erstellt/bearbeitet und abgefragt/ausgeführt werden**
   - **Dateien durchsuchen, die erstellt/bearbeitet/ausgeführt werden**

   Angenommen, die dritte Option wird aktiviert: Wird eine neue Datei auf den Endpunkt heruntergeladen, wird sie durchsucht und bleibt an ihrem aktuellen Speicherort, wenn kein Sicherheitsrisiko entdeckt wird. Dieselbe Datei wird erneut durchsucht, wenn sie geöffnet wird und bevor etwaige Änderungen daran gespeichert werden.

2. Wählen Sie unter **Sucheinstellungen** eine oder mehrere der folgenden Optionen aus:

   - **Komprimierte Dateien durchsuchen**: Einzelne Dateien innerhalb einer Archivdatei durchsuchen

Weitere Informationen finden Sie unter *Unterstützte komprimierte Dateitypen auf Seite 21-11*.

- **Scan network drive**: Durchsucht Verzeichnisse, die sich physisch auf anderen Endpunkten befinden, aber dem lokalen Endpunkt zugeordnet sind

Echtzeitsuche: Registerkarte "Aktion"

Auf der Registerkarte **Aktionen** konfigurieren Sie die Suchaktionen, die Apex One (Mac) bei entdeckten Sicherheitsbedrohungen durchführen soll.

Prozedur

1. Geben Sie unter **Aktion** die Suchaktionen an.

Optionen	Beschreibung
ActiveAction verwenden	In ActiveAction sind mehrere vorkonfigurierte Aktionen für die Suche nach unterschiedlichen Arten von Sicherheitsrisiken zusammengefasst. Trend Micro empfiehlt die Verwendung von ActiveAction, wenn Sie nicht genau wissen, welche Suchaktion sich für einen bestimmten Typ von Sicherheitsrisiko am besten eignet. Die ActiveAction-Einstellungen werden in den Pattern-Dateien ständig aktualisiert, um Endpunkte gegen die neuesten Sicherheitsrisiken und Angriffsmethoden zu schützen.

Optionen	Beschreibung
Die gleiche Aktion für alle Typen von Sicherheitsrisiken verwenden	Wählen Sie diese Option, wenn dieselbe Aktion für alle Typen von Sicherheitsrisiken außer für wahrscheinliche Viren/Malware durchgeführt werden soll. Beim Typ „Wahrscheinlich Virus/ Malware“ erfolgt stets die Aktion „Übergehen“. Wenn Sie „Säubern“ als erste Aktion auswählen, geben Sie eine Ersatzaktion an, die Apex One (Mac) durchführt, falls das Säubern fehlschlägt. Nur wenn die erste Aktion „Säubern“ ist, ist eine zweite Aktion einstellbar. Details zu den Suchoptionen finden Sie unter *Suchaktionen auf Seite 21-12*.

2. Wählen Sie **Eine Benachrichtigung auf dem Agent anzeigen, wenn Viren-/Malware erkannt wird**, um eine Benachrichtigung anzuzeigen, wenn Apex One (Mac) während der Echtzeitsuche ein Sicherheitsrisiko erkennt.

Unterstützte komprimierte Dateitypen

Apex One (Mac) unterstützt die folgenden Komprimierungstypen.

Erweiterung	Typ
.zip	Mit Pkzip erstelltes Archiv
.rar	Mit RAR erstelltes Archiv
.tar	Mit Tar erstelltes Archiv
.arj	ARJ-komprimiertes Archiv
.hqx	BINHEX
.gz; .gzip	Gnu ZIP
.Z	LZW/16-Bit-komprimiert
.bin	MacBinary

Erweiterung	Typ
.cab	Microsoft Kabinettdatei
Microsoft-komprimiert/MSCOMP	
.eml; .mht	MIME
.td0	Teledisk Format
.bz2	Mit Unix BZ2 Bzip komprimierte Datei
.uu	UUEncode
.ace	WinAce

Suchaktionen

Geben Sie die Aktionen an, die Apex One (Mac) durchführt, wenn ein bestimmter Suchtyp ein Sicherheitsrisiko erkennt.

Die Aktion, die von Apex One (Mac) ausgeführt wird, ist abhängig vom Suchtyp, der das Sicherheitsrisiko erkannt hat. Wenn beispielsweise bei der manuellen Suche (Suchtyp) ein Sicherheitsrisiko von Apex One (Mac) erkannt wird, wird die infizierte Datei gesäubert (Aktion).

Apex One (Mac) kann die folgenden Aktionen bei Sicherheitsrisiken durchführen:

Suchaktion	Details
Löschen	Apex One (Mac) entfernt die infizierte Datei vom Endpunkt.

Suchaktion	Details
Quarantäne	Die infizierte Datei wird von Apex One (Mac) umbenannt und in das Quarantäneverzeichnis des Endpunkts `<Agent installation folder>/common/lib/vsapi/quarantine` verschoben. Nachdem die Datei in das Quarantäneverzeichnis verschoben wurde, kann Apex One (Mac) weitere Aktionen für diese Datei durchführen, je nachdem, welche Aktion vom Benutzer angegeben wurde. Apex One (Mac) kann die Datei säubern, löschen oder wiederherstellen. Die Datei wiederherzustellen bedeutet, dass sie an ihren ursprünglichen Speicherort zurückverschoben wird, ohne dass irgendeine Aktion ausgeführt wird. Benutzer können eine Datei wiederherstellen, wenn sie sich als unbedenklich herausstellt. Eine Datei zu säubern bedeutet, dass das Sicherheitsrisiko von der Datei in der Quarantäne entfernt wird und sie nach erfolgreicher Säuberung an ihren ursprünglichen Speicherort zurückverschoben wird.
Säubern	Apex One (Mac) entfernt das Sicherheitsrisiko aus einer infizierten Datei und ermöglicht dann erst den Zugriff darauf. Lässt sich die Datei nicht säubern, führt Apex One (Mac) zusätzlich eine der folgenden Aktionen aus: Quarantäne, Löschen oder Übergehen. Zum Konfigurieren der zweiten Aktion navigieren Sie zu **Agent-Verwaltung** > **Einstellungen** > **{Suchtyp}**, und klicken Sie auf die Registerkarte **Aktion**.

Suchaktion	Details
Übergehen	Apex One (Mac) führt keine Aktion für die infizierte Datei aus. Das erkannte Sicherheitsrisiko wird jedoch in den Protokolldateien verzeichnet. Die Datei wird nicht verschoben. Apex One (Mac) führt bei Dateien mit Infektionen des Typs „Wahrscheinlich Virus/Malware“ stets die Aktion „Übergehen“ aus, um das Risiko von Fehlalarmen zu verringern. Wenn weitere Analysen bestätigen, dass Viren/Malware wahrscheinlich tatsächlich ein Sicherheitsrisiko darstellen, wird ein neues Pattern veröffentlicht, damit Apex One (Mac) die entsprechende Suchaktion durchführen kann. Wenn sich wahrscheinliche Viren/Malware als unbedenklich herausstellen, werden diese nicht mehr entdeckt. Beispiel: Apex One (Mac) entdeckt „x_wahrscheinlicher_Virus“ in einer Datei „123.pdf“ und führt bei Fund keine Aktion durch. Trend Micro bestätigt anschließend, dass „x_wahrscheinlicher_Virus“ ein Trojaner ist und veröffentlicht eine neue Version des Viren-Patterns. Nach dem Laden der neuen Pattern-Version erkennt Apex One (Mac) „x_wahrscheinlicher_Virus“ als Trojaner und löscht „123.pdf“, wenn für diese Dateien die Aktion „Löschen“ festgelegt wurde. **Hinweis** Diese Aktion ist für die Echtzeitsuche nicht verfügbar.
Zugriff verweigern	Beim Versuch, eine Infizierte Datei zu öffnen oder auszuführen, wird dieser Vorgang durch Apex One (Mac) sofort gesperrt. Die infizierte Datei kann manuell gelöscht werden.

Manuelle Suche

Die manuelle Suche wird bei Bedarf gestartet, wenn der Benutzer sie in der Agent-Konsole aktiviert. Die Dauer der Suche hängt von der Anzahl der zu durchsuchenden Dateien und den Hardware-Ressourcen des Endpunkts ab.

Sie können die Einstellungen für die manuelle Suche für einen oder mehrere Security Agents und Gruppen bzw. für alle Security Agents, die vom Server verwaltet werden, konfigurieren und anwenden.

Einstellungen für manuelle Suche konfigurieren

Prozedur

1. Klicken Sie auf die Registerkarte **Ziel**, um die Einstellungen für die allgemeine Suche und die CPU-Nutzung zu konfigurieren.

   Weitere Informationen finden Sie unter *Manuelle Suche: Registerkarte "Ziel" auf Seite 21-15*.

2. Klicken Sie auf die Registerkarte **Aktion**, um die Suchaktionen zu konfigurieren, die Apex One (Mac) bei entdeckten Sicherheitsbedrohungen durchführen soll.

   Weitere Informationen finden Sie unter *Manuelle Suche: Registerkarte "Aktion" auf Seite 21-17*.

Manuelle Suche: Registerkarte "Ziel"

Prozedur

1. Wählen Sie im Abschnitt **Zu durchsuchende Dateien** eine der folgenden Optionen aus:

   - **Alle durchsuchbaren Dateien**: alle durchsuchbaren Dateien werden berücksichtigt. Zu den nicht durchsuchbaren Dateien gehören kennwortgeschützte und verschlüsselte Dateien sowie Dateien, die die vom Benutzer festgelegten Suchkriterien nicht erfüllen.

     Hinweis

     Das Durchsuchen jeder Datei erfordert viel Zeit und viele Ressourcen und ist möglicherweise in manchen Fällen gar nicht notwendig. Deshalb können Sie bei Bedarf die Anzahl der Dateien begrenzen, die der Security Agent durchsucht.

- **Nur Mach-O-Dateien durchsuchen**: Nur Mach-O-Dateien auf Endpunkten durchsuchen. Apex One (Mac) Security Agents durchsucht keine anderen Dateitypen auf Malware.

Hinweis

Wenn Sie diese Option auswählen, müssen Sie die Funktion für intelligente Suche aktivieren, um Schutz vor den neuesten Malware-Angriffen auf OS X- und macOS-Plattformen zu gewährleisten.

2. Wählen Sie unter **Sucheinstellungen** eine oder mehrere der folgenden Optionen aus:

   - **Komprimierte Dateien durchsuchen**: Einzelne Dateien innerhalb einer Archivdatei durchsuchen

     Weitere Informationen finden Sie unter *Unterstützte komprimierte Dateitypen auf Seite 21-11*.

   - **Scan network drive**: Durchsucht Verzeichnisse, die sich physisch auf anderen Endpunkten befinden, aber dem lokalen Endpunkt zugeordnet sind

   - **Zeitmaschine durchsuchen**: Nur Dateien auf Time Machine-Laufwerken durchsuchen

Hinweis

Nach dem Aktivieren der Option **Zeitmaschine durchsuchen** für die manuelle und zeitgesteuerte Suche kann Apex One (Mac) Malware-Bedrohungen nur erkennen. Aufgrund von Berechtigungseinschränkungen im Mac-Betriebssystem können keine entsprechenden Aktionen (Bereinigen, Quarantäne oder Löschen) ergriffen werden. Konfigurierte Suchaktionen werden in den Produktprotokollen als nicht erfolgreich angezeigt.

3. Konfigurieren Sie im Abschnitt **CPU-Auslastung** die erforderlichen Einstellungen.

- **Hoch**: Ohne Pause zwischen den Suchläufen
- **Niedrig**: Pause zwischen den Suchläufen, wenn die CPU-Auslastung über 20 % liegt, sonst keine Pause

Manuelle Suche: Registerkarte "Aktion"

Auf der Registerkarte **Aktionen** konfigurieren Sie die Suchaktionen, die Apex One (Mac) bei entdeckten Sicherheitsbedrohungen durchführen soll.

Optionen	Beschreibung
ActiveAction verwenden	In ActiveAction sind mehrere vorkonfigurierte Aktionen für die Suche nach unterschiedlichen Arten von Sicherheitsrisiken zusammengefasst. Trend Micro empfiehlt die Verwendung von ActiveAction, wenn Sie nicht genau wissen, welche Suchaktion sich für einen bestimmten Typ von Sicherheitsrisiko am besten eignet. Die ActiveAction-Einstellungen werden in den Pattern-Dateien ständig aktualisiert, um Endpunkte gegen die neuesten Sicherheitsrisiken und Angriffsmethoden zu schützen.
Die gleiche Aktion für alle Typen von Sicherheitsrisiken verwenden	Wählen Sie diese Option, wenn dieselbe Aktion für alle Typen von Sicherheitsrisiken außer für wahrscheinliche Viren/Malware durchgeführt werden soll. Beim Typ „Wahrscheinlich Virus/Malware“ erfolgt stets die Aktion „Übergehen“. Wenn Sie „Säubern“ als erste Aktion auswählen, geben Sie eine Ersatzaktion an, die Apex One (Mac) durchführt, falls das Säubern fehlschlägt. Nur wenn die erste Aktion „Säubern“ ist, ist eine zweite Aktion einstellbar. Details zu den Suchoptionen finden Sie unter *Suchaktionen auf Seite 21-12*.

Unterstützte komprimierte Dateitypen

Apex One (Mac) unterstützt die folgenden Komprimierungstypen.

Erweiterung	Typ
.zip	Mit Pkzip erstelltes Archiv
.rar	Mit RAR erstelltes Archiv
.tar	Mit Tar erstelltes Archiv
.arj	ARJ-komprimiertes Archiv
.hqx	BINHEX
.gz; .gzip	Gnu ZIP
.Z	LZW/16-Bit-komprimiert
.bin	MacBinary
.cab	Microsoft Kabinettdatei
Microsoft-komprimiert/MSCOMP	
.eml; .mht	MIME
.td0	Teledisk Format
.bz2	Mit Unix BZ2 Bzip komprimierte Datei
.uu	UUEncode
.ace	WinAce

Suchaktionen

Geben Sie die Aktionen an, die Apex One (Mac) durchführt, wenn ein bestimmter Suchtyp ein Sicherheitsrisiko erkennt.

Die Aktion, die von Apex One (Mac) ausgeführt wird, ist abhängig vom Suchtyp, der das Sicherheitsrisiko erkannt hat. Wenn beispielsweise bei der manuellen Suche (Suchtyp) ein Sicherheitsrisiko von Apex One (Mac) erkannt wird, wird die infizierte Datei gesäubert (Aktion).

Apex One (Mac) kann die folgenden Aktionen bei Sicherheitsrisiken durchführen:

Suchaktion	Details
Löschen	Apex One (Mac) entfernt die infizierte Datei vom Endpunkt.
Quarantäne	Die infizierte Datei wird von Apex One (Mac) umbenannt und in das Quarantäneverzeichnis des Endpunkts `<Agent installation folder>/common/lib/vsapi/quarantine` verschoben. Nachdem die Datei in das Quarantäneverzeichnis verschoben wurde, kann Apex One (Mac) weitere Aktionen für diese Datei durchführen, je nachdem, welche Aktion vom Benutzer angegeben wurde. Apex One (Mac) kann die Datei säubern, löschen oder wiederherstellen. Die Datei wiederherzustellen bedeutet, dass sie an ihren ursprünglichen Speicherort zurückverschoben wird, ohne dass irgendeine Aktion ausgeführt wird. Benutzer können eine Datei wiederherstellen, wenn sie sich als unbedenklich herausstellt. Eine Datei zu säubern bedeutet, dass das Sicherheitsrisiko von der Datei in der Quarantäne entfernt wird und sie nach erfolgreicher Säuberung an ihren ursprünglichen Speicherort zurückverschoben wird.
Säubern	Apex One (Mac) entfernt das Sicherheitsrisiko aus einer infizierten Datei und ermöglicht dann erst den Zugriff darauf. Lässt sich die Datei nicht säubern, führt Apex One (Mac) zusätzlich eine der folgenden Aktionen aus: Quarantäne, Löschen oder Übergehen. Zum Konfigurieren der zweiten Aktion navigieren Sie zu **Agent-Verwaltung** > **Einstellungen** > **{Suchtyp}**, und klicken Sie auf die Registerkarte **Aktion**.

Suchaktion	Details
Übergehen	Apex One (Mac) führt keine Aktion für die infizierte Datei aus. Das erkannte Sicherheitsrisiko wird jedoch in den Protokolldateien verzeichnet. Die Datei wird nicht verschoben. Apex One (Mac) führt bei Dateien mit Infektionen des Typs „Wahrscheinlich Virus/Malware“ stets die Aktion „Übergehen“ aus, um das Risiko von Fehlalarmen zu verringern. Wenn weitere Analysen bestätigen, dass Viren/Malware wahrscheinlich tatsächlich ein Sicherheitsrisiko darstellen, wird ein neues Pattern veröffentlicht, damit Apex One (Mac) die entsprechende Suchaktion durchführen kann. Wenn sich wahrscheinliche Viren/Malware als unbedenklich herausstellen, werden diese nicht mehr entdeckt. Beispiel: Apex One (Mac) entdeckt „x_wahrscheinlicher_Virus“ in einer Datei „123.pdf“ und führt bei Fund keine Aktion durch. Trend Micro bestätigt anschließend, dass „x_wahrscheinlicher_Virus“ ein Trojaner ist und veröffentlicht eine neue Version des Viren-Patterns. Nach dem Laden der neuen Pattern-Version erkennt Apex One (Mac) „x_wahrscheinlicher_Virus“ als Trojaner und löscht „123.pdf“, wenn für diese Dateien die Aktion „Löschen“ festgelegt wurde. **Hinweis** Diese Aktion ist für die Echtzeitsuche nicht verfügbar.
Zugriff verweigern	Beim Versuch, eine Infizierte Datei zu öffnen oder auszuführen, wird dieser Vorgang durch Apex One (Mac) sofort gesperrt. Die infizierte Datei kann manuell gelöscht werden.

Zeitgesteuerte Suche

Die zeitgesteuerte Suche wird automatisch zur angegebenen Uhrzeit am angegebenen Datum ausgeführt. Verwenden Sie die zeitgesteuerte Suche, um die routinemäßige Suche auf dem Security Agent zu automatisieren und die Verwaltung der Virensuche zu optimieren.

Konfigurieren und Anwenden der Einstellungen für die Zeitgesteuerte Suche für einen oder mehrere Security Agents und Gruppen bzw. für alle Security Agents, die vom Server verwaltet werden.

Einstellungen für zeitgesteuerte Suche konfigurieren

Prozedur

1. Aktivieren Sie das Kontrollkästchen, um die zeitgesteuerte Suche zu aktivieren.
2. Klicken Sie auf der Registerkarte **Ziel** die Einstellungen für die allgemeine Suche und die CPU-Nutzung sowie die Einstellungen für die zeitgesteuerte Suche.

   Weitere Informationen finden Sie unter *Zeitgesteuerte Suche: Registerkarte "Ziel" auf Seite 21-21*.
3. Klicken Sie auf die Registerkarte **Aktion**, um die Suchaktionen zu konfigurieren, die Apex One (Mac) bei entdeckten Sicherheitsbedrohungen durchführen soll.

   Weitere Informationen finden Sie unter *Zeitgesteuerte Suche: Registerkarte "Aktion" auf Seite 21-23*.

Zeitgesteuerte Suche: Registerkarte "Ziel"

Prozedur

1. Unter **Zeitplan** stellen Sie ein, wie oft (täglich, wöchentlich oder monatlich) und wann die zeitgesteuerte Suche durchgeführt werden soll.

   Für die monatliche zeitgesteuerte Suche, wenn Sie den 29., 30. oder 31. Tag ausgewählt haben und ein Monat diesen Tag nicht hat, führt Apex One (Mac) die zeitgesteuerte Suche am letzten Tag des Monats durch.
2. Wählen Sie im Abschnitt **Zu durchsuchende Dateien** eine der folgenden Optionen aus:

   - **Alle durchsuchbaren Dateien**: alle durchsuchbaren Dateien werden berücksichtigt. Zu den nicht durchsuchbaren Dateien gehören kennwortgeschützte und verschlüsselte Dateien sowie Dateien, die die vom Benutzer festgelegten Suchkriterien nicht erfüllen.

Hinweis

Das Durchsuchen jeder Datei erfordert viel Zeit und viele Ressourcen und ist möglicherweise in manchen Fällen gar nicht notwendig. Deshalb können Sie bei Bedarf die Anzahl der Dateien begrenzen, die der Security Agent durchsucht.

- **Dateitypen gescannt von IntelliScan**: Durchsucht nur Dateien, die potenziell bösartigen Code enthalten, selbst wenn dieser sich hinter einer scheinbar harmlosen Erweiterung verbirgt.
- **Geben Sie den Pfad oder den vollständigen Pfad an**: Geben Sie manuell die Dateien oder Verzeichnisse an, die durchsucht werden sollen. Zum Beispiel `/Shared/Files/mytext.txt` oder `/Shared/Files`.

3. Wählen Sie unter **Sucheinstellungen** eine oder mehrere der folgenden Optionen aus:
   - **Komprimierte Dateien durchsuchen**: Einzelne Dateien innerhalb einer Archivdatei durchsuchen

     Weitere Informationen finden Sie unter *Unterstützte komprimierte Dateitypen auf Seite 21-11*.
   - **Zeitmaschine durchsuchen**: Nur Dateien auf Time Machine-Laufwerken durchsuchen

     Hinweis

     Nach dem Aktivieren der Option **Zeitmaschine durchsuchen** für die manuelle und zeitgesteuerte Suche kann Apex One (Mac) Malware-Bedrohungen nur erkennen. Aufgrund von Berechtigungseinschränkungen im Mac-Betriebssystem können keine entsprechenden Aktionen (Bereinigen, Quarantäne oder Löschen) ergriffen werden. Konfigurierte Suchaktionen werden in den Produktprotokollen als nicht erfolgreich angezeigt.
4. Konfigurieren Sie im Abschnitt **CPU-Auslastung** die erforderlichen Einstellungen.

- **Hoch**: Ohne Pause zwischen den Suchläufen
- **Niedrig**: Pause zwischen den Suchläufen, wenn die CPU-Auslastung über 20 % liegt, sonst keine Pause

Zeitgesteuerte Suche: Registerkarte "Aktion"

Auf der Registerkarte **Aktionen** konfigurieren Sie die Suchaktionen, die Apex One (Mac) bei entdeckten Sicherheitsbedrohungen durchführen soll.

Prozedur

1. Geben Sie unter **Aktion** die Suchaktionen an.

Optionen	Beschreibung
ActiveAction verwenden	In ActiveAction sind mehrere vorkonfigurierte Aktionen für die Suche nach unterschiedlichen Arten von Sicherheitsrisiken zusammengefasst. Trend Micro empfiehlt die Verwendung von ActiveAction, wenn Sie nicht genau wissen, welche Suchaktion sich für einen bestimmten Typ von Sicherheitsrisiko am besten eignet. Die ActiveAction-Einstellungen werden in den Pattern-Dateien ständig aktualisiert, um Endpunkte gegen die neuesten Sicherheitsrisiken und Angriffsmethoden zu schützen.
Die gleiche Aktion für alle Typen von Sicherheitsrisiken verwenden	Wählen Sie diese Option, wenn dieselbe Aktion für alle Typen von Sicherheitsrisiken außer für wahrscheinliche Viren/Malware durchgeführt werden soll. Beim Typ „Wahrscheinlich Virus/Malware“ erfolgt stets die Aktion „Übergehen“. Wenn Sie „Säubern“ als erste Aktion auswählen, geben Sie eine Ersatzaktion an, die Apex One (Mac) durchführt, falls das Säubern fehlschlägt. Nur wenn die erste Aktion „Säubern“ ist, ist eine zweite Aktion einstellbar. Details zu den Suchoptionen finden Sie unter *Suchaktionen auf Seite 21-12*.

2. Unter **Zeitgesteuerte Suche – Berechtigungen** angeben, ob Benutzer eine zeitgesteuerte Suche verschieben oder überspringen können.

Berechtigung	Beschreibung
Zeitgesteuerte Suche verschieben	Benutzer mit der Berechtigung "Zeitgesteuerte Suche verschieben" können die folgenden Aktionen durchführen: • Zeitgesteuerte Suche verschieben, bevor diese durchgeführt wird, und anschließend die Dauer der Verschiebung festlegen. Die zeitgesteuerte Suche kann nur einmal verschoben werden. • Wenn die zeitgesteuerte Suche gerade durchgeführt wird, können Benutzer die Suche beenden und später neu starten. Der Benutzer legt anschließend fest, nach wie viel Minuten die Suche erneut durchgeführt werden soll. Wenn die Suche erneut durchgeführt wird, werden alle bereits durchsuchten Dateien nochmal durchsucht. Die zeitgesteuerte Suche kann nur einmal beendet und neu gestartet werden. Der Benutzer kann die Anzahl der Stunden und Minuten für folgende Einstellungen angeben: • die maximale Dauer der Verschiebung • die maximalen Zeit, die bis zum Neustart der Suche verstreichen soll
Zeitgesteuerte Suche überspringen und beenden	Mit dieser Berechtigung darf ein Benutzer folgende Aktionen durchführen: • Zeitgesteuerte Suche überspringen, bevor diese durchgeführt wird • Zeitgesteuerte Suche beenden, wenn diese gerade durchgeführt wird

3. Unter **Einstellungen für die zeitgesteuerte Suche** die Benachrichtigungs- und Akkuleistungseinstellungen festlegen.

Einstellung	Beschreibung
Vor Beginn der zeitgesteuerten Suche Benachrichtigung anzeigen	Wenn Sie diese Option aktivieren, wird einige Minuten vor Beginn der zeitgesteuerten Suche eine Benachrichtigung auf dem betreffenden Endpunkt angezeigt. Darin erhalten die Benutzer Auskunft über den Zeitplan (Datum und Uhrzeit) und ihre Berechtigungen im Zusammenhang mit der zeitgesteuerten Suche, etwa ob sie das Recht haben, sie zu verschieben, zu überspringen oder anzuhalten. Sie können die Dauer der Anzeige der Benachrichtigung in Minuten festlegen.
Zeitgesteuerte Suche automatisch anhalten, wenn Suche länger als __ Stunden und __ Minuten dauert	Der Security Agent beendet die Suche automatisch, wenn die festgelegte Zeit überschritten wurde und die Suche noch nicht abgeschlossen ist. Bei der Suche benachrichtigt der Security Agent die Benutzer sofort über die entdeckten Sicherheitsrisiken.
Zeitgesteuerte Suche überspringen, wenn die Akkulaufzeit eines Wireless-Endpunkts weniger als __ % beträgt und der AC-Adapter nicht angeschlossen ist	Apex One (Mac) überspringt eine zeitgesteuerte Suche, wenn festgestellt wird, dass die Akkulebensdauer eines drahtlosen Endpunkts niedrig und das Netzteil nicht angeschlossen ist. Wenn die Akkulebensdauer niedrig ist, aber das Netzteil angeschlossen ist, wird die Suche fortgesetzt. Wenn eine Suche ausgeführt wird und die Akkulebensdauer niedrig ist, wird die Suche nicht beendet.

Unterstützte komprimierte Dateitypen

Apex One (Mac) unterstützt die folgenden Komprimierungstypen.

Erweiterung	Typ
.zip	Mit Pkzip erstelltes Archiv
.rar	Mit RAR erstelltes Archiv
.tar	Mit Tar erstelltes Archiv
.arj	ARJ-komprimiertes Archiv
.hqx	BINHEX
.gz; .gzip	Gnu ZIP

Erweiterung	Typ
.Z	LZW/16-Bit-komprimiert
.bin	MacBinary
.cab	Microsoft Kabinettdatei
Microsoft-komprimiert/MSCOMP	
.eml; .mht	MIME
.td0	Teledisk Format
.bz2	Mit Unix BZ2 Bzip komprimierte Datei
.uu	UUEncode
.ace	WinAce

Suchaktionen

Geben Sie die Aktionen an, die Apex One (Mac) durchführt, wenn ein bestimmter Suchtyp ein Sicherheitsrisiko erkennt.

Die Aktion, die von Apex One (Mac) ausgeführt wird, ist abhängig vom Suchtyp, der das Sicherheitsrisiko erkannt hat. Wenn beispielsweise bei der manuellen Suche (Suchtyp) ein Sicherheitsrisiko von Apex One (Mac) erkannt wird, wird die infizierte Datei gesäubert (Aktion).

Apex One (Mac) kann die folgenden Aktionen bei Sicherheitsrisiken durchführen:

Suchaktion	Details
Löschen	Apex One (Mac) entfernt die infizierte Datei vom Endpunkt.

Suchaktion	Details
Quarantäne	Die infizierte Datei wird von Apex One (Mac) umbenannt und in das Quarantäneverzeichnis des Endpunkts `<Agent installation folder>/common/lib/vsapi/quarantine` verschoben. Nachdem die Datei in das Quarantäneverzeichnis verschoben wurde, kann Apex One (Mac) weitere Aktionen für diese Datei durchführen, je nachdem, welche Aktion vom Benutzer angegeben wurde. Apex One (Mac) kann die Datei säubern, löschen oder wiederherstellen. Die Datei wiederherzustellen bedeutet, dass sie an ihren ursprünglichen Speicherort zurückverschoben wird, ohne dass irgendeine Aktion ausgeführt wird. Benutzer können eine Datei wiederherstellen, wenn sie sich als unbedenklich herausstellt. Eine Datei zu säubern bedeutet, dass das Sicherheitsrisiko von der Datei in der Quarantäne entfernt wird und sie nach erfolgreicher Säuberung an ihren ursprünglichen Speicherort zurückverschoben wird.
Säubern	Apex One (Mac) entfernt das Sicherheitsrisiko aus einer infizierten Datei und ermöglicht dann erst den Zugriff darauf. Lässt sich die Datei nicht säubern, führt Apex One (Mac) zusätzlich eine der folgenden Aktionen aus: Quarantäne, Löschen oder Übergehen. Zum Konfigurieren der zweiten Aktion navigieren Sie zu **Agent-Verwaltung** > **Einstellungen** > **{Suchtyp}**, und klicken Sie auf die Registerkarte **Aktion**.

Suchaktion	Details
Übergehen	Apex One (Mac) führt keine Aktion für die infizierte Datei aus. Das erkannte Sicherheitsrisiko wird jedoch in den Protokolldateien verzeichnet. Die Datei wird nicht verschoben. Apex One (Mac) führt bei Dateien mit Infektionen des Typs „Wahrscheinlich Virus/Malware“ stets die Aktion „Übergehen“ aus, um das Risiko von Fehlalarmen zu verringern. Wenn weitere Analysen bestätigen, dass Viren/Malware wahrscheinlich tatsächlich ein Sicherheitsrisiko darstellen, wird ein neues Pattern veröffentlicht, damit Apex One (Mac) die entsprechende Suchaktion durchführen kann. Wenn sich wahrscheinliche Viren/Malware als unbedenklich herausstellen, werden diese nicht mehr entdeckt. Beispiel: Apex One (Mac) entdeckt „x_wahrscheinlicher_Virus“ in einer Datei „123.pdf“ und führt bei Fund keine Aktion durch. Trend Micro bestätigt anschließend, dass „x_wahrscheinlicher_Virus“ ein Trojaner ist und veröffentlicht eine neue Version des Viren-Patterns. Nach dem Laden der neuen Pattern-Version erkennt Apex One (Mac) „x_wahrscheinlicher_Virus“ als Trojaner und löscht „123.pdf“, wenn für diese Dateien die Aktion „Löschen“ festgelegt wurde. **Hinweis** Diese Aktion ist für die Echtzeitsuche nicht verfügbar.
Zugriff verweigern	Beim Versuch, eine Infizierte Datei zu öffnen oder auszuführen, wird dieser Vorgang durch Apex One (Mac) sofort gesperrt. Die infizierte Datei kann manuell gelöscht werden.

Advanced Threat Protection

In diesem Abschnitt wird beschrieben, wie die erweiterten Bedrohungsschutz-Einstellungen auf macOS Security Agents konfiguriert werden.

Einstellungen für Vorausschauendes Maschinenlernen

Das Trend Micro Vorausschauendes Maschinenlernen setzt moderne Technologien ein, um Bedrohungsinformationen zu korrelieren und ausführliche Dateianalysen durchzuführen und so unbekannte neue

Sicherheitsrisiken durch digitale DNS-Fingerabdrücke, API-Zuordnung und weitere Funktionen zu erkennen. Beim 'Vorausschauendes Maschinenlernen' wird außerdem eine Verhaltensanalyse für unbekannte Prozesse oder Prozesse mit geringer Prävalenz durchgeführt, um zu ermitteln, ob eine neue oder unbekannte Bedrohung versucht, das Netzwerk zu infizieren.

Beim 'Vorausschauendes Maschinenlernen' handelt es sich um ein leistungsstarkes Tool, mit dem Ihre Umgebung vor unbekannten und Zero-Day-Angriffen geschützt wird.

Um diese Funktion zu aktivieren, wählen Sie **Vorausschauendes Maschinenlernen aktivieren**.

Web Reputation

Die Web-Reputation-Technologie bewertet die Glaubwürdigkeit von Webdomänen nach einem Scoring-Verfahren, indem Informationen wie das Alter einer Website, historische Änderungen des Speicherorts und Anzeichen von verdächtigen Aktivitäten zurückverfolgt werden, die durch die Malware-Verhaltensanalyse entdeckt wurden. Anschließend werden Websites durchsucht und Benutzer vom Zugriff auf infizierte Websites abgehalten.

Security Agents senden Anfragen an die Smart Protection Quellen, um die Reputation von Websites, auf die ein Benutzer zugreifen möchte, zu überprüfen. Die Reputation einer Website wird mit einer spezifischen, auf dem jeweiligen Endpunkt gültigen Web-Reputation-Richtlinie abgeglichen. Die jeweils angewendete Richtlinie bestimmt, ob Security Agents den Zugriff auf eine Website zulässt oder sperrt.

Hinweis

Diese Funktion unterstützt die neuesten Versionen von Safari™, Mozilla™, Firefox™ und Google Chrome™-Browsern.

Web-Reputation-Einstellungen konfigurieren

Die Web Reputation-Einstellungen umfassen Richtlinien, die festlegen, ob Apex One (Mac) den Zugriff auf eine Website sperren oder erlauben wird.

Um die geeignete Richtlinie zu bestimmen, überprüft Apex One (Mac) den Standort des Security Agent. Der Standort eines Security Agent ist "intern", wenn der Security Agent eine Verbindung zum Apex One (Mac) Server herstellen kann. Andernfalls ist der Standort für den Security Agent "extern".

Prozedur

1. So konfigurieren Sie eine Richtlinie für externe Security Agents:
   a. Klicken Sie auf die Registerkarte **Externe Agenten**.
   b. Wählen Sie **Aktivieren Sie "Web Reputation-Richtlinie"**.

      Wenn die Richtlinie aktiviert ist, senden externe Security Agents Web-Reputation-Abfragen an das Smart Protection Network.

      Hinweis

      Wenn ein Agent ausschließlich eine IPv6-Adresse aufweist, lesen Sie den Abschnitt über die Einschränkungen bei IPv6 für Web Reputation-Abfragen in *Einschränkungen bei reinen IPv6-Agents auf Seite 21-45*.

   c. Wählen Sie unter den vorhandenen Web Reputation-Sicherheitsstufen aus: **Hoch**, **Mittel** oder **Niedrig**

      Hinweis

      Die Sicherheitsstufen legen fest, ob Apex One (Mac) den Zugriff auf eine URL zulässt oder sperrt. Wenn zum Beispiel die Sicherheitsstufe auf "Niedrig" festgelegt ist, sperrt Apex One (Mac) nur URLs, die als Internet-Bedrohungen bekannt sind. Bei einer Erhöhung der Sicherheitsstufe verbessert sich die Erkennungsrate von Internet-Bedrohungen, doch gleichzeitig steigt auch die Wahrscheinlichkeit von Fehlalarmen.

   d. Um Web Reputation-Feedback anzugeben, klicken Sie auf die entsprechende URL. In einem Browserfenster wird das Web Reputation-Hilfesystem von Trend Micro geöffnet.

2. Um eine Richtlinie für interne Security Agents zu konfigurieren:

   a. Klicken Sie auf die Registerkarte **Interne Agents**.

   b. Wählen Sie **Aktivieren Sie "Web Reputation-Richtlinie"**.

      Wenn die Richtlinie aktiviert ist, senden interne Security Agents Web Reputation-Abfragen an:

      - Smart Protection Server, wenn die Option **Anfragen an Smart Protection Server senden** aktiviert ist.
      - Smart Protection Network, wenn die Option **Anfragen an Smart Protection Server senden** deaktiviert ist.

      Hinweis

      Wenn ein Agent ausschließlich eine IPv6-Adresse aufweist, lesen Sie den Abschnitt über die Einschränkungen bei IPv6 für Web Reputation-Abfragen in *Einschränkungen bei reinen IPv6-Agents auf Seite 21-45*.

   c. Wählen Sie **Anfragen an Smart Protection Server senden**, wenn Sie möchten, dass interne Security Agents Web Reputation-Abfragen an Smart Protection Server senden.

      - Wenn Sie diese Option aktivieren, verweist Security Agents auf dieselbe Smart Protection-Quellenliste, die von Apex One Security Agents verwendet wird, um die Smart Protection Server zu bestimmen, an die Anfragen gesendet werden.
      - Wenn Sie diese Option deaktivieren, senden Security Agents Web Reputation-Abfragen an das Smart Protection Network. Für ein erfolgreiches Senden der Abfragen müssen die Endpunkte mit dem Internet verbunden sein.

   d. Wählen Sie unter den vorhandenen Web Reputation-Sicherheitsstufen aus: **Hoch**, **Mittel** oder **Niedrig**

Hinweis

Die Sicherheitsstufen legen fest, ob Apex One (Mac) den Zugriff auf eine URL zulässt oder sperrt. Wenn zum Beispiel die Sicherheitsstufe auf "Niedrig" festgelegt ist, sperrt Apex One (Mac) nur URLs, die als Internet-Bedrohungen bekannt sind. Bei einer Erhöhung der Sicherheitsstufe verbessert sich die Erkennungsrate von Internet-Bedrohungen, doch gleichzeitig steigt auch die Wahrscheinlichkeit von Fehlalarmen.

Security Agents sperren Sie nicht getestete Websites nicht, unabhängig von der Sicherheitsstufe.

e. Um Web Reputation-Feedback anzugeben, klicken Sie auf die entsprechende URL. In einem Browserfenster wird das Web Reputation-Hilfesystem von Trend Micro geöffnet.

f. Wählen Sie, ob der Security Agents Web Reputation-Protokolle an den Server senden darf. Gestatten Sie Security Agents das Senden von Protokollen, wenn Sie die von Apex One (Mac) gesperrten URLs analysieren und bei als sicher eingestuften URLs eine entsprechende Aktion durchführen möchten.

Listen genehmigter und gesperrter URLs konfigurieren

Fügen Sie Websites, die Sie als sicher bzw. gefährlich einstufen, zur Liste der zulässigen bzw. gesperrten URLs hinzu. Erkennt Apex One (Mac) einen Zugriff auf eine dieser Websites, wird der Zugriff automatisch zugelassen bzw. gesperrt und es werden keine weiteren Abfragen an die Smart Protection-Quellen gesendet.

Prozedur

1. Öffnen Sie die Webkonsole von Apex One (Mac).
2. Navigieren Sie zu **Agents** > **Globale Agent-Einstellungen** > **Liste der zulässigen/gesperrten Web Reputation-URLs**.

3. Geben Sie eine URL in das Textfeld ein. Sie können an einer beliebigen Stelle der URL ein Platzhalterzeichen (*) einfügen.

   Beispiele:

   - `www.trendmicro.com/*` steht für alle Seiten der Domäne www.trendmicro.com.
   - `*.trendmicro.com/*` steht für alle Seiten auf allen Unterdomänen von trendmicro.com.

   Sie können auch URLs eingeben, die IP-Adressen enthalten. Bei URLs mit IPv6-Adressen müssen Sie diese zwischen eckige Klammern setzen.

4. Klicken Sie auf **Zur Liste der zulässigen URLs hinzufügen** oder **Zur Liste der gesperrten URLs hinzufügen**.
5. Um einen Einträge zu löschen, wählen Sie eine Option aus dem Listenfeld **Ansicht**, und klicken Sie auf das Symbol neben dem URL.
6. Klicken Sie auf **Deploy**.

Gerätesteuerung

Die Gerätesteuerung reguliert den Zugriff auf externe Speichergeräte und Netzwerkressourcen, die mit Endpunkten verbunden sind. Die Gerätesteuerung trägt dazu bei, Datenverluste und Datenlecks zu verhindern und bietet, gemeinsam mit der Dateiprüfung, Schutz vor Sicherheitsrisiken.

Sie können Gerätesteuerungsrichtlinien für interne und externe Agents konfigurieren. In der Regel konfigurieren Administratoren eine strengere Richtlinie für externe Agents.

Richtlinien sind granulare Einstellungen im Agentenbaum. Sie können spezifische Richtlinien für Agentengruppen oder einzelne Security Agents durchsetzen. Sie können auch eine einzelne Richtlinie für alle Security Agents durchsetzen.

Einstellungen der Gerätesteuerung konfigurieren

Prozedur

1. Klicken Sie auf die Registerkarte **Externe Agents**, um Einstellungen für externe Agents zu konfigurieren, oder auf die Registerkarte **Interne Agents**, um Einstellungen für interne Agents zu konfigurieren.
2. Wählen Sie **Gerätesteuerung aktivieren**.
3. Unter **Geräte** wählen Sie eine Berechtigung für jedes Speichermedium aus.

   Weitere Informationen zu Berechtigungen finden Sie unter *Berechtigungen für Speichergeräte auf Seite 21-35*.
4. (Optional) Wenn die Berechtigung für USB-Speichergeräte **Sperren** lautet, können Sie unter **USB-Speichergerät Zulässige Liste** eine Liste zulässiger Geräte konfigurieren. Benutzer können auf diese Geräte zugreifen, und Sie können die Zugriffsstufe durch Berechtigungen steuern.
   a. Geben Sie den Gerätehersteller ein.
   b. Geben Sie das Gerätemodell und die Seriennummer ein.
   c. Wählen Sie die Berechtigung für dieses Gerät.

      Weitere Informationen zu Berechtigungen finden Sie unter *Berechtigungen für Speichergeräte auf Seite 21-35*.

      Hinweis

      USB-Speichergeräte auf der zulässigen Liste müssen eine höhere Berechtigungsstufe haben als die Berechtigungseinstellung für USB-Speichergeräte im **Geräte**-Abschnitt.
5. Unter **Benachrichtigung** wählen Sie die Option **Eine Benachrichtigung auf dem Agent anzeigen, wenn ein neues Gerät erkannt wird**, um eine Benachrichtigung anzuzeigen, wenn ein neues Speichermedium mit dem Endpunkt verbunden wird. Die Benachrichtigung zeigt die Zugriffsberechtigung für das neue Speichermedium an.

6. Klicken Sie auf **Deploy**.

Berechtigungen für Speichergeräte

Gerätesteuerung-Berechtigungen für Speichergeräte werden verwendet, wenn Sie:

- Erlauben Sie den Zugriff auf USB-Speichergeräte, CD/DVD, SD-Karten, Netzwerklaufwerke und Thunderbolt SATA-Speichergeräte. Sie können den Zugriff auf diese Geräte entweder uneingeschränkt zulassen oder die Zugriffsstufe einschränken.
- Konfigurieren Sie die Liste der zulässigen USB-Speichergeräte. Mit der Gerätesteuerung können Sie den Zugriff auf alle USB-Speichergeräte sperren, mit Ausnahme der Geräte, die Sie in der Liste zulässiger Geräte hinzugefügt haben. Sie können den Zugriff auf die zulässigen Geräte entweder uneingeschränkt zulassen oder die Zugriffsstufe einschränken.

Die folgende Tabelle enthält eine Liste der Berechtigungen für Speichergeräte.

Tabelle 21-4. Gerätesteuerungsberechtigungen für Speichergeräte

Berechtigungen	Dateien auf dem Gerät	Eingehende Dateien
Vollständiger Zugriff	Zulässige Aktionen: Kopieren, Verschieben, öffnen, Speichern, Löschen, Ausführen	Zulässige Aktionen: Speichern, Verschieben, Kopieren Das bedeutet, dass eine Datei kann auf dem Gerät gespeichert, verschoben und kopiert werden kann.
Nur lesen	Zulässige Aktionen: Kopieren, öffnen Unzulässige Aktionen: Speichern, Verschieben, Löschen, Ausführen	Unzulässige Aktionen: Speichern, Verschieben, Kopieren

Berechtigungen	Dateien auf dem Gerät	Eingehende Dateien
Sperren	Unzulässige Aktionen: Alle Aktionen Das Gerät und die darin enthaltenen Dateien sind nicht für den Benutzer sichtbar (zum Beispiel über Finder).	Unzulässige Aktionen: Speichern, Verschieben, Kopieren

Hinweis

Die Nur-Lese-Berechtigung ist für Netzlaufwerke nicht verfügbar.

Erkennung und Reaktion

In diesem Abschnitt wird beschrieben, wie Erkennungs- und Reaktionseinstellungen auf macOS Security Agents konfiguriert werden.

Endpoint Sensor

Endpoint Sensor ist ein leistungsstarkes Überwachungs- und Untersuchungswerkzeug, mit dem das Vorhandensein, der Standort und der Eintrittspunkt von Bedrohungen identifiziert werden können. Mittels detaillierter Systemereignisaufzeichnung und Verlaufsanalyse können Sie historische Untersuchungen durchführen, um in Ihrem Netzwerk verborgene Bedrohungen und alle betroffenen Endpoints zu ermitteln. Erstellen Sie Berichte zur Fehlerursachenanalyse, um die Art und Aktivität der Malware seit Auftreten der Bedrohung am Endpoint zu verstehen.

Konfigurieren von Einstellungen für Endpoint Sensor

Wichtig

Die Endpoint Sensor-Funktion erfordert eine spezielle Lizenzierung und zusätzliche Systemvoraussetzungen. Stellen Sie sicher, dass Sie die richtige Lizenz haben, bevor Sie Endpoint Sensor-Richtlinien auf Endpunkten bereitstellen. Für weitere Informationen zum Erwerb von Lizenzen wenden Sie sich an Ihren Support-Anbieter.

Prozedur

1. Wählen Sie **Endpoint Sensor aktivieren**.

Ausnahmen

In diesem Abschnitt wird beschrieben, wie Ausnahmeeinstellungen auf macOS Security Agents konfiguriert werden.

Suchausschlüsse

Konfigurieren Sie die Suchausschlüsse, um die Suchleistung zu verbessern und bekannte Dateien zu überspringen, die keinen Schaden anrichten können. Während ein bestimmter Suchtyp ausgeführt wird, überprüft Apex One (Mac) die Ausschlussliste, um die Dateien auf dem Endpunkt zu bestimmen, die von der Suche ausgeschlossen werden.

Ausschlussliste	Details
Dateien	Apex One (Mac) durchsucht in folgenden Fällen keine Datei: • die Datei sich im Verzeichnispfad befindet, der in der Ausschlussliste angegeben ist • die Datei dem vollständigen Dateipfad (Verzeichnispfad und Dateiname) entspricht, der in der Ausschlussliste angegeben ist
Dateierweiterungen	Apex One (Mac) durchsucht eine Datei nicht, wenn ihre Erweiterung einer der Erweiterungen in der Ausschlussliste entspricht.

Suchausschlusslisten konfigurieren

Weitere Informationen zu Suchausschlusslisten finden Sie unter *Suchausschlüsse auf Seite 21-37*.

Prozedur

1. Aktivieren Sie das Kontrollkästchen, um den Suchausschluss zu aktivieren.
2. Um die **Ausschlussliste für Virensuche (Dateien)** zu konfigurieren:

a. Geben Sie einen vollständigen Dateipfad oder einen Verzeichnispfad ein und klicken Sie auf **Hinzufügen**.

Erinnerung:

- Die Eingabe nur eines Dateinamens ist nicht zulässig.
- Es können maximal 64 Pfade angegeben werden. Beispiele erhalten Sie in der folgenden Tabelle.

Pfad	Details	Beispiele
Vollständiger Dateipfad	Schließt eine bestimmte Datei auf dem Endpunkt aus.	• Beispiel 1: `/file.log` • Beispiel 2: `/System/file.log`

Pfad	Details	Beispiele

Verzeichnispfad	Schließt alle Dateien in einem bestimmten Ordner und dessen Unterordnern aus.	• Beispiel 1:
		`/System/`
		Beispiele für aus Suchvorgängen ausgeschlossene Dateien:
		• `/System/file.log`
		• `/System/Library/file.log`
		Beispiele für Dateien, die durchsucht werden:
		• `/Applications/file.log`
		• Beispiel 2:
		`/System/Library`
		Beispiele für aus Suchvorgängen ausgeschlossene Dateien:
		• `/System/Library/file.log`
		• `/System/Library/Filters/file.log`
		Beispiele für Dateien, die durchsucht werden:
		• `/System/file.log`

- Sie können statt Ordnernamen auch ein Sternchen (*) als Platzhalterzeichen verwenden.

  Beispiele erhalten Sie in der folgenden Tabelle.

Pfad	Beispiele für die Verwendung von Platzhalterzeichen
Vollständiger Dateipfad	`/Users/Mac/*/file.log` Beispiele für aus Suchvorgängen ausgeschlossene Dateien: • `/Users/Mac/Desktop/file.log` • `/Users/Mac/Movies/file.log` Beispiele für Dateien, die durchsucht werden: • `/Users/file.log` • `/Users/Mac/file.log`

Verzeichnispfad	• Beispiel 1:
	`/Users/Mac/*`
	Beispiele für aus Suchvorgängen ausgeschlossene Dateien:
	• `/Users/Mac/doc.html`
	• `/Users/Mac/Documents/doc.html`
	• `/Users/Mac/Documents/Pics/pic.jpg`
	Beispiele für Dateien, die durchsucht werden:
	• `/Users/doc.html`
	• Beispiel 2:
	`/*/Components`
	Beispiele für aus Suchvorgängen ausgeschlossene Dateien:
	• `/Users/Components/file.log`
	• `/System/Components/file.log`
	Beispiele für Dateien, die durchsucht werden:
	• `/file.log`
	• `/Users/file.log`
	• `/System/Files/file.log`

- Teilweise Übereinstimmungen mit Ordnernamen sind nicht zulässig. So ist es beispielsweise nicht möglich, durch Eingabe von `/Users/*user/temp` auch Dateien in Ordnern auszuschließen, deren Namen auf „Benutzer“ enden, etwa „Endbenutzer“ oder „neuer_benutzer“.

b. Wählen Sie zum Löschen eines Pfads den Pfad aus, und klicken Sie auf **Entfernen**.

3. Um die **Ausschlussliste für Virensuche (Dateierweiterungen)** zu konfigurieren:

   a. Geben Sie eine Dateierweiterung ohne Punkt (.) ein und klicken Sie auf **Hinzufügen**. Geben Sie z. B. `pdf` ein. Es können maximal 64 Dateierweiterungen angegeben werden.

   b. Um eine Erweiterung zu löschen, wählen Sie sie aus und klicken auf **Entfernen**.

Ausnahmelisten

Sie können den Bildschirm Ausnahmelisten verwenden, um Security Agents so zu konfigurieren, dass die Suche bei vertrauenswürdigen Prozessen übersprungen wird und Erkennungen bestimmter Regeln ausgeschlossen werden.

- **Rule Exceptions**: Geben Sie an, welche Erkennungen mithilfe der Regel-ID ausgeschlossen werden sollen. Sie können Regel-IDs auf dem Bildschirm "Protokollabfrage" finden.
- **Liste der vertrauenswürdigen Programme**: Geben Sie vertrauenswürdige Programme an, die bei der Durchführung von Scans übersprungen werden sollen. Für weitere Informationen siehe *Liste der vertrauenswürdigen Programme konfigurieren auf Seite 21-41*.

Liste der vertrauenswürdigen Programme konfigurieren

Die Liste der vertrauenswürdigen Programme schließt Programme und alle untergeordneten Prozesse aus, die über die Echtzeitsuche vom Programm aufgerufen werden.

Sie können Security Agents so konfigurieren, dass die Suche für vertrauenswürdige Prozesse bei der Echtzeitsuche und der Ereignisaufzeichnung übersprungen wird. Nach dem Hinzufügen eines Programms zur Liste der vertrauenswürdigen Programme führt der Security Agent keine Echtzeitsuche und keine Ereignisaufzeichnung für das Programm oder für vom Programm ausgeführte Prozesse aus. Fügen Sie vertrauenswürdige Programme zur Liste der vertrauenswürdigen Programme hinzu, um die Suchleistung auf Endpunkten zu verbessern.

Hinweis

Sie können Dateien zur Liste der vertrauenswürdigen Programme hinzufügen, wenn die folgenden Anforderungen erfüllt sind:

- Die Datei befindet sich nicht im Systemverzeichnis.
- Die Datei weist eine gültige digitale Signatur auf.

Hinweis

Sie können Dateien zur Liste der vertrauenswürdigen Programme hinzufügen, wenn die folgenden Anforderungen erfüllt sind:

- Die Datei befindet sich nicht im Systemverzeichnis.
- Die Datei weist eine gültige digitale Signatur auf.

- Dateiprüfung mit der Echtzeitsuche
- Durchsuchen von Prozessen mit der Echtzeitsuche
- Ereignisaufzeichnung

Prozedur

1. Geben Sie den vollständigen Programmpfad für das Programm an, das von der Liste ausgeschlossen werden soll.
2. Klicken Sie auf **+ Hinzufügen**.

3. Um ein Programm aus der Liste zu entfernen, klicken Sie auf das Symbol **Delete**.

Agent-Konfigurationen

In diesem Abschnitt wird beschrieben, wie die Agenteneinstellungen auf macOS Security Agents konfiguriert werden.

Update-Einstellungen

Um sicherzustellen, dass Security Agents vor den neuesten Sicherheitsrisiken geschützt bleibt, aktualisieren Sie die Update-Agent-Komponenten regelmäßig. Aktualisieren Sie außerdem Security Agents mit stark veralteten Komponenten und bei einem Ausbruch. Komponenten veralten stark, wenn der Security Agent über einen längeren Zeitraum nicht vom Apex One (Mac)-Server oder dem ActiveUpdate-Server aktualisieren kann.

Agent-Update-Methoden

Es gibt mehrere Möglichkeiten, Security Agents zu aktualisieren.

Update-Methode	Beschreibung
Vom Administrator eingeleitetes manuelles Update	Updates können in den folgenden Webkonsolen-Fenstern gestartet werden: • Agent-Verwaltung: • Übersicht:

Update-Methode	Beschreibung
Automatisches Update	• Nachdem der Server ein Update abgeschlossen hat, benachrichtigt er Security Agents sofort, um zu aktualisieren. • Updates können gemäß dem von Ihnen konfigurierten Zeitplan ausgeführt werden. Sie können einen Zeitplan konfigurieren, der für ein oder mehrere Security Agents und Domänen gilt, oder für alle Security Agents, die der Server verwaltet. Weitere Informationen finden Sie unter *Update-Einstellungen für Agent konfigurieren auf Seite 21-46*.
Vom Benutzer eingeleitete manuelle Aktualisierung	Benutzer starten das Update von ihrem Endpunkt aus.

Agent-Update-Adresse

Standardmäßig laden Security Agents Komponenten vom Apex One (Mac) Server herunter. Zusätzlich zu den Komponenten erhalten Security Agents auch aktualisierte Konfigurationsdateien, wenn sie vom Apex One (Mac) Server aktualisieren. Security Agents benötigen diese Konfigurationsdateien, um neue Einstellungen zu übernehmen. Bei jeder Änderung der Apex One (Mac) Einstellungen über die Webkonsole ändern sich auch die Konfigurationsdateien.

Bevor Sie das Security Agents aktualisieren, überprüfen Sie, ob der Apex One (Mac) Server die neuesten Komponenten hat.

Konfigurieren Sie einen, mehrere oder alle Security Agents, um vom Trend Micro ActiveUpdate Server herunterzuladen, falls der Apex One (Mac) Server nicht verfügbar ist.

Weitere Informationen finden Sie unter *Update-Einstellungen für Agent konfigurieren auf Seite 21-46*.

Hinweis

Wenn ein Agent ausschließlich eine IPv6-Adresse aufweist, lesen Sie den Abschnitt über die Einschränkungen bei IPv6 für Agent-Updates in *Einschränkungen bei reinen IPv6-Agents auf Seite 21-45*.

Hinweise und Erinnerungen für Agent-Updates

- Security Agents können Proxy-Einstellungen während eines Updates verwenden. Proxy-Einstellungen werden in der Agentenkonsole konfiguriert.
- Während eines Updates zeigt das Symbol für Security Agent in der Menüleiste des Endpunkts den laufenden Aktualisierungsvorgang an. Ist ein Upgrade für das Security Agent-Programm verfügbar, führen Security Agents zunächst das Update und dann das Upgrade auf die neueste Programmversion oder den neuesten Build durch. Bis zum Abschluss des Updates können keine Tasks über die Konsole gestartet werden.
- Greifen Sie auf den Übersichtsbildschirm zu, um zu überprüfen, ob alle Security Agents aktualisiert wurden.

Einschränkungen bei reinen IPv6-Agents

Die folgende Tabelle enthält eine Liste von Einschränkungen, wenn Security Agents nur über eine IPv6-Adresse verfügen.

TABELLE 21-5. Einschränkungen bei reinen IPv6-Agents

VORGANG	EINSCHRÄNKUNG
Übergeordneter Server	Reine IPv6-Agents können nicht über einen reinen IPv4-Server verwaltet werden.
Updates	Reine IPv6-Agents können nicht aus reinen IPv4-Aktualisierungsquellen wie die folgenden aktualisiert werden: • Trend Micro ActiveUpdate Server • Ein reiner IPv4-Apex One (Mac) Server

Vorgang	Einschränkung
Web Reputation-Abfragen	Reine IPv6-Agents können keine Web Reputation-Abfragen an das Trend Micro Smart Protection Network senden.
Proxy-Verbindung	Reine IPv6-Agents können keine Verbindungen über reine IPv4-Proxyserver herstellen.
Bereitstellung von Agents	Apple Remote Desktop ist nicht in der Lage, reinen IPv6-Endpunkten Agents bereitzustellen, da diese Endpunkte immer als offline angezeigt werden.

Die meisten dieser Einschränkungen können mit Hilfe eines Dualstapel-Proxyservers umgangen werden, der IPv4- in IPv6-Adressen und umgekehrt umwandeln kann (z. B. DeleGate). Setzen Sie den Proxyserver zwischen die Agents und die Entitäten, mit denen sie sich verbinden sollen.

Update-Einstellungen für Agent konfigurieren

Detaillierte Erklärungen zu Agent-Updates erhalten Sie unter *Update-Einstellungen auf Seite 21-43*.

Prozedur

1. Wählen Sie **Agenten laden Updates vom Trend Micro ActiveUpdate Server herunter, wenn sie keine Verbindung zum Apex One (Mac) Server herstellen können**, um Agenten zu erlauben, Updates vom Trend Micro ActiveUpdate Server herunterzuladen.

   Hinweis

   Wenn ein Security Agent ausschließlich eine IPv6-Adresse aufweist, lesen Sie den Abschnitt über die Einschränkungen bei IPv6 für Agent-Updates in *Einschränkungen bei reinen IPv6-Agents auf Seite 21-45*.

2. Wählen Sie **Agenten können die Komponenten aktualisieren, aber nicht das Agentenprogramm upgraden oder Hot Fixes installieren**, um Komponenten-Updates zuzulassen, aber verhindert ein Agenten-Upgrade.

3. Führen Sie die folgenden Schritte aus, um geplante Updates einzurichten:

   a. Wählen Sie **Zeitgesteuertes Update aktivieren**.

   b. Konfigurieren Sie den Zeitplan.

   c. Geben Sie bei Auswahl von **Täglich** oder **Wöchentlich** die Uhrzeit des Updates und den Zeitraum an, in dem der Apex One (Mac) Server Security Agents zum Update der Komponenten auffordert. Wenn Sie die Startzeit beispielsweise für 12 Uhr und den Zeitraum mit 2 Stunden festlegen, fordert der Server zwischen 12 und 14 Uhr in zufälligen Abständen alle online geschalteten Security Agents zum Update auf. Mit dieser Einstellung wird verhindert, dass sich alle Security Agents gleichzeitig zum festgelegten Zeitpunkt mit dem Server verbinden, damit es zu keiner Überlastung des Servers kommt.

Cache-Einstellungen für die Suche

Bei jeder Suche prüft der Agent den Zwischenspeicher für geänderte Dateien, um zu ermitteln, ob eine Datei seit dem letzten Start des Agent geändert wurde.

- Ist dies der Fall, durchsucht der Agent die Datei und fügt sie dem Zwischenspeicher für durchsuchte Dateien hinzu.
- Wurde die Datei nicht geändert, sieht der Agent nach, ob sich die Datei im Zwischenspeicher für durchsuchte Dateien befindet.
  - Wenn sie dort vorhanden ist, wird sie bei der Suche übersprungen.
  - Wenn sie sich nicht im Zwischenspeicher für durchsuchte Dateien befindet, sieht der Agent im Zwischenspeicher für genehmigte Dateien nach.

Hinweis

Der Cache für genehmigte Dateien enthält alle Dateien, die Apex One (Mac) für vertrauenswürdig erachtet. Vertrauenswürdige Dateien wurden von aufeinanderfolgenden Versionen des Pattern durchsucht und jedes Mal als bedrohungsfrei erklärt. Es kann sich auch um bedrohungsfreie Dateien handeln, die während eines längeren Zeitraums nicht geändert wurden.

- Wenn die Datei im Zwischenspeicher für genehmigte Dateien vorhanden ist, wird sie bei der Suche übersprungen.
- Ist dies nicht der Fall, durchsucht der Agent die Datei und fügt Sie dem Zwischenspeicher für durchsuchte Dateien hinzu.

Bei jeder Aktualisierung der Such-Engine bzw. des Such-Pattern werden alle oder zumindest einige der Zwischenspeicher geleert.

Wenn Suchvorgänge häufig ausgeführt werden und sich bereits viele Dateien in den Zwischenspeichern befinden, reduziert sich die Suchzeit erheblich.

Wenn Sie die Suche nur selten ausführen, deaktivieren Sie die Zwischenspeicher, so dass bei jeder Suche alle Dateien auf Bedrohungen durchsucht werden können.

Berechtigungen und andere Einstellungen

Konfigurieren Sie Security Agents, um wichtige Security Agent-Dateien und -Ordner zu schützen.

Abschnitt	Beschreibung
Eigenschutz des Security Agents	Wählen Sie **Dateien schützen, die vom Security Agent verwendet werden**, um zu verhindern, dass andere Programme und sogar der Benutzer Dateien, die von Security Agent verwendet werden, ändern oder löschen. Eine Liste der Dateien und Ordner, die durch diese Funktion geschützt werden, finden Sie unter *Geschützte Security Agent Dateien auf Seite 21-49*.

Geschützte Security Agent Dateien

Wenn Sie die Security Agent-Selbstschutzfunktion aktivieren, sperrt Apex One (Mac) die folgenden Dateien und Ordner, um zu verhindern, dass andere Programme und sogar der Benutzer Security Agent-Dateien ändern oder löschen:

- /Library/Application Support/TrendMicro/common
- /Library/Application Support/TrendMicro/Kext
- /Library/Application Support/TrendMicro/TmccMac
- /Library/Application Support/TrendMicro/TmccUpdate
- /Library/Application Support/TrendMicro/Plug-in
- /Library/Application Support/TrendMicro/Tools
- /Library/LaunchDaemons/com.trendmicro.icore.*
- /Library/LaunchDaemons/com.trendmicro.tmsm.plugin.plist
- /Library/LaunchDaemons/com.trendmicro.tmsm.launcher.plist
- /Application/TrendMicroSecurity.app

Hinweis

Apex One (Mac) lässt zu, dass Dateien dem Ordner `/Library/Application Support/TrendMicro/Tools` hinzugefügt werden. Die darin enthaltenen Dateien können jedoch nicht gelöscht werden.

Teil VIII

Deep Discovery Widgets und Richtlinien

Kapitel 22

Deep Discovery Analyzer- und Email Inspector-Dashboard (Widgets)

Dieser Abschnitt enthält Hilfethemen für die Deep Discovery Analyzer- und Deep Discovery Email Inspector-Dashboard-Widgets, die in Trend Micro Apex Central unterstützt werden.

Es werden folgende Themen behandelt:

Deep Discovery Analyzer (Widgets)

Dieser Abschnitt enthält Hilfethemen für alle in Trend Micro Apex Central unterstützten Deep Discovery Analyzer-Widgets.

Virtual Analyzer – Überblick – Widget

In diesem Widget wird die Gesamtanzahl der an Virtual Analyzer übermittelten Beispiele sowie die Anzahl der Beispiele mit Risiken angezeigt. Im Widget können Daten aus einer oder mehreren Deep Discovery Analyzer-Appliances angezeigt werden. Das Widget zeigt die Daten in einer Tabelle und einem zugehörigen Tortendiagramm an.

Bezeichnung	Beschreibung
Übermittlungen	Die Gesamtanzahl der Übermittlungen an Virtual Analyzer.
Identifizierte Risiken	Die Gesamtanzahl der Übermittlungen mit erkannten Risiken.
Hohes Risiko	Die Gesamtanzahl der Übermittlungen mit hohem Risiko.
Mittleres Risiko	Die Gesamtanzahl der Übermittlungen mit mittlerem Risiko.
Niedriges Risiko	Die Gesamtanzahl der Übermittlungen mit geringem Risiko.
% aller Übermittlungen, die Risiken darstellen	Der Prozentsatz aller Übermittlungen, die Risiken darstellen.
Verteilung bösartiger Ereignisse	Ein Tortendiagramm, in dem der Prozentsatz der erkannten Risiken mit hohem, mittlerem und geringem Risiko angezeigt wird.

Ändern Sie den Zeitraum, indem Sie eine Option in der Dropdown-Liste **Bereich** oben links im Widget auswählen.

Geben Sie an, ob die angezeigten Daten aus allen registrierten Deep Discovery Analyzer-Appliances oder einer bestimmten Appliance stammen sollen, indem Sie die Option in der Dropdown-Liste **Anzeigen** oben links im Widget auswählen.

Zeigen Sie nach Auswahl einer Appliance weitere Informationen an, indem Sie auf die Gesamtzahl der Übermittlungen, die Anzahl der Übermittlungen

mit hohem, mittlerem oder geringem Risiko oder einen Bereich im Tortendiagramm klicken.

Deep Discovery Email Inspector (Widgets)

Dieser Abschnitt enthält Hilfethemen für alle Deep Discovery Email Inspector-Widgets, die in Trend Micro Apex Central unterstützt werden.

E-Mail-Nachrichten mit komplexen Bedrohungen – Widget

Das Widget **E-Mail-Nachrichten mit komplexen Bedrohungen** zeigt alle E-Mail-Nachrichten mit bösartigen und verdächtigen Merkmalen an, die von Deep Discovery Email Inspector erkannt werden. Zu den verdächtigen Merkmalen zählen anormales Verhalten, falsche oder irreführende Daten, verdächtige oder bösartige Verhaltensmuster sowie Zeichenfolgen, die auf gefährdete Systeme hindeuten, aber weitere Untersuchungen erfordern.

Die Grafik basiert auf dem ausgewählten Zeitraum.Die Y-Achse steht für die Anzahl der E-Mail-Nachrichten. Die X-Achse steht für den Zeitraum. Bewegen Sie den Mauszeiger über die Grafik, um die Anzahl der Nachrichten mit hohem Risiko und den Zeitraum anzuzeigen.

Klicken Sie auf ein Element in der Widget-Legende, um Daten mit Bezug auf diese Metrik ein- oder auszublenden.

Klicken Sie auf **Erkannte Nachrichten anzeigen**, um alle Erkennungen anzuzeigen.

Die häufigsten E-Mail-Empfänger komplexer Bedrohungen – Widget

Im Widget **Häufigste E-Mail-Empfänger komplexer Bedrohungen** werden die Empfänger angezeigt, die die höchste Zahl an verdächtigen Nachrichten in Deep Discovery Email Inspector empfangen haben.

Die Tabelle enthält Funde basierend auf dem ausgewählten Zeitraum. Klicken Sie auf eine Zahl unter **Funde** oder **Nachrichten mit hohem Risiko**, um weitere Informationen über die Funde zu erhalten. **Funde**: Enthält

alle erkannten E-Mail-Nachrichten, einschließlich Nachrichten mit hohem Risiko.

Kapitel 23

Integration und Richtlinieneinstellungen für Deep Discovery Inspector

In diesem Abschnitt wird erläutert, wie Deep Discovery Inspector in Apex Central integriert und Richtlinien über die Apex Central-Konsole verwaltet werden.

Es werden folgende Themen behandelt:

Übersicht über die Integration von Deep Discovery Inspector

In diesem Abschnitt wird der Umfang der Vernetzung (Integration) zwischen Apex Central und den unterstützten Versionen von Deep Discovery Inspector erörtert.

Integrierte Funktion	5.0
Registrierung	Über die Deep Discovery Inspector Management-Konsole (durch den MCP Agent)
Single Sign-On	Unterstützt
Lizenzverwaltung	Keine
Befehlsnachverfolgung	Unterstützt
Über Apex Central verteilte Komponenten	Alle Komponenten
Über Apex Central verwaltete und verteilte Richtlinien	• *Liste 'Verweigern'/Liste 'Zulassen' auf Seite 23-10* • *Überwachte Netzwerkgruppen hinzufügen auf Seite 23-12* • *Registrierte Dienste hinzufügen auf Seite 23-14* • *Einstellungen für Virtual Analyzer konfigurieren auf Seite 23-15*
Im Benutzer-/Endpunktverzeichnis angezeigte Informationen	Keine
Ad-hoc-Abfragen	Wählen Sie eine der folgenden Datenansichten während der Ausführung einer Ad-hoc-Abfrage zum Anzeigen von Produktinformationen und Protokollen aus: • Informationen zum Produktstatus • Deep Discovery Informationen

Integrierte Funktion	5.0
Produktspezifische Dashboard-Widgets	• *Deep Discovery Inspector – Systemstatus – Widget auf Seite 23-7* • *Von Deep Discovery Inspector betroffene Hosts – Widget auf Seite 23-4*
Gemeinsam mit anderen verwalteten Produkten genutzte Dashboard-Widgets	Keine
Statische Berichtsvorlagen	Trend Micro Deep Discovery Inspector-Berichte
Benutzerdefinierte Berichtvorlagen (vordefiniert)	• Trend Micro Deep Discovery Inspector – Hostschweregrad – Übersicht • Erkennung verdächtiger Bedrohungen durch Trend Micro Discovery Inspector – Übersicht
Ereignisbenachrichtigungen	Erweiterte Bedrohungsaktivität • C&C-Callback-Warnung • C&C-Callback-Ausbruchswarnung • Virtual Analyzer Funde mit hohem Risiko • Hostfunde mit hohem Risiko • Funde von bekanntem gezieltem Angriffsverhalten • Potenzielle Dokumenten-Schwachstellenfunde • Rootkit- oder Hacking-Tool-Funde • SHA-1-Funde Liste 'Verweigern' • Wurm- oder Dateiinfektorverteilung gefunden • Funde korrelierter Vorfälle
Vorfallsmanagement für die Funktion 'Prävention vor Datenverlust' (Data Loss Prevention, DLP)	Nicht zutreffend

Integrierte Funktion	5.0
Verwaltung von verdächtigen Objekten und IOC-Dateien	• Sendet verdächtige Objekte an Apex Central • Synchronisiert verdächtige Objekte mit Apex Central

Von Deep Discovery Inspector betroffene Hosts – Widget

Dieses Widget zeigt Informationen zu den Deep Discovery Inspector-Funden auf betroffenen Hosts an.

In der Standardansicht werden nur die wichtigsten 10 Hosts mit dem Schweregrad 'Hoch' nach **Anzahl der Funde** angezeigt.

Um zu ändern, ob das Widget Hosts nach Erkennungsanzahl oder nach Erkennungszeit anzeigt, klicken Sie auf das Einstellungssymbol (>) und wählen Sie eine der folgenden Optionen aus:

- **Anzahl der Funde**: Wählen Sie die Anzahl der Hosts (Die wichtigsten 10, 25 oder 50) in der Dropdown-Liste aus.
- **Zeitpunkt der Erkennung**: Wählen Sie die Anzahl der Hosts (die letzten 10/25/50/100) in der Dropdown-Liste aus.

Verwenden Sie die Dropdown-Liste **Bereich**, um den Zeitraum für die angezeigten Daten auszuwählen.

- Wenn Sie Hosts nach **Anzahl der Funde** anzeigen, können Sie Daten für 'Heute', '1 Woche', '2 Wochen' oder '1 Monat' anzeigen.
- Wenn Sie Hosts nach dem **Zeitpunkt der Erkennung** anzeigen, können Sie nur Daten für 'Heute' oder '1 Woche' anzeigen.

Sie können auch die Dropdown-Liste **Schweregrad** verwenden, um den Schweregrad anzugeben, wenn Hosts nach **Zeitpunkt der Erkennung** angezeigt werden.

Spalte	Beschreibung
IP-Adresse	Zeigt die IP-Adresse des betroffenen Hosts an

Spalte	Beschreibung
Host-Name	Zeigt den Namen des betroffenen Hosts an.
Netzwerkgruppe	Zeigt den Namen der Gruppe der überwachten Netzwerke an, die es Deep Discovery Inspector gestatten, zu ermitteln, ob Angriffe von innerhalb oder außerhalb des Netzwerks stammen
Funde	Zeigt die Anzahl der auf betroffenen Hosts erkannten Funde an • Klicken Sie auf eine Zahl in der Spalte **Funde**, um weitere Informationen im Fenster **Funde** anzuzeigen. • Klicken Sie auf den Link **Anzeigen** in der Spalte **Details**, um sich mittels Single Sign-On bei Deep Discovery Inspector anzumelden und das Fenster **Protokollabfragedetails zu Funden** anzuzeigen. Wenn das Protokoll gelöscht wird, zeigt die Konsole eine Meldung an, die Sie über die Aktion informiert.
Neuester Fund	Zeigt das Datum und die Uhrzeit an, zu dem/der Deep Discovery Inspector zuletzt ein potenzielles/bekanntes Risiko erkannt hat.

Von Deep Discovery Inspector betroffene Hostfunde

Durch Klicken auf einen Wert in der Spalte **Funde** des Widgets 'Von Deep Discovery Inspector betroffene Hosts' wird eine Tabelle mit hostbezogenen Informationen angezeigt:

Tabelle 23-1. Informationen im Zusammenhang mit Hosts

Name der Spalte	Informationen
Datum	Datum und Uhrzeit, zu dem/der Deep Discovery Inspector das Erkennungsprotokoll erstellt hat

Name der Spalte	Informationen
Schweregrad	Beschreibung der Schweregrade: • Hoch: Bekanntes bösartiges Verhalten oder an Verbindungen mit hohem Risiko beteiligt • Mittel: IP-Adresse/Domäne/URL ist dem Reputation-Dienst nicht bekannt • Niedrig: Reputation-Dienst gibt vorherige Infektion oder Spam-Beteiligung an • Information: Ein Objekt, das wahrscheinlich harmlos ist
Erkennung	Die Beschreibung der Regel oder der Malware-Name
Bedrohungsart	Eine der folgenden Optionen: • Datei-Pattern • Bösartiges Verhalten • Verdächtiges Verhalten • Schwachstelle • Grayware • Web Reputation • Störende Anwendungen
Quell-IP	Die IP-Adresse der Quelle, von der ein verdächtiges Objekt stammt
Ziel-IP	Die IP-Adresse des vorgesehenen Ziels eines verdächtigen Objekts
Protokoll	Das bei der Übertragung eines verdächtigen Objekts von der Quelle zum Ziel verwendete Protokoll
Dateiname	Der aus dem Beispiel extrahierte Dateiname
Protokolliert von	Der Hostname von Deep Discovery Inspector, der das Beispiel analysiert hat
Details	Klicken Sie auf **Anzeigen**, um ein anderes Fenster zu öffnen, das eine detaillierte Analyse des verdächtigen Objekts in Deep Discovery Inspector bietet.

Deep Discovery Inspector – Systemstatus – Widget

Verwenden Sie dieses Widget für Deep Discovery Inspector Appliances, um die Ressourcennutzung und die Anzahl der Beispiele in der Warteschlange anzuzeigen, die auf die Verarbeitung durch Virtual Analyzer warten.

Standardmäßig zeigt das Widget alle Daten für alle verwalteten Produkte/Server an, die gemäß den Kontoberechtigungen eines Benutzers zulässig sind.

Klicken Sie auf das Einstellungssymbol (>), um Folgendes zu konfigurieren:

- **Titel**: Geben Sie einen neuen und aussagekräftigen Titel für das Widget an.
- **Bereich: Alle Produkte**: Klicken Sie auf die Schaltfläche **>>**, um die Produkte anzugeben, die Daten für die Anzeige beitragen.

Das Widget zeigt die folgenden Daten der Systemressourcen an, um zu überprüfen, ob alle Ressourcen von Deep Discovery Inspector den Spezifikationen entsprechen.

Spalte	Beschreibung
Servername	Der Servername für jede einzelne Deep Discovery Inspector-Appliance • **Detaillierten Status anzeigen**: Klicken Sie auf diese Option, um Details zum Produktstatus anzuzeigen. Daten vom Typ 'Einzelheiten zum Status anzeigen' können auch über eine Protokollabfrage des Produktstatus angezeigt werden. Diese Tabelle enthält den Prozentsatz der CPU-Auslastung, die prozentuale und tatsächliche Speicher- und Festplattennutzung sowie die Anzahl der Beispiele in der Warteschlange, die auf die Verarbeitung durch Virtual Analyzer warten. Informationen zur Fehlerbehebung finden Sie in den Feldern 'Produkthost', 'Produkt-IP', 'Verbindungsstatus' und 'Produktversion'. Deep Discovery Inspector sendet alle 5 Minuten ein Update des Systemstatus an Apex Central. Wenn angezeigt wird, erhält Apex Central die neuesten Systemstatusprotokolle von Deep Discovery Inspector nicht. Bestätigen Sie, dass Deep Discovery Inspector aktiv ist und über eine Verbindung verfügt. • **Anmeldekonsole**: Klicken Sie auf diese Option, um auf die Management-Konsole von Deep Discovery Inspector zuzugreifen. Es sind keine Anmeldedaten erforderlich.
CPU-Auslastung	Der Prozentsatz der vom Server ausgelasteten CPU • wird angezeigt, wenn die CPU-Auslastung des Servers im Durchschnitt 80 % überschreitet. **Hinweis** Die Grenzwerte für CPU, Arbeitsspeicher, Festplattennutzung und Beispiele in der Warteschlange können nicht konfiguriert werden. Wenn Warnungen kontinuierlich auftreten, sollten Sie ein Upgrade Ihrer Deep Discovery Inspector/Virtual Analyzer-Appliances in Betracht ziehen.

Spalte	Beschreibung
Speicherauslastung	Der Prozentsatz des auf dem Server verfügbaren Speicherplatzes • wird angezeigt, wenn die Speicherauslastung 80 % überschreitet. **Hinweis** Die Grenzwerte für CPU, Arbeitsspeicher, Festplattennutzung und Beispiele in der Warteschlange können nicht konfiguriert werden. Wenn Warnungen kontinuierlich auftreten, sollten Sie ein Upgrade Ihrer Deep Discovery Inspector/Virtual Analyzer-Appliances in Betracht ziehen.
Festplattennutzung	Der Prozentsatz der auf dem Server verfügbaren Festplattenspeicher • wird angezeigt, wenn die Festplattennutzung 80 % überschreitet. **Hinweis** Die Grenzwerte für CPU, Arbeitsspeicher, Festplattennutzung und Beispiele in der Warteschlange können nicht konfiguriert werden. Wenn Warnungen kontinuierlich auftreten, sollten Sie ein Upgrade Ihrer Deep Discovery Inspector/Virtual Analyzer-Appliances in Betracht ziehen.

Spalte	Beschreibung
Beispiele in der Warteschlange	Die Anzahl der Beispiele in der Warteschlange, die auf die Verarbeitung durch Virtual Analyzer warten • wird angezeigt, wenn die Warteschlange von Virtual Analyzer 40 Beispiele überschreitet. **Hinweis** Die Grenzwerte für CPU, Arbeitsspeicher, Festplattennutzung und Beispiele in der Warteschlange können nicht konfiguriert werden. Wenn Warnungen kontinuierlich auftreten, sollten Sie ein Upgrade Ihrer Deep Discovery Inspector/Virtual Analyzer-Appliances in Betracht ziehen.

Richtlinieneinstellungen für Deep Discovery Inspector

In diesem Abschnitt wird erläutert, wie Deep Discovery Inspector-Richtlinieneinstellungen im Fenster **Richtlinie erstellen** konfiguriert werden.

Liste 'Verweigern'/Liste 'Zulassen'

Das Fenster der Liste 'Verweigern'/Liste 'Zulassen' ist in die folgenden Registerkarten unterteilt: 'Liste 'Verweigern", Liste 'Zulassen", 'Importieren/Exportieren'.

Tabelle 23-2. Liste 'Verweigern'/Liste 'Zulassen' – Registerkarten

Registerkarten	Beschreibung
Liste 'Verweigern'	Deep Discovery Inspector überwacht die Verbindung mit den Einträgen in der Liste 'Verweigern' oder überwacht die Verbindung und setzt sie zurück.

Registerkarten	Beschreibung
Zulassungsliste	Deep Discovery Inspector lässt die Verbindung mit Einträgen in der Liste 'Zulassen' zu. **Tipp** Verwenden Sie die Liste 'Zulassen', um die Anzahl der falsch positiven Funde in der Liste 'Verweigern' zu reduzieren.
Importieren/Exportieren	Sie können Einträge der Liste 'Verweigern' oder der Liste 'Zulassen' importieren oder exportieren.

Benutzerdefinierte Liste 'Verweigern' erstellen

Prozedur

1. Wählen Sie die Registerkarte **Liste 'Verweigern'** aus.
2. Um der Liste 'Verweigern' eine Entität hinzuzufügen, wählen Sie **Hinzufügen** aus.

   Das Fenster **Element zur Liste 'Verweigern' hinzufügen** wird angezeigt.
3. Überprüfen Sie im Fenster **Elemente zur Liste 'Verweigern' hinzufügen** die Informationen, fügen Sie ggf. Kommentare hinzu und klicken Sie auf **Speichern**.

Benutzerdefinierte Liste 'Zulassen' erstellen

Prozedur

1. Wählen Sie die Registerkarte **Liste 'Zulassen'** aus.
2. Um der Liste 'Zulassen' eine Entität hinzuzufügen, wählen Sie **Hinzufügen** aus.

Das Fenster **Elemente zur Liste 'Zulassen' hinzufügen** wird angezeigt.

3. Überprüfen Sie im Fenster **Elemente zur Liste 'Zulassen' hinzufügen** die Informationen, fügen Sie ggf. Kommentare hinzu und klicken Sie auf **Speichern**.

Benutzerdefinierte Listen 'Verweigern' oder 'Zulassen' importieren/exportieren

Prozedur

1. Wählen Sie die Registerkarte **Importieren/Exportieren** aus.
2. Um die aktuelle Liste 'Verweigern' oder 'Zulassen' zu exportieren, wählen Sie eine Liste aus und klicken Sie auf **Exportieren**.
3. Um die aktuelle Liste 'Verweigern' oder 'Zulassen' zu überschreiben, navigieren Sie zum Speicherort und klicken Sie auf **Importieren**.

   Die aktuelle ausgewählte Liste wird überschrieben.

Überwachte Netzwerkgruppen hinzufügen

Richten Sie Gruppen überwachter Netzwerke mit Hilfe von IP-Adressen ein, um es Deep Discovery Inspector zu ermöglichen, zu ermitteln, welche Angriffe von innerhalb oder außerhalb des Netzwerks stammen.

Prozedur

1. Klicken Sie auf **Hinzufügen**.
2. Geben Sie einen Gruppennamen an.

Tipp

Geben Sie bestimmte Gruppen mit beschreibenden Namen zur einfachen Identifizierung des Netzwerks an, zu dem die IP-Adresse gehört. Zum Beispiel 'Finanznetzwerk', 'IT-Netzwerk' oder 'Administration'.

3. Geben Sie einen IP-Adressbereich im Textfeld an (bis zu 1000 IP-Adressbereiche).

   Im Lieferumfang von Deep Discovery Inspector ist ein überwachtes Netzwerk namens **Standard** enthalten, das die folgenden IP-Adressblöcke enthält, die von der IANA (Internet Assigned Numbers Authority) für private Netzwerke reserviert sind:

   - 10.0.0.0 - 10.255.255.255
   - 172.16.0.0 - 172.31.255.255
   - 192.168.0.0 - 192.168.255.255

   Hinweis

   - Wenn Sie das Netzwerk **Standard** nicht entfernen, müssen Sie diese IP-Adressblöcke nicht angeben, wenn Sie ein neues überwachtes Netzwerk hinzufügen.
   - Verwenden Sie einen Bindestrich, um einen IP-Adressbereich anzugeben.

     Beispiel: 192.168.1.0-192.168.1.255.
   - Verwenden Sie einen Schrägstrich, um die Subnetzmaske für die IP-Adressen anzugeben.

     Beispiel: 192.168.1.0/255.255.255.0 oder 192.168.1.0/24.
   - Bis zu drei Ebenen von Untergruppen können hinzugefügt werden.

4. Wählen Sie die Netzwerkzone der Netzwerkgruppe aus:
   - **Vertrauenswürdig**: Dies ist ein sicheres Netzwerk
   - **Nicht vertrauenswürdig**: Es bestehen gewisse Zweifel an der Sicherheit des Netzwerks.
5. Klicken Sie auf **Hinzufügen**.
6. Klicken Sie auf **Fertig stellen**.

Registrierte Dienste hinzufügen

Fügen Sie verschiedene Server für bestimmte Dienste hinzu, die Ihre Organisation intern verwendet oder als vertrauenswürdig für die Einrichtung des Netzwerkprofils erachtet. Durch die Ermittlung vertrauenswürdiger Dienste im Netzwerk wird die Erkennung nicht autorisierter Anwendungen und Dienste gewährleistet.

Fügen Sie nur vertrauenswürdige Dienste (bis zu 1000 Dienste) hinzu, um die Genauigkeit Ihres Netzwerkprofils sicherzustellen.

Prozedur

1. Wählen Sie einen Dienst aus der Dropdown-Liste aus.

TABELLE 23-3. Diensttypen

DIENST	BESCHREIBUNG
DNS	Der als DNS-Server verwendete Netzwerkserver.
FTP	Der als FTP-Server verwendete Netzwerkserver.
HTTP-Proxy	Der als HTTP-Proxy-Server verwendete Netzwerkserver.
SMTP	Der als SMTP-Server verwendete Netzwerkserver.
SMTP Open Relay	Der als SMTP Open Relay-Server verwendete Netzwerkserver.
Software-Update-Server	Der für WSUS (Windows Server Update Services) verwendete Netzwerkserver oder der Server, der die Remote-Verteilung durchführt.
Server für Sicherheitsaudit	Der zur Erkennung von Schwachstellen und unsicheren Konfigurationen verwendete Netzwerkserver.

Dienst	Beschreibung
Active Directory	Der als Active Directory-Server verwendete Netzwerkserver.
Domänencontroller	Der als Domänencontroller-Server verwendete Netzwerkserver.
Datenbankserver	Der als Datenbankserver verwendete Netzwerkserver.
Authentifizierungsserver – Kerberos	Der zur Bereitstellung der Kerberos-Authentifizierung verwendete Netzwerkserver.
Dateiserver	Der zur Bereitstellung eines Speicherorts für den Zugriff auf freigegebene Dateien verwendete Netzwerkserver.
Webserver	Der als Webserver verwendete Netzwerkserver.
Content Management Server	Der für die Verwaltung von Inhalten verwendete Netzwerkserver.
RADIUS-Server	Der als Radius-Authentifizierungsserver verwendete Netzwerkserver.

Namen registrierter Dienste werden im Abschnitt **Definierte registrierte Dienste** angezeigt.

2. Geben Sie einen Servernamen an.
3. Geben Sie eine IP-Adresse an.
4. Klicken Sie auf **Hinzufügen**.

Einstellungen für Virtual Analyzer konfigurieren

Verwenden Sie diese Option, um die Analyse von Bedrohungsdateien zu aktivieren oder zu deaktivieren.

Prozedur

1. Stellen Sie sicher, dass der Verwaltungsport auf das Internet zugreifen kann. Virtual Analyzer muss möglicherweise Daten über diesen Port abfragen.
2. Aktivieren Sie im Fenster **Virtual Analyzer Konfiguration** die Option **Dateien an Virtual Analyzer übermitteln**.
3. Wählen Sie ein Analysemodul.
   - Wählen Sie unter **Interner Analyzer** einen Netzwerktyp aus.

TABELLE 23-4. Analyzer-Netzwerktypen

MODULOPTION	BESCHREIBUNG
Management-Netzwerk	Wählen Sie diesen Netzwerktyp aus, um Virtual Analyzer Datenverkehr über einen Verwaltungsport zu leiten.
Benutzerdefiniertes Netzwerk/ Bestimmtes Netzwerk	Wählen Sie diesen Netzwerktyp aus, um einen bestimmten Port für Virtual Analyzer-Datenverkehr zu konfigurieren. Stellen Sie sicher, dass der Port direkt eine Verbindung zu einem externen Netzwerk herstellen kann.
Kein Netzwerk/Isoliertes Netzwerk	Wählen Sie diesen Netzwerktyp aus, um Virtual Analyzer-Datenverkehr in Virtual Analyzer zu isolieren, und wenn die Umgebung keine Verbindung zu einem externen Netzwerk hat.

TABELLE 23-5. Optionen für 'Benutzerdefiniertes Netzwerk/Bestimmtes Netzwerk'

OPTIONEN	AKTION
Virtual Analyzer-Port	Wählen Sie einen Virtual Analyzer-Port aus. **Hinweis** Weisen Sie einen Virtual Analyzer-Port zu, der sich vom Deep Discovery Inspector-Datenport unterscheidet.
IPv4 konfigurieren	**Automatisch (über DHCP)** ist ausgewählt. Diese Einstellung kann nicht geändert werden.

- Geben Sie für **Externer Analyzer** eine Virtual Analyzer-IP-Adresse und einen API-Schlüssel ein.

Tipp

Der externe Analyzer (Deep Discovery Advisor oder Deep Discovery Analyzer) verfügt über mehr Analysefunktionen als der interne Analyzer (Virtual Analyzer).

4. (Optional) Aktivieren und konfigurieren Sie für den internen Virtual Analyzer einen dedizierten Proxy.

Hinweis

Um die Proxy-Einstellungen zu konfigurieren, muss das Management-Netzwerk oder das benutzerdefinierte Netzwerk als Netzwerktyp ausgewählt werden.

a. Wählen Sie in den **Proxy -Einstellungen** die Option **Dedizierte Proxy-Einstellungen verwenden** aus.

b. Geben Sie unter **Server-Adresse** die IP-Adresse, den Hostnamen oder den FQDN des Proxy-Servers ein.

c. Geben Sie die Portnummer ein.

d. (Optional) Geben Sie Anmeldedaten für die Authentifizierung beim Proxy-Server ein.

5. (Optional) Wählen Sie für den internen Virtual Analyzer die Option **Mögliche Mac OS Bedrohungen zur Analyse an die Trend Micro Cloud-Sandboxes senden** aus.

6. Konfigurieren Sie die Optionen unter **Dateiübermittlung**:

   a. Geben Sie die maximale Dateigröße an. Das Ändern dieser Einstellung kann die Leistung von Deep Discovery Inspector beeinträchtigen.

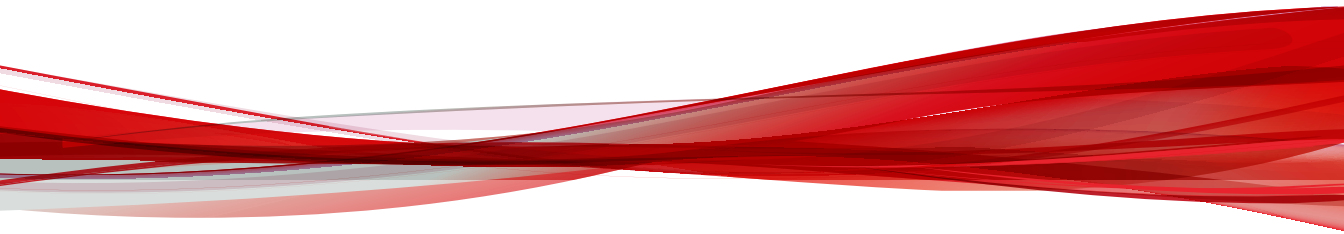
   b. Aktivieren Sie Certified Safe Software Service (CSSS).

Hinweis

Certified Safe Software Service (CSSS) ist die Trend Micro Cloud-Datenbank für sichere Dateien. Deep Discovery Inspector fragt Trend Micro Datenzentren ab, um in der Datenbank zu überprüfen, welche Dateien übermittelt wurden.

Teil IX

Deep Security Manager Widgets



Kapitel 24

Deep Security Manager Dashboard Widgets

Dieser Abschnitt enthält Hilfethemen für die im Trend Micro Apex Central unterstützten Deep Security Manager Dashboard Widgets.

Es werden folgende Themen behandelt:

Deep Security – Anti-Malware-Ereignisverlauf – Widget

Dieses Widget zeigt die Anzahl der Anti-Malware-Ereignisse an, die im angegebenen Zeitraum aufgetreten sind.

Klicken Sie auf einen Balken, um die Seite **Ereignisse** von Deep Security Manager zu öffnen, die so gefiltert ist, dass Anti-Malware-Ereignisse für den angegebenen Ereignistyp und Zeitraum angezeigt werden. Sie können auch auf die Ereignistypen in der Legende klicken, um die Diagrammansicht zu ändern.

Verwenden Sie die Dropdown-Liste **Bereich**, um den Zeitraum für die angezeigten Daten auszuwählen.

Ändern Sie den verwalteten Server, den das Widget als Quelle verwendet, indem Sie auf das Einstellungssymbol klicken (>). Wählen Sie auf dem erscheinenden Bildschirm den verwalteten Server aus, der als Quelle verwendet werden soll, und klicken Sie auf **Speichern**.

Hinweis

Die im Widget angezeigten Daten sind auf die Daten beschränkt, die aufgrund der Benutzerkontoberechtigungen zulässig sind.

Tipp

Dieses Widget kann nur Daten von einem einzigen Deep Security-Server anzeigen. Erstellen Sie ein neues Widget für jeden Server, um mehrere Deep Security-Server zu überwachen.

Deep Security – Anti-Malware-Status (Malware) – Widget

Dieses Widget zeigt die fünf häufigsten Malware-Bedrohungen an, die auf Endpunkten erkannt werden.

Klicken Sie auf einen Zähler in der Spalte **Gesamt**, um zusätzliche Details in der Deep Security Manager-Konsole anzuzeigen.

Verwenden Sie die Dropdown-Liste **Bereich**, um den Zeitraum für die angezeigten Daten auszuwählen.

Ändern Sie den verwalteten Server, den das Widget als Quelle verwendet, indem Sie auf das Einstellungssymbol klicken (>). Wählen Sie auf dem erscheinenden Bildschirm den verwalteten Server aus, der als Quelle verwendet werden soll, und klicken Sie auf **Speichern**.

Um eine Deep Security-Installation für die Deep Security-Widgets verfügbar zu machen, gehen Sie zu **Administration** > **Verwaltete Server** > **Serverregistrierung** und fügen Sie einen neuen Deep Security Server hinzu.

Hinweis

Die im Widget angezeigten Daten sind auf die Daten beschränkt, die aufgrund der Benutzerkontoberechtigungen zulässig sind.

Tipp

Dieses Widget kann nur Daten von einem einzigen Deep Security-Server anzeigen. Erstellen Sie ein neues Widget für jeden Server, um mehrere Deep Security-Server zu überwachen.

Daten	Beschreibung
Malware-Name	Name der Malware-Bedrohung
Anzahl an Dateien, die nicht gesäubert werden können	Anzahl der Vorkommen der Bedrohung, die Deep Security nicht säubern konnte
Gesamt	Anzahl der Ereignisse im Zeitraum und Prozentsatz der darin dargestellten gesamten Ereignisse dieses Typs
Vorherige Gesamtanzahl	Anzahl der Ereignisse im Zeitraum, der dem aktuellen Zeitraum vorangeht

Daten	Beschreibung
Trend	Änderung in Prozent vom vorherigen zum aktuellen Zeitraum

Deep Security – (erkannte) Aktivität des Anwendungstyps – Widget

Dieses Widget zeigt die fünf häufigsten, mit IPS (erkannten) Ereignissen verbundenen Anwendungstypen an.

Klicken Sie auf einen Wert in der Spalte **Gesamt**, um das Fenster **Ereignisse** von Deep Security Manager zu öffnen, in dem gefilterte IPS (erkannte) Ereignisse angezeigt werden, die mit dem spezifischen Anwendungstyp verbunden sind.

Ändern Sie den verwalteten Server, den das Widget als Quelle verwendet, indem Sie auf das Einstellungssymbol klicken (>). Wählen Sie auf dem erscheinenden Bildschirm den verwalteten Server aus, der als Quelle verwendet werden soll, und klicken Sie auf **Speichern**.

Hinweis

Die im Widget angezeigten Daten sind auf die Daten beschränkt, die aufgrund der Benutzerkontoberechtigungen zulässig sind.

Tipp

Dieses Widget kann nur Daten von einem einzigen Deep Security-Server anzeigen. Erstellen Sie ein neues Widget für jeden Server, um mehrere Deep Security-Server zu überwachen.

Daten	Beschreibung
Name des Anwendungstyps	Der Name des Anwendungstyps

Daten	Beschreibung
Gesamt	Die Anzahl der Ereignisse im Zeitraum und der Prozentsatz der gesamten Ereignisse, die dieser Typ darstellt
Vorherige Gesamtanzahl	Die Anzahl der Ereignisse im Zeitraum, der dem aktuellen Zeitraum vorangeht
Trend	Die Änderung in Prozent vom vorherigen zum aktuellen Zeitraum

Deep Security – (verhinderte) Aktivität des Anwendungstyps – Widget

Dieses Widget zeigt die fünf häufigsten, mit IPS (verhinderten) Ereignissen verbundenen Anwendungstypen an.

Klicken Sie auf einen Wert in der Spalte **Gesamt**, um das Fenster **Ereignisse** von Deep Security Manager zu öffnen, in dem gefilterte IPS (verhinderte) Ereignisse angezeigt werden, die mit dem spezifischen Anwendungstyp verbunden sind.

Ändern Sie den verwalteten Server, den das Widget als Quelle verwendet, indem Sie auf das Einstellungssymbol klicken (>). Wählen Sie auf dem erscheinenden Bildschirm den verwalteten Server aus, der als Quelle verwendet werden soll, und klicken Sie auf **Speichern**.

Hinweis

Die im Widget angezeigten Daten sind auf die Daten beschränkt, die aufgrund der Benutzerkontoberechtigungen zulässig sind.

Tipp

Dieses Widget kann nur Daten von einem einzigen Deep Security-Server anzeigen. Erstellen Sie ein neues Widget für jeden Server, um mehrere Deep Security-Server zu überwachen.

Daten	Beschreibung
Name des Anwendungstyps	Der Name des Anwendungstyps
Gesamt	Die Anzahl der Ereignisse im Zeitraum und der Prozentsatz der gesamten Ereignisse, die dieser Typ darstellt
Vorherige Gesamtanzahl	Die Anzahl der Ereignisse im Zeitraum, der dem aktuellen Zeitraum vorangeht
Trend	Die Änderung in Prozent vom vorherigen zum aktuellen Zeitraum

Deep Security – Überblick über die Komponenten – Widget

Dieses Widget zeigt die Versionsnummern der verfügbaren Deep Security Komponenten-Updates und den Prozentsatz der Endpunkte an, die auf die neueste Version aktualisiert wurden.

Wichtig

Das Widget zeigt nur Daten von Deep Security 7.5 oder höher an.

Ändern Sie den verwalteten Server, den das Widget als Quelle verwendet, indem Sie auf das Einstellungssymbol klicken (>). Wählen Sie auf dem erscheinenden Bildschirm den verwalteten Server aus, der als Quelle verwendet werden soll, und klicken Sie auf **Speichern**.

Hinweis

Die im Widget angezeigten Daten sind auf die Daten beschränkt, die aufgrund der Benutzerkontoberechtigungen zulässig sind.

Daten	Beschreibung
Komponenten	Der Name der Deep Security Komponente.

Daten	Beschreibung
Aktuelle Version	Die Version, die gegenwärtig auf Deep Security Manager verfügbar ist.
Aktualisierter Prozentsatz	Der Prozentsatz der verwalteten Computer, die auf die neueste Version aktualisiert wurden. **Hinweis** Updates sind möglicherweise nicht für alle verwalteten Computer zutreffend.

Das Widget zeigt die Versionsnummern für die folgenden Komponenten an.

Komponente	Beschreibung
Smart Scan Agent Pattern	Die kleinere Malware-Pattern-Erkennungsdatei, die an die Deep Security Virtual Appliance gesendet wird. Wenn ein Vergleich mit diesen Pattern darauf hinweist, dass eine Datei auf einem Computer möglicherweise bösartig ist, wird die Datei zwecks Bestätigung mit der zuverlässigeren Pattern-Datei auf dem Smart Scan Server verglichen.
Viren-Pattern	Eine Datei, die der Deep Security Virtual Appliance dabei hilft, Virensignaturen zu erkennen, d. h. eindeutige Abfolgen von Bits und Bytes, die auf einen Virus hindeuten.
IntelliTrap-Pattern	IntelliTrap sucht nach möglicherweise in Dateien verborgener Malware, bei der Echtzeitkomprimierung in Verbindung mit anderen Malware-Merkmalen, z. B. Packer, verwendet wird.
Spyware-Aktivmonitor-Pattern	Pattern zur Spyware-Erkennung.
Virensuch-Engine	Die Engine, die Viren-Pattern bei einer Virensuche auf eine Datei anwendet.
Deep Security Regelaktualisierung	DPI-Regeln bieten Schutz mittels Intrusion Detection/Prevention (IDS/IPS), indem Schwachstellen vor bekannten und bisher noch unbekannten Angriffen geschützt werden.

Deep Security – Funktionsübersicht – Widget

Dieses Widget zeigt die letzte Aktivität jedes Deep Security Moduls.

Verwenden Sie die Dropdown-Liste **Bereich**, um den Zeitraum für die angezeigten Daten auszuwählen.

Das Widget zeigt aggregierte Informationen von mehreren verwalteten Servern an.

Ändern Sie den verwalteten Server, den das Widget als Quelle verwendet, indem Sie auf das Einstellungssymbol klicken (>). Wählen Sie auf dem erscheinenden Bildschirm den verwalteten Server aus, der als Quelle verwendet werden soll, und klicken Sie auf **Speichern**.

Tipp

Zum Anzeigen von nicht aggregierten Daten von mehreren verwalteten Servern fügen Sie ein neues Widget für jeden verwalteten Server hinzu.

Hinweis

Die im Widget angezeigten Daten sind auf die Daten beschränkt, die aufgrund der Benutzerkontoberechtigungen zulässig sind.

Daten	Beschreibung
Modul	Das Modul Deep Security
Geschützte Computer	Die aktuelle Anzahl der verwalteten Computer, die durch dieses Modul geschützt werden, und der Prozentsatz aller verwalteten Computer, die dies darstellt
Anzahl der Ereignisse	Die Anzahl der Ereignisse, die während des festgelegten Zeitraums vom Modul generiert wurden
Trend	Die Änderung in Prozent bei der Anzahl der Ereignisse seit dem vorherigen Zeitraum
Gesamtzahl der Computer	Die Gesamtzahl der Computer, die von Deep Security verwaltet werden

Deep Security – (erkannte) Firewall-Aktivität – Widget

Dieses Widget zeigt die fünf häufigsten Firewall-Regeln an, die die größte Anzahl der Ereignisse ausgelöst haben und im Erkennungsmodus verwendet werden.

Klicken Sie auf einen Wert in der Spalte **Gesamt**, um das Fenster **Ereignisse** von Deep Security Manager zu öffnen, das so gefiltert ist, dass von der spezifischen Regel ausgelöste Firewall-Ereignisse angezeigt werden.

Ändern Sie den verwalteten Server, den das Widget als Quelle verwendet, indem Sie auf das Einstellungssymbol klicken (>). Wählen Sie auf dem erscheinenden Bildschirm den verwalteten Server aus, der als Quelle verwendet werden soll, und klicken Sie auf **Speichern**.

Hinweis

Die im Widget angezeigten Daten sind auf die Daten beschränkt, die aufgrund der Benutzerkontoberechtigungen zulässig sind.

Daten	Beschreibung
Grund	Name der Regel
Gesamt	Die Anzahl der Ereignisse im Zeitraum und der Prozentsatz der gesamten Ereignisse, die dieser Typ darstellt
Vorherige Gesamtanzahl	Die Anzahl der Ereignisse im Zeitraum, der dem aktuellen Zeitraum vorangeht
Trend	Die Änderung in Prozent vom vorherigen zum aktuellen Zeitraum

Deep Security – (verhinderte) Firewall-Aktivität – Widget

Dieses Widget zeigt die fünf häufigsten Firewall-Regeln an, die die größte Anzahl der Ereignisse ausgelöst haben und im Modus 'Verhindern' verwendet werden.

Klicken Sie auf einen Wert in der Spalte **Gesamt**, um das Fenster **Ereignisse** von Deep Security Manager zu öffnen, das so gefiltert ist, dass von der spezifischen Regel ausgelöste Firewall-Ereignisse angezeigt werden.

Ändern Sie den verwalteten Server, den das Widget als Quelle verwendet, indem Sie auf das Einstellungssymbol klicken (>). Wählen Sie auf dem erscheinenden Bildschirm den verwalteten Server aus, der als Quelle verwendet werden soll, und klicken Sie auf **Speichern**.

Hinweis

Die im Widget angezeigten Daten sind auf die Daten beschränkt, die aufgrund der Benutzerkontoberechtigungen zulässig sind.

Daten	Beschreibung
Grund	Name der Regel
Gesamt	Die Anzahl der Ereignisse im Zeitraum und der Prozentsatz der gesamten Ereignisse, die dieser Typ darstellt
Vorherige Gesamtanzahl	Die Anzahl der Ereignisse im Zeitraum, der dem aktuellen Zeitraum vorangeht
Trend	Die Änderung in Prozent vom vorherigen zum aktuellen Zeitraum

Deep Security – Firewall-Ereignisverlauf – Widget

Dieses Widget zeigt die Anzahl der Firewall-Ereignisse an, die von Deep Security Manager im angegebenen Zeitraum erkannt wurden. Das Diagramm zeigt die von Firewall-Regeln ausgelösten Ereignisse im Erkennungs- und im Verhinderungsmodus an.

Klicken Sie auf einen Balken, um zusätzliche Details in der Deep Security Manager-Konsole anzuzeigen. Sie können auch auf die Ereignistypen in der Legende klicken, um die Diagrammansicht zu ändern.

Verwenden Sie die Dropdown-Liste **Bereich**, um den Zeitraum für die angezeigten Daten auszuwählen.

Ändern Sie den verwalteten Server, den das Widget als Quelle verwendet, indem Sie auf das Einstellungssymbol klicken (>). Wählen Sie auf dem erscheinenden Bildschirm den verwalteten Server aus, der als Quelle verwendet werden soll, und klicken Sie auf **Speichern**.

Um eine Deep Security-Installation für die Deep Security-Widgets verfügbar zu machen, gehen Sie zu **Administration** > **Verwaltete Server** > **Serverregistrierung** und fügen Sie einen neuen Deep Security Server hinzu.

Hinweis

Die im Widget angezeigten Daten sind auf die Daten beschränkt, die aufgrund der Benutzerkontoberechtigungen zulässig sind.

Tipp

Dieses Widget kann nur Daten von einem einzigen Deep Security-Server anzeigen. Erstellen Sie ein neues Widget für jeden Server, um mehrere Deep Security-Server zu überwachen.

Deep Security – Aktivität der Integritätsüberwachung – Widget

Dieses Widget zeigt die fünf häufigsten Integritätsüberwachungsregeln an, die die größte Anzahl Ereignisse ausgelöst haben.

Klicken Sie auf einen Wert in der Spalte **Gesamt**, um das Fenster **Ereignisse** von Deep Security Manager anzuzeigen, das so gefiltert ist, dass von der spezifischen Regel ausgelöste Integritätsüberwachungsereignisse angezeigt werden.

Ändern Sie den verwalteten Server, den das Widget als Quelle verwendet, indem Sie auf das Einstellungssymbol klicken (>). Wählen Sie auf dem erscheinenden Bildschirm den verwalteten Server aus, der als Quelle verwendet werden soll, und klicken Sie auf **Speichern**.

Hinweis

Die im Widget angezeigten Daten sind auf die Daten beschränkt, die aufgrund der Benutzerkontoberechtigungen zulässig sind.

Daten	Beschreibung
Grund	Name der Regel
Gesamt	Die Anzahl der Ereignisse im Zeitraum und der Prozentsatz der gesamten Ereignisse, die dieser Typ darstellt
Vorherige Gesamtanzahl	Die Anzahl der Ereignisse im Zeitraum, der dem aktuellen Zeitraum vorangeht
Trend	Die Änderung in Prozent vom vorherigen zum aktuellen Zeitraum

Deep Security – Ereignisverlauf der Integritätsüberwachung – Widget

Dieses Widget zeigt den Schweregrad der Ereignisse an, die durch Suchläufe der Integritätsüberwachung für den angegebenen Zeitraum protokolliert wurden.

Verwenden Sie die Dropdown-Liste **Bereich**, um den Zeitraum für die angezeigten Daten auszuwählen.

Ändern Sie den verwalteten Server, den das Widget als Quelle verwendet, indem Sie auf das Einstellungssymbol klicken (>). Wählen Sie auf dem erscheinenden Bildschirm den verwalteten Server aus, der als Quelle verwendet werden soll, und klicken Sie auf **Speichern**.

Hinweis

Die im Widget angezeigten Daten sind auf die Daten beschränkt, die aufgrund der Benutzerkontoberechtigungen zulässig sind.

Tipp

Dieses Widget kann nur Daten von einem einzigen Deep Security-Server anzeigen. Erstellen Sie ein neues Widget für jeden Server, um mehrere Deep Security-Server zu überwachen.

Deep Security – Ereignisverlauf des Eindringschutzes – Widget

Dieses Widget zeigt die Anzahl der Ereignisse des Eindringschutzes an, die von Deep Security im angegebenen Zeitraum erkannt wurden. Das Diagramm zeigt die von IPS-Regeln ausgelösten Ereignisse im Erkennungs- und im Verhinderungsmodus an.

Klicken Sie auf einen Balken, um die Seite **Ereignisse** von Deep Security Manager zu öffnen, die so gefiltert ist, dass die IPS-Ereignisse für den angegebenen Modus und Zeitraum angezeigt werden. Sie können in der Legende auf einen Modus (**Erkennen** oder **Verhindern**) klicken, um die Diagrammansicht zu ändern.

Verwenden Sie die Dropdown-Liste **Bereich**, um den Zeitraum für die angezeigten Daten auszuwählen.

Ändern Sie den verwalteten Server, den das Widget als Quelle verwendet, indem Sie auf das Einstellungssymbol klicken (>). Wählen Sie auf dem erscheinenden Bildschirm den verwalteten Server aus, der als Quelle verwendet werden soll, und klicken Sie auf **Speichern**.

Hinweis

Die im Widget angezeigten Daten sind auf die Daten beschränkt, die aufgrund der Benutzerkontoberechtigungen zulässig sind.

Tipp

Dieses Widget kann nur Daten von einem einzigen Deep Security-Server anzeigen. Erstellen Sie ein neues Widget für jeden Server, um mehrere Deep Security-Server zu überwachen.

Deep Security – (erkannte) IPS-Aktivität – Widget

Dieses Widget zeigt die fünf häufigsten IPS-Regeln an, die die größte Anzahl von Ereignissen ausgelöst haben und im Erkennungsmodus verwendet werden.

Klicken Sie auf einen Wert in der Spalte **Gesamt**, um das Fenster **Ereignisse** von Deep Security Manager anzuzeigen, das so gefiltert ist, dass die von der spezifischen Regel ausgelösten (erkannten) IPS-Ereignisse angezeigt werden.

Ändern Sie den verwalteten Server, den das Widget als Quelle verwendet, indem Sie auf das Einstellungssymbol klicken (>). Wählen Sie auf dem erscheinenden Bildschirm den verwalteten Server aus, der als Quelle verwendet werden soll, und klicken Sie auf **Speichern**.

Hinweis

Die im Widget angezeigten Daten sind auf die Daten beschränkt, die aufgrund der Benutzerkontoberechtigungen zulässig sind.

Daten	Beschreibung
Grund	Name der Regel
Gesamt	Die Anzahl der Ereignisse im Zeitraum und der Prozentsatz der gesamten Ereignisse, die dieser Typ darstellt
Vorherige Gesamtanzahl	Die Anzahl der Ereignisse im Zeitraum, der dem aktuellen Zeitraum vorangeht
Trend	Die Änderung in Prozent vom vorherigen zum aktuellen Zeitraum

Deep Security – (verhinderte) IPS-Aktivität – Widget

Dieses Widget zeigt die fünf häufigsten IPS-Regeln an, die die größte Anzahl von Ereignissen ausgelöst haben und im Verhinderungsmodus verwendet werden.

Klicken Sie auf einen Wert in der Spalte **Gesamt**, um das Fenster **Ereignisse** von Deep Security Manager anzuzeigen, das so gefiltert ist, dass die von der spezifischen Regel ausgelösten (verhinderten) IPS-Ereignisse angezeigt werden.

Ändern Sie den verwalteten Server, den das Widget als Quelle verwendet, indem Sie auf das Einstellungssymbol klicken (>). Wählen Sie auf dem erscheinenden Bildschirm den verwalteten Server aus, der als Quelle verwendet werden soll, und klicken Sie auf **Speichern**.

Hinweis

Die im Widget angezeigten Daten sind auf die Daten beschränkt, die aufgrund der Benutzerkontoberechtigungen zulässig sind.

Daten	Beschreibung
Grund	Name der Regel
Gesamt	Die Anzahl der Ereignisse im Zeitraum und der Prozentsatz der gesamten Ereignisse, die dieser Typ darstellt
Vorherige Gesamtanzahl	Die Anzahl der Ereignisse im Zeitraum, der dem aktuellen Zeitraum vorangeht
Trend	Die Änderung in Prozent vom vorherigen zum aktuellen Zeitraum

Deep Security – Protokollinspektionsaktivität – Widget

Dieses Widget zeigt die fünf häufigsten Protokollinspektionsregeln an, die die größte Anzahl von Ereignissen ausgelöst haben.

Klicken Sie auf einen Wert in der Spalte **Gesamt**, um das Fenster **Ereignisse** von Deep Security Manager anzuzeigen, das so gefiltert ist, dass die von der spezifischen Regel ausgelösten Protokollinspektionsereignisse angezeigt werden.

Ändern Sie den verwalteten Server, den das Widget als Quelle verwendet, indem Sie auf das Einstellungssymbol klicken (>). Wählen Sie auf dem erscheinenden Bildschirm den verwalteten Server aus, der als Quelle verwendet werden soll, und klicken Sie auf **Speichern**.

Hinweis

Die im Widget angezeigten Daten sind auf die Daten beschränkt, die aufgrund der Benutzerkontoberechtigungen zulässig sind.

Daten	Beschreibung
Grund	Name der Regel
Gesamt	Die Anzahl der Ereignisse im Zeitraum und der Prozentsatz der gesamten Ereignisse, die dieser Typ darstellt
Vorherige Gesamtanzahl	Die Anzahl der Ereignisse im Zeitraum, der dem aktuellen Zeitraum vorangeht
Trend	Die Änderung in Prozent vom vorherigen zum aktuellen Zeitraum

Deep Security – Ereignisverlauf der Protokollinspektion – Widget

Dieses Widget zeigt die Anzahl der von Regeln der Protokollinspektion ausgelösten Ereignisse an, die im angegebenen Zeitraum aufgetreten sind.

Klicken Sie auf einen Balken ('Erkennen' oder 'Verhindern'), um die Seite **Ereignisse** von Deep Security Manager zu öffnen, die so gefiltert ist, dass Ereignisse der Protokollinspektion für den angegebenen Ereignistyp und Zeitraum angezeigt werden. Sie können auch auf die Ereignistypen in der Legende klicken, um die Diagrammansicht zu ändern.

Verwenden Sie die Dropdown-Liste **Bereich**, um den Zeitraum für die angezeigten Daten auszuwählen.

Ändern Sie den verwalteten Server, den das Widget als Quelle verwendet, indem Sie auf das Einstellungssymbol klicken (>). Wählen Sie auf dem erscheinenden Bildschirm den verwalteten Server aus, der als Quelle verwendet werden soll, und klicken Sie auf **Speichern**.

Hinweis

Die im Widget angezeigten Daten sind auf die Daten beschränkt, die aufgrund der Benutzerkontoberechtigungen zulässig sind.

Tipp

Dieses Widget kann nur Daten von einem einzigen Deep Security-Server anzeigen. Erstellen Sie ein neues Widget für jeden Server, um mehrere Deep Security-Server zu überwachen.

Deep Security – Ereignisverlauf der Aufklärungssuche – Widget

Dieses Widget zeigt die Anzahl der von den Erkennungseinstellungen der Aufklärungssuche angezeigten Ereignisse an, die im angegebenen Zeitraum stattgefunden haben.

Klicken Sie auf einen Balken, um die Seite **Ereignisse** von Deep Security Manager zu öffnen, die so gefiltert ist, dass die Funde der Aufklärungssuche für den angegebenen Ereignistyp und Zeitraum angezeigt werden. Sie können auch auf die Ereignistypen in der Legende klicken, um die Diagrammansicht zu ändern.

Verwenden Sie die Dropdown-Liste **Bereich**, um den Zeitraum für die angezeigten Daten auszuwählen.

Ändern Sie den verwalteten Server, den das Widget als Quelle verwendet, indem Sie auf das Einstellungssymbol klicken (>). Wählen Sie auf dem erscheinenden Bildschirm den verwalteten Server aus, der als Quelle verwendet werden soll, und klicken Sie auf **Speichern**.

Hinweis

Die im Widget angezeigten Daten sind auf die Daten beschränkt, die aufgrund der Benutzerkontoberechtigungen zulässig sind.

Tipp

Dieses Widget kann nur Daten von einem einzigen Deep Security-Server anzeigen. Erstellen Sie ein neues Widget für jeden Server, um mehrere Deep Security-Server zu überwachen.

Deep Security – Statusüberblick – Widget

Dieses Widget zeigt die Anzahl der kritischen Benachrichtigungen und der Warnungsbenachrichtigungen sowie den Status der Endpunkte im gesamten Netzwerk an.

Das Widget zeigt aggregierte Informationen von mehreren verwalteten Servern an.

Ändern Sie den verwalteten Server, den das Widget als Quelle verwendet, indem Sie auf das Einstellungssymbol klicken (>). Wählen Sie auf dem erscheinenden Bildschirm den verwalteten Server aus, der als Quelle verwendet werden soll, und klicken Sie auf **Speichern**.

Tipp

Zum Anzeigen von nicht aggregierten Daten von mehreren verwalteten Servern fügen Sie ein neues Widget für jeden verwalteten Server hinzu.

Hinweis

Die im Widget angezeigten Daten sind auf die Daten beschränkt, die aufgrund der Benutzerkontoberechtigungen zulässig sind.

TABELLE 24-1. Warnungen

DATEN	BESCHREIBUNG
Kritische Warnungen	Die Anzahl der kritischen Warnungen **Hinweis** Ob eine Warnung als 'Kritisch' oder 'Achtung' eingestuft wird, kann vom Benutzer in der Webkonsole von Deep Security Manager festgelegt werden.
Warnungsbenachrichtigungen	Die Anzahl der Warnungsbenachrichtigungen **Hinweis** Ob eine Warnung als 'Kritisch' oder 'Achtung' eingestuft wird, kann vom Benutzer in der Webkonsole von Deep Security Manager festgelegt werden.

TABELLE 24-2. Computerstatus

DATEN	BESCHREIBUNG
Verwaltet (Grün)	Geschützt und ohne Fehler oder Warnungen.
Nicht verwaltet (Blau)	Nicht geschützt.
Gesperrt (Grau)	Gesperrt. Wenn sich ein Computer im gesperrten Zustand befindet, kommuniziert Deep Security Manager nicht mit dem Agent bzw. der Appliance und generiert keine computerbezogenen Warnungen.
Kritisch (Rot)	Im Fehlerzustand.
Warnung (Gelb)	Im Warnungszustand.

Deep Security – Web-Reputation-Ereignisverlauf – Widget

Dieses Widget zeigt die Anzahl der im angegebenen Zeitraum von Web-Reputation-Diensten ausgelösten Ereignisse an.

Verwenden Sie die Dropdown-Liste **Bereich**, um den Zeitraum für die angezeigten Daten auszuwählen.

Ändern Sie den verwalteten Server, den das Widget als Quelle verwendet, indem Sie auf das Einstellungssymbol klicken (>). Wählen Sie auf dem erscheinenden Bildschirm den verwalteten Server aus, der als Quelle verwendet werden soll, und klicken Sie auf **Speichern**.

Hinweis

Die im Widget angezeigten Daten sind auf die Daten beschränkt, die aufgrund der Benutzerkontoberechtigungen zulässig sind.

Daten	Beschreibung
Gefährlich	Bekanntermaßen betrügerische URL oder Bedrohungsquellen
Äußerst verdächtig	Die URL steht im Verdacht, betrügerisch oder möglicherweise eine Bedrohungsquelle zu sein.
Verdächtig	Die URL wird mit Spam in Verbindung gebracht oder ist möglicherweise infiziert.
Gesperrt	Die URL wurde von einem Administrator gesperrt.
Nicht getestet	Die URL wurde von Trend Micro noch nicht getestet. Obwohl Trend Micro Websites aktiv auf deren Sicherheit testet, ist es möglich, dass Benutzer auf ungetestete Websites treffen, wenn diese neu sind oder seltener besucht werden.

Deep Security – Aktivität der Web-Reputation-URLs – Widget

Dieses Widget zeigt die fünf häufigsten URLs von Web-Reputation-Diensten an, für die die größte Anzahl von Ereignissen vorliegt.

Ändern Sie den verwalteten Server, den das Widget als Quelle verwendet, indem Sie auf das Einstellungssymbol klicken (>). Wählen Sie auf dem erscheinenden Bildschirm den verwalteten Server aus, der als Quelle verwendet werden soll, und klicken Sie auf **Speichern**.

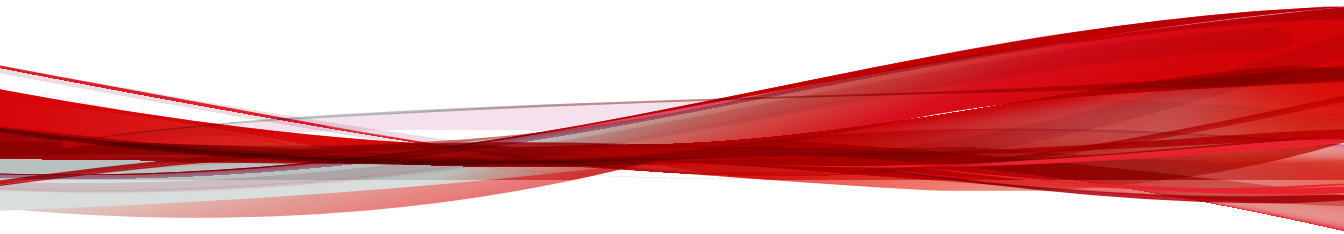
Hinweis

Die im Widget angezeigten Daten sind auf die Daten beschränkt, die aufgrund der Benutzerkontoberechtigungen zulässig sind.

Daten	Beschreibung
URL	Die URL
Gesamt	Die Anzahl der Ereignisse im Zeitraum und der Prozentsatz der gesamten Ereignisse, die dieser Typ darstellt
Vorherige Gesamtanzahl	Die Anzahl der Ereignisse im Zeitraum, der dem aktuellen Zeitraum vorangeht
Trend	Änderung in Prozent vom vorherigen zum aktuellen Zeitraum

Teil X

Endpoint Application Control – Widgets und Richtlinien



Kapitel 25

Endpoint Application Control-Dashboard – Widgets

Dieser Abschnitt enthält Hilfethemen für alle Endpoint Application Control-Dashboard-Widgets, die in Trend Micro Apex Central unterstützt werden.

Es werden folgende Themen behandelt:

Endpoint Application Control – Wichtigste Leistungsindikatoren – Widget

Dieses Widget zeigt anhand ausgewählter Kriterien die wichtigsten Leistungsindikatoren für Endpoint Application Control an. Es enthält anpassbare Vorlagen für erstmalig erkannte Anwendungen und für Anwendungen, die nicht in der Certified Safe Software-Liste enthalten sind, durchschnittlich beendete Agents, durchschnittlich nicht verbundene Endpunkte, Sperr- und Lockdown-Regeln.

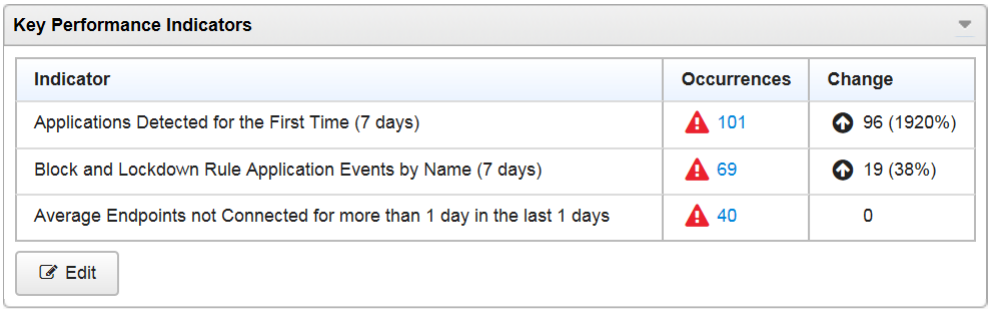


ABBILDUNG 25-1. KPI-Widget – Beispiel

Standardmäßig werden Ereignisse von Widgets bei 5 Vorkommen als „Wichtig“ (

) und bei 10 Vorkommen als „Kritisch“ (

) gekennzeichnet. Markieren Sie Ereignisse als 'Wichtig' oder 'Kritisch', indem Sie Ereignisschwellenwerte anpassen.

Weitere Informationen finden Sie in der Tabelle *Indikatoraufgaben hinzufügen oder bearbeiten*.

Gehen Sie zu **Dashboard** und wählen Sie dann **Widget-Einstellungen** im Menü im oberen rechten Bereich des Widgets, um die folgenden Tasks durchzuführen:

TABELLE 25-1. Konfigurationsaufgaben für KPI-Widgets

AUFGABE	SCHRITTE
Von diesem Widget verwendete Indikatortrendberechnung bearbeiten.	Das Widget zeigt Trends in der Spalte **Ändern** an. Das Widget berechnet Indikatortrends, indem der aktuelle Zeitraum mit einem Durchschnitt der vorherigen Zeiträume verglichen wird. Geben Sie unter **Trendberechnungen** die Anzahl der vorherigen Zeiträume für den Durchschnitt ein. Die Standardeinstellung ist **1**.

Navigieren Sie zu **Dashboard**, suchen Sie dieses Widget und klicken Sie dann auf **Bearbeiten**, um die folgenden indikatorbezogenen Aufgaben durchzuführen. Klicken Sie nach Abschluss der Aufgaben auf **Fertig**.

TABELLE 25-2. Indikatoraufgaben für KPI-Widgets

AUFGABE	SCHRITTE
Neuen Indikator hinzufügen	1. Klicken Sie auf **Indikator hinzufügen**. Das Fenster **Indikator hinzufügen** wird angezeigt. 2. Wählen Sie eine Vorlage aus, passen Sie bei Bedarf die Einstellungen an und klicken Sie dann auf **Speichern**. Weitere Informationen finden Sie in der Tabelle *Indikatoraufgaben hinzufügen oder bearbeiten*.
Indikator bearbeiten.	1. Klicken Sie auf den Indikator in der Liste. Das Fenster **Indikator bearbeiten** wird angezeigt. 2. Passen Sie die Einstellungen an und klicken Sie dann auf **Speichern**. Weitere Informationen finden Sie in der Tabelle *Indikatoraufgaben hinzufügen oder bearbeiten*.
Indikator löschen.	Klicken Sie auf links neben dem Indikator und klicken Sie dann auf **Löschen**.

TABELLE 25-3. Indikatoraufgaben hinzufügen oder bearbeiten

AUFGABE	SCHRITTE
Namen für den Indikator festlegen.	Unter **Titel** einen Namen eingeben. **Tipp** Lassen Sie dieses Feld leer, um es Trend Micro Apex Central zu gestatten, basierend auf Ihrer Konfiguration einen Namen für den Indikator festzulegen.
Vorlage auswählen.	Unter **Vorlage** eine Vorlage auswählen. Weitere Informationen finden Sie unter *Info über Vorlagen*.
Zeitraum bearbeiten.	Wählen Sie unter **Zeitraum** einen Zeitraum für die Indikatordaten aus.
Symbole für den Schwellenwert anzeigen.	Wählen Sie **Schwellenwerte aktivieren** aus.
Symbole für den Schwellenwert ausblenden.	Deaktivieren Sie die Option **Schwellenwerte aktivieren**.
Legen Sie den Schwellenwert „Wichtig“ ( ) fest.	Geben Sie unter **Ereignisse als 'Wichtig' markieren** die Mindestanzahl der Ereignisvorkommen ein. Das Symbol wird in der Spalte **Vorfälle** angezeigt, wenn die folgenden Aussagen wahr sind: • Die Anzahl der Ereignisvorkommen, die diesem Indikator entsprechen, ist gleich oder größer als der Schwellenwert. • **Schwellenwerte aktivieren** ist ausgewählt.

Aufgabe	Schritte
Legen Sie den Schwellenwert „Kritisch“ ( ) fest.	Geben Sie unter **Ereignisse als 'Kritisch' markieren** die Mindestanzahl der Ereignisvorkommen ein. Das Symbol wird in der Spalte **Vorfälle** angezeigt, wenn die folgenden Aussagen wahr sind: • Die Anzahl der Ereignisvorkommen, die diesem Indikator entsprechen, ist gleich oder größer als der Schwellenwert. • **Schwellenwerte aktivieren** ist ausgewählt.

Dieses Widget enthält anpassbare Vorlagen für die folgenden Indikatoren:

„Vorlage“	„Protokolltyp“	„Von“ Vorkommen zusammengefasst nach Datenspalte	„Zeitraum“ (Standard)
Erstmalig erkannte Anwendungen	Vertrauenswürdige Anwendungen **Wichtig** Diese Daten entsprechen dem Protokolltyp „Bekannte Anwendungen“.		7 Tage
Nicht in der Certified Safe Software Liste enthaltene Anwendungen	Richtlinienaktionen		7 Tage

„Vorlage“	„Protokolltyp“	„Von“ Vorkommen zusammengefasst nach Datenspalte	„Zeitraum“ (Standard)
Durchschnittliche beendete Agents	Client-Stichproben **Wichtig** Diese Daten stimmen mit der Datenquelle „Benutzer und Endpunkte“ überein.		1 Tag
Durchschnittlich nicht verbundene Endpunkte	Client-Stichproben **Wichtig** Diese Daten stimmen mit der Datenquelle „Benutzer und Endpunkte“ überein.		Mehr als 1 Tag in den letzten 24 Stunden
Anwendungsereignisse für Sperr- und Lockdown-Regeln	Richtlinienaktionen	• Endpunktname • Name (Standard) • Benutzername	7 Tage

„Vorlage“	„Protokolltyp“	„Von“ Vorkommen zusammengefasst nach Datenspalte	„Zeitraum“ (Standard)
Anwendungsereignisse für Sperrregeln	Richtlinienaktionen	• Endpunktname • Name (Standard) • Benutzername	7 Tage
Anwendungsereignisse für Lockdown-Regeln	Richtlinienaktionen	• Endpunktname • Name (Standard) • Benutzername	7 Tage
Erkannte nicht kategorisierte Anwendungen	Richtlinienaktionen		7 Tage

Endpoint Application Control Regelverwaltung

Dieses Widget enthält eine Liste der Regeltypen und -namen in Endpoint Application Control-Regeln.

Zum Hinzufügen neuer Regeln zu Endpoint Application Control klicken Sie auf **Regel hinzufügen**, um spezifische hinzuzufügende Regeltypen auszuwählen.

Regel	Beschreibung
Zulassen	Mit der Regel **Zulassen** können Sie die Rechte zum Zulassen für vertrauenswürdige Anwendungen erweitern.

Regel	Beschreibung
Sperren	Verwenden Sie die Regel **Sperren**, um Anwendungen vor oder nach der Ausführung zu sperren.
Lockdown	Verwenden Sie die Regel **Lockdown**, um alle zurzeit installierten Anwendungen zuzulassen. Daher ist eine umfassende und aktuelle Endpunktbestandsliste erforderlich.

Endpoint Application Control-Benutzer und -Endpunkte – Zusammenfassung – Widget

Dieses Widget zeigt anhand ausgewählter Kriterien eine Verteilungsübersicht der Endpoint Application Control-Benutzer und -Endpunkte. Es enthält anpassbare Vorlagen für Agent-Verbindungen, Agent-Versionen, Endpunkt-Windows-Versionen, Richtlinien, Richtlinienaktualisierungen und Regeln. Ändern Sie die Vorlagen mithilfe von benutzerdefinierten Einstellungen.

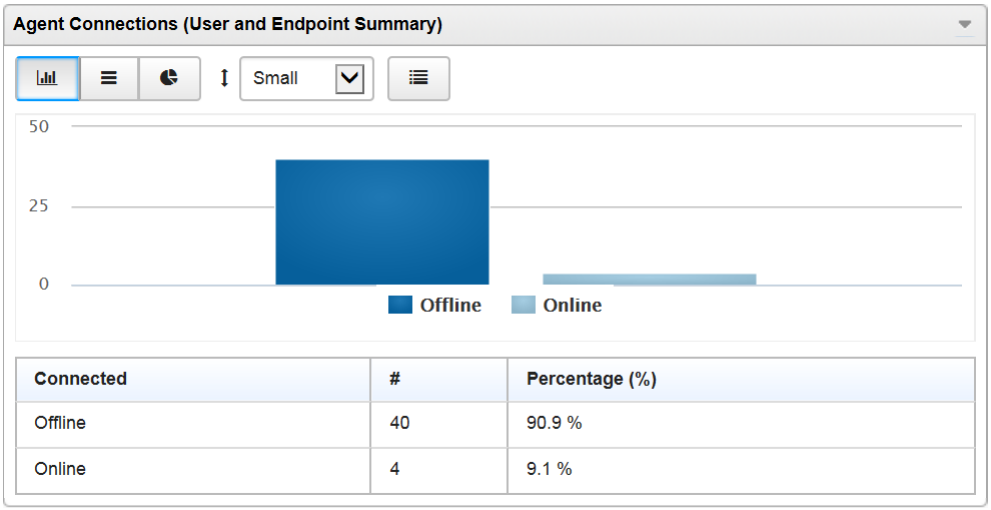
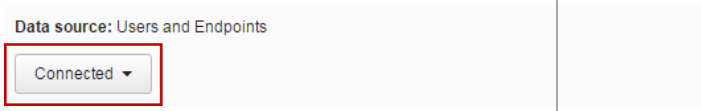


Abbildung 25-2. Widget für Benutzer und Endpunktzusammenfassung – Beispiel

Gehen Sie zu **Dashboard** und wählen Sie dann **Widget-Einstellungen** im Menü im oberen rechten Bereich des Widgets, um die folgenden Tasks durchzuführen:

TABELLE 25-4. Widget für Benutzer und Endpunktzusammenfassung – Konfigurationsaufgaben

AUFGABE	SCHRITTE
Name für das Widget festlegen.	Unter **Titel** einen Namen eingeben. **Tipp** Lassen Sie dieses Feld leer, um es Trend Micro Apex Central zu gestatten, basierend auf Ihrer Konfiguration einen Namen für das Widget festzulegen.
Vorlage auswählen.	Unter **Vorlage** eine Vorlage auswählen.
Datenquelle bearbeiten.	Wählen Sie **Erweitert**. Wählen Sie unter **Datenquelle** eine Datenquelle für die vom Widget angezeigten Daten aus.  **ABBILDUNG 25-3. Datenquelle**
Schränken Sie die angezeigten Ergebnisse ein.	Wählen Sie **Erweitert**. Unter **Ergebnisse auf Folgendes beschränken** dynamische Suche verwenden.

Aufgabe	Schritte
Diagrammtyp ändern.	Wählen Sie unter **Anzeige** einen der folgenden Diagrammtypen aus: • Wählen Sie für ein Liniendiagramm mit Datenpunkten aus. • Wählen Sie für ein horizontales Histogramm aus. • Wählen Sie für ein Tortendiagramm aus. (Standard) • Wählen Sie für eine Datentabelle aus. **Hinweis** Dieses Steuerelement ist nicht verfügbar, wenn (Datentabelle unter Diagramm anzeigen) ausgewählt ist.

Aufgabe	Schritte
Diagrammgröße ändern.	Wählen Sie rechts neben den Diagrammtypen eine der folgenden Diagrammgrößen aus: • Wählen Sie **Klein** für ein Diagramm aus, das ca. 1 Einheit hoch ist. • Wählen Sie **Mittel** für ein Diagramm aus, das ca. 2 Einheiten hoch ist. (Standard) • Wählen Sie **Groß** für ein Diagramm aus, das ca. 4 Einheiten hoch ist. **Abbildung 25-4. Diagrammgröße**
Position der Legende ändern.	Wählen Sie unter **Legende** eine der folgenden Positionen: • **Keine** • **Unten** (Standard) • **Rechts** • **Top** • **Links** **Hinweis** Dieses Steuerelement ist nicht verfügbar, wenn (Daten als Tortendiagramm anzeigen) ausgewählt ist.
Diagrammsteuerelemente im Widget anzeigen.	Aktivieren Sie das Kontrollkästchen **Symbolleiste**. (Standard)
Diagrammsteuerelemente im Widget ausblenden.	Deaktivieren Sie das Kontrollkästchen **Symbolleiste**.

Aufgabe	Schritte
Datenübersichtstabelle unter Diagramm anzeigen.	Wählen Sie **Datenübersichtstabelle unter Diagramm**.
Datenübersichtstabelle unter Diagramm ausblenden.	**Datenübersichtstabelle unter Diagramm** löschen. (Standardeinstellung)
Speichern Sie die Konfiguration als neue Vorlage.	Unter **Vorlage** wählen Sie + **Aktuelle Einstellungen als Vorlage speichern** aus.
Widget löschen.	Wählen Sie **Widget schließen** im Menü oben rechts im Widget aus. Das Widget und alle Anpassungen, die Sie an den Einstellungen des Widgets vorgenommen haben, werden gelöscht.

Dieses Widget enthält die folgenden anpassbaren Vorlagen:

Hinweis

Es können nicht mehrere Vorlagen gleichzeitig angezeigt werden.

„Vorlage“	„Datenquelle“	Bereich	„Erweitert“ Datenspalte (Standard)
Agent-Verbindungen	Benutzer und Endpunkte	Alle (nicht konfigurierbar durch Benutzer)	Verbunden
Agent-Versionen	Benutzer und Endpunkte	Top 3	Agent-Version
Endpunkt-Windows-Versionen	Benutzer und Endpunkte	Top 3	Windows-Version
Richtlinien	Benutzer und Endpunkte	Top 3	Richtlinie

„Vorlage“	„Datenquelle“	Bereich	„Erweitert“ Datenspalte (Standard)
Richtlinienaktualisierungen	Benutzer und Endpunkte	Alle (nicht konfigurierbar durch Benutzer)	Richtlinienaktualisierungen
Regeln	Benutzer und Endpunkte	Top 3	Regeln

Endpoint Application Control-Anwendungs-, Regel- und Richtlinienereignisse – Widget

Verwenden Sie dieses Widget, um einen Überblick über die Verteilung der Endpoint Application Control-Anwendungsereignisse anhand ausgewählter Kriterien anzuzeigen.

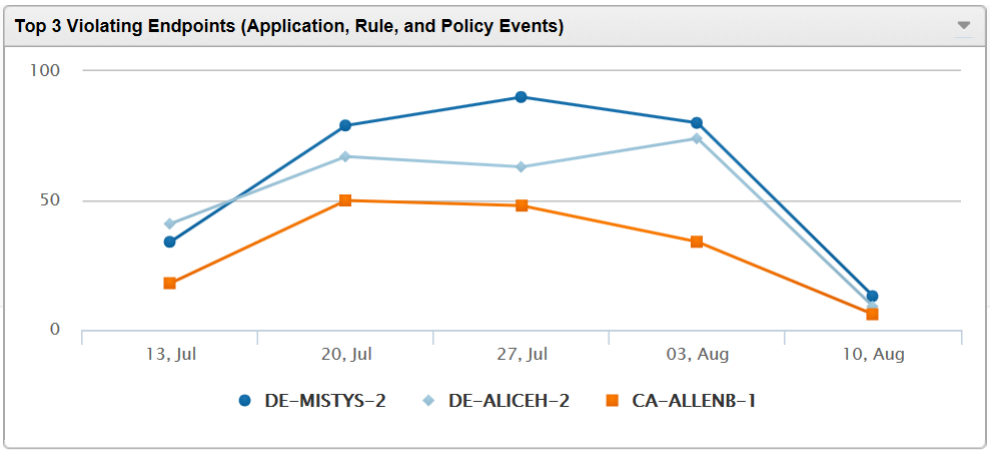
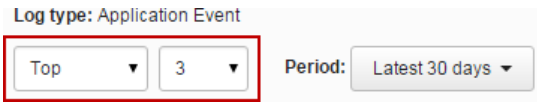
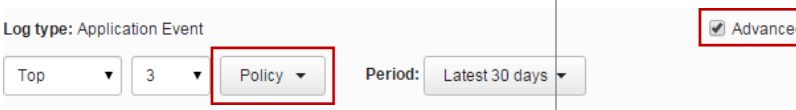


Abbildung 25-5. Widget für Anwendungs-, Regel- und Richtlinienereignisse – Beispiel

Gehen Sie zu **Dashboard** und wählen Sie dann **Widget-Einstellungen** im Menü im oberen rechten Bereich des Widgets, um die folgenden Tasks durchzuführen:

TABELLE 25-5. Konfigurationsaufgaben für das Widget für Anwendungs-, Regel- und Richtlinienereignisse

AUFGABE	SCHRITTE
Name für das Widget festlegen.	Unter **Titel** einen Namen eingeben. **Tipp** Lassen Sie dieses Feld leer, um es Trend Micro Apex Central zu gestatten, basierend auf Ihrer Konfiguration einen Namen für das Widget festzulegen.
Vorlage auswählen.	Unter **Vorlage** eine Vorlage auswählen. Weitere Informationen finden Sie unter **Info über Vorlagen**.
Bearbeiten Sie den Datenbereich.	Unter **Protokolltyp** wählen Sie einen Bereich für die durch das Widget angezeigten Daten aus.  **ABBILDUNG 25-6. Datenbereich**
Zeitraum bearbeiten.	Wählen Sie unter **Zeitraum** einen Zeitraum für die Widget-Daten aus.
Datenquelle bearbeiten.	1. Wählen Sie **Erweitert**. Das Widget zeigt zusätzliche Einstellungen an. 2. Wählen Sie unter **Protokolltyp** eine Datenquelle für die vom Widget angezeigten Daten aus.  **ABBILDUNG 25-7. Datenquelle**

AUFGABE	SCHRITTE
Schränken Sie die angezeigten Ergebnisse ein.	Wählen Sie **Erweitert**. Unter **Ergebnisse auf Folgendes beschränken** dynamische Suche verwenden.
Diagrammtyp ändern.	Wählen Sie unter **Anzeige** einen der folgenden Diagrammtypen aus: • Wählen Sie für ein Liniendiagramm mit Datenpunkten aus. (Standard) • Wählen Sie für ein vertikales Histogramm aus. • Wählen Sie für ein horizontales Histogramm aus. • Wählen Sie für ein Tortendiagramm aus. • Wählen Sie für eine Datentabelle aus. **Hinweis** Dieses Steuerelement ist nicht verfügbar, wenn (Datentabelle unter Diagramm anzeigen) ausgewählt ist.

Aufgabe	Schritte
Diagrammgröße ändern.	Wählen Sie rechts neben den Diagrammtypen eine der folgenden Diagrammgrößen aus: • Wählen Sie **Klein** für ein Diagramm aus, das ca. 1 Einheit hoch ist. • Wählen Sie **Mittel** für ein Diagramm aus, das ca. 2 Einheiten hoch ist. (Standard) • Wählen Sie **Groß** für ein Diagramm aus, das ca. 4 Einheiten hoch ist. **Abbildung 25-8. Diagrammgröße** **Hinweis** Dieses Steuerelement ist nicht verfügbar, wenn (Daten als Tabelle anzeigen) ausgewählt ist.

Aufgabe	Schritte
Position der Legende ändern.	Wählen Sie unter **Legende** eine der folgenden Positionen: • **Keine** • **Unten** (Standard) • **Rechts** • **Top** • **Links** **Hinweis** Dieses Steuerelement ist nicht verfügbar, wenn (Daten als Tortendiagramm anzeigen) oder (Daten als Tabelle anzeigen) ausgewählt ist.
Diagrammsteuerelemente im Widget anzeigen.	Aktivieren Sie das Kontrollkästchen **Symbolleiste**.
Diagrammsteuerelemente im Widget ausblenden.	Deaktivieren Sie das Kontrollkästchen **Symbolleiste**. (Standard)
Datenübersichtstabelle unter Diagramm anzeigen.	Wählen Sie **Datenübersichtstabelle unter Diagramm**.
Datenübersichtstabelle unter Diagramm ausblenden.	**Datenübersichtstabelle unter Diagramm** löschen. (Standardeinstellung)
Speichern Sie die Konfiguration als neue Vorlage.	Unter **Vorlage** wählen Sie **Aktuelle Einstellungen als Vorlage speichern** aus.

Dieses Widget enthält die folgenden anpassbaren Vorlagen:

Hinweis

Es können nicht mehrere Vorlagen gleichzeitig angezeigt werden.

„Vorlage“	„Protokolltyp“	Bereich (Standard)	„Zeitraum“ (Standard)	„Erweitert“ Datenspalte (Standard)	„Erweitert“ Dynamische Suche (Standard)
Anwendungen ohne Regeln	Anwendungsereignis **Wichtig** Diese Daten entsprechen dem Protokolltyp „Richtlinienaktionen“.	Top 3	Letzte 14 Tage	Name	Regel ist leer
Angewendete Richtlinien	Anwendungsereignis **Wichtig** Diese Daten entsprechen dem Protokolltyp „Richtlinienaktionen“.	Top 3	Letzte 14 Tage	Richtlinie	Richtlinie ist nicht leer

„Vorlage“	„Protokolltyp“	Bereich (Standard)	„Zeitraum“ (Standard)	„Erweitert“ Datenspalte (Standard)	„Erweitert“ Dynamische Suche (Standard)
Gesperrte Anwendungen	Anwendungsereignis **Wichtig** Diese Daten entsprechen dem Protokolltyp „Richtlinienaktionen“.	Top 3	Letzte 14 Tage	Name	Durchgeführte Aktion wird gesperrt
Verwendete Anwendungen	Anwendungsereignis **Wichtig** Diese Daten entsprechen dem Protokolltyp „Richtlinienaktionen“.	Top 3	Letzte 14 Tage	Name	Durchgeführte Aktion ist zulässig

„Vorlage“	„Protokolltyp“	Bereich (Standard)	„Zeitraum“ (Standard)	„Erweitert“ Datenspalte (Standard)	„Erweitert“ Dynamische Suche (Standard)
Richtlinienverstöße	Anwendungsereignis **Wichtig** Diese Daten entsprechen dem Protokolltyp „Richtlinienaktionen“.	Top 3	Letzte 14 Tage	Richtlinie	Richtlinie ist nicht leer AND Durchgeführte Aktion wird gesperrt
Regelverstöße	Anwendungsereignis **Wichtig** Diese Daten entsprechen dem Protokolltyp „Richtlinienaktionen“.	Top 3	Letzte 14 Tage	Name	Regel ist nicht leer AND Durchgeführte Aktion wird gesperrt

„Vorlage“	„Protokolltyp“	Bereich (Standard)	„Zeitraum“ (Standard)	„Erweitert“ Datenspalte (Standard)	„Erweitert“ Dynamische Suche (Standard)
Verstöße gegen Endpunkte	Anwendungsereignis **Wichtig** Diese Daten entsprechen dem Protokolltyp „Richtlinienaktionen“.	Top 3	Letzte 14 Tage	Endpunktname	Durchgeführte Aktion wird gesperrt
Verstöße gegen Benutzer	Anwendungsereignis **Wichtig** Diese Daten entsprechen dem Protokolltyp „Richtlinienaktionen“.	Top 3	Letzte 14 Tage	Benutzername	Durchgeführte Aktion wird gesperrt

Kapitel 26

Endpoint Application Control – Richtlinieneinstellungen

Mit den folgenden Endpoint Application Control-Richtlinieneinstellungen können Sie Ihre Endpoint Application Control-Agents über Apex Central verwalten.

Richtlinienregeln

Erweitern Sie **Regeln**, um die folgenden Aufgaben durchzuführen:

Aufgabe	Schritte
Anzeigen einer Liste mit Regeln, die dieser Richtlinie zugewiesen sind.	Der Richtlinie zugewiesene Regeln werden in der Tabelle unterhalb der Schaltfläche **Regel zuweisen** angezeigt. **Tipp** Betriebssystemanwendungen, die von Certified Safe Software als sicher betrachtet werden, sind zugelassen, es sei denn, sie sind durch eine Regel speziell blockiert.
Zuweisen der Regel zu dieser Richtlinie.	Klicken Sie auf **Regel zuweisen**, und führen Sie dann einen der folgenden Schritte aus: • Zur Auswahl vorhandener Regeln, die der Richtlinie zugewiesen werden sollen, wählen Sie **Vorhanden** aus. Das Fenster **Vorhandene Regeln der Richtlinie zuweisen** wird geöffnet. Wählen Sie die zuzuweisenden Regeln aus und klicken Sie dann auf **Regeln zuweisen**.
Entfernen ausgewählter Regeln aus dieser Richtlinie.	Wählen Sie die Regel oder Regeln in der Liste aus, klicken Sie auf **Ausgewählte entfernen** und klicken Sie dann erneut auf **Ausgewählte entfernen**.

In der folgenden Tabelle werden weitere Konfigurationsoptionen erläutert.

Richtlinieneinstellung	Details
Alle Anwendungen im Windows-Verzeichnis stets zulassen (Sperr- und Lockdown-Regeln werden überschrieben)	Standardmäßig lässt Endpoint Application Control alle Anwendungen zu, die sich im Windows-Verzeichnis befinden. Diese Funktion ähnelt einer **Zulassen** für den Windows-Standardpfad, die alle **Sperren** oder **Lockdown** überschreibt.

Richtlinieneinstellung	Details
Lockdown-Regeln automatisch auf Endpunkte anwenden, während sie getrennt sind	Getrennte Endpunkte können neue Richtlinien weder empfangen noch anwenden. In der Regel bedeutet dies, dass ein getrennter Endpunkt weiterhin seine aktuelle Richtlinie anwendet.
Schutz gegen verdächtige Objekte aktivieren (erfordert ein Abonnement für Apex Central)	Endpoint Application Control schützt übereinstimmende Endpunkte vor verdächtigen Objekten.
Kompatiblere, weniger funktionsreiche Sperrmethode auf Benutzerebene verwenden	Durch die Sperrung auf Kernelebene wird durch das Sperren des Dateizugriffs verhindert, dass Anwendungen gestartet werden. Dadurch erhalten Sie mehr Sicherheit, aber möglicherweise wird der Zugriff auf bestimmte Dateien, die von zulässigen Anwendungen benötigt werden, unerwartet gesperrt oder der Zugriff wird zeitweise verzögert. Diese Funktion wird nur von Richtlinien unterstützt, bei denen zuerst das Kriterium 'Benutzer und Gruppen' (ausgenommen das Konto 'SYSTEM') abgeglichen wird. Bei der Sperrung auf Benutzerebene können Anwendungen auf Aufgabenebene gestartet und anschließend wieder angehalten werden. Möglicherweise können mit dieser Funktion bestimmte Anwendungen nicht angehalten werden, nachdem sie gestartet wurden, und die Funktion 'Vertrauenswürdige Quelle' und das Sperren von DLLs und Java-Interpreter-Anwendungen werden nicht unterstützt.

Protokollierung von Richtlinien

Erweitern Sie **Protokollierung**, um die folgenden Richtlinieneinstellungen für übereinstimmende Benutzer und Endpunkte zu konfigurieren:

Richtlinieneinstellung	Details
Folgende Aktionen protokollieren	Wählen Sie eine der folgenden Einschränkungen für die Protokollierung aus: • Wählen Sie **Keine**, um keine Aktionen zu protokollieren. • Wählen Sie **Sperren** aus, um alle gesperrten Anwendungsstarts oder -zugriffe zu protokollieren, die nicht aus einem ausgeschlossenen Verzeichnis stammen. Dies ist die Standardeinstellung für eine neue Richtlinie. • Wählen Sie **Ausgewählt** aus, um alle ausgewählten Anwendungsstarts oder -zugriffe zu protokollieren, die nicht aus einem ausgeschlossenen Verzeichnis stammen. Verwenden Sie die angezeigte Liste, um die entsprechenden Regeln auszuwählen. • Wählen Sie **Beliebig** aus, um alle Anwendungsstarts oder -zugriffe zu protokollieren, die nicht aus einem ausgeschlossenen Verzeichnis stammen. **Hinweis** Bei Auswahl dieser Option können große Protokolldateien erzeugt und Datenübertragungen im Netzwerk drastisch erhöht werden.
Folgende Verzeichnisse von Protokollen ausschließen	Wählen Sie die Option **Folgende Verzeichnisse von Protokollen ausschließen** aus und geben Sie die auszuschließenden Anwendungspfade ein. Trennen Sie die einzelnen Pfade durch einen Wagenrücklauf. Die Standardpfade sind `%SYSTEMROOT%` und `%WINDIR%`.

Richtlinieneinstellung	Details
Aggregierte Protokolle alle sammeln	Wählen Sie den Zeitraum zum Sammeln der Protokolle aus, die von Endpunkten aggregiert wurden. Die Standardeinstellung beträgt **2 Stunden**. Die empfohlene Einstellung richtet sich nach der Anzahl der bereitgestellten Agents.

Richtlinienbereitstellung

Erweitern Sie **Verteilung**, um die folgenden Richtlinieneinstellungen für übereinstimmende Benutzer und Endpunkte zu konfigurieren:

Richtlinieneinstellung	Details
Senden Sie Richtlinienaktualisierungen alle	Wählen Sie das Zeitintervall für die Richtlinienaktualisierung aus. Die Standardeinstellung liegt bei **15 Minuten**. Der vorgeschlagene Zeitraum richtet sich nach der Anzahl der bereitgestellten Agents. Standardmäßig enthalten bereitgestellte Richtlinien lediglich übereinstimmende, bereits in der Bestandsliste eines Endpunkts gefundene Anwendungen, um Datenübertragen im Netzwerk zu verringern und lokale Speicheranforderungen zu minimieren. Nach jedem Richtlinienbereitstellungsintervall enthält Endpoint Application Control alle neu hinzugefügten Anwendungen auf dem Endpunkt, die Regeln in der bereitgestellten Richtlinie entsprechen.

Richtlinieneinstellung	Details
Stellen Sie die vollständige Richtlinie unter den folgenden Bedingungen bereit **Hinweis** Bei Auswahl dieser Optionen werden Datenübertragungen im Netzwerk signifikant erhöht.	Sie können optional die „Vollständige Richtlinie“ bereitstellen, die alle übereinstimmenden Anwendungen enthält und den Bestandslistenabgleich auf dem Endpunkt missachtet. • Wählen Sie **Endpunkt verbindet für weniger als** aus und geben Sie die Anzahl der Stunden pro Woche an, wenn übereinstimmende Endpunkte nicht regelmäßig eine Verbindung zum Server herstellen. • Wählen Sie **Endpunkt beginnt mit der Anwendung von Sperrregeln** aus, wenn übereinstimmenden Endpunkten erlaubt werden soll, alle unter **Zulassen** angegebene Anwendungen nach Anwenden von Lockdown-Regeln zu installieren und auszuführen.

Policy Server-Verbindung

Erweitern Sie **Server-Verbindung**, um die folgenden Richtlinieneinstellungen für übereinstimmende Benutzer und Endpunkte zu konfigurieren:

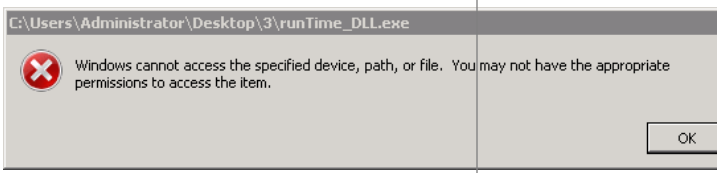
Richtlinieneinstellung	Details
Mit dem folgenden Server verbinden	Ihr Netzwerk enthält unter Umständen mehrere Endpoint Application Control-Server oder ein Server wurde an eine neue IP-Adresse verschoben. Geben Sie den Server an, zu dem der Endpunkt nach Anwendung dieser Richtlinie eine Verbindung herstellen soll. • Wählen Sie **Standard** aus, um den Server zu verwenden, auf dem auch die Webkonsole gehostet wird. Dies ist die Standardeinstellung für eine neue Richtlinie. • Wählen Sie **Spezifiziert** aus und geben Sie dann die Serveradresse und den Port zur Angabe eines Servers ein.

Richtlinieneinstellung	Details
HTTPS verwenden	Endpoint Application Control verwendet standardmäßig die HTTP- oder HTTPS-Konfiguration, die während der Serverinstallation ausgewählt wurde. Wählen Sie **HTTPS verwenden** aus, um alle übereinstimmenden Benutzer oder Endpunkte dauerhaft zur Verwendung von HTTPS festzulegen. **Tipp** Bei Verwendung dieser Option müssen Sie die Server-CA in Agent-Endpunkte importieren. Ausführliche Anweisungen finden Sie unter https://success.trendmicro.com/en-US/solution/KA-0006790

Richtlinien – Benutzererlebnis

Erweitern Sie **Benutzererfahrung**, um die folgenden Richtlinieneinstellungen für übereinstimmende Benutzer und Endpunkte zu konfigurieren:

Richtlinieneinstellung	Details
System-Tray-Symbol anzeigen	Über das Taskleistensymbol ( ) von Endpoint Application Control haben Benutzer die Möglichkeit, Benachrichtigungen anzuzeigen, Zugriff auf Anwendungen anzufordern und Endpoint Application Control-Einstellungen und -Protokolle manuell zu aktualisieren. • Wählen Sie **Ja** aus, um das Symbol in den Windows-Aufgabenleisten der entsprechenden Benutzer anzuzeigen. • Wählen Sie **Nein**, um das Symbol auszublenden.

Richtlinieneinstellung	Details
Benachrichtigungspopups anzeigen	Die Anzeige von Benachrichtigungen kann für bestimmte Benutzer unangebracht sein. Beispiel: Benutzer spezieller Endpunkte, wie z. B. Geldautomaten, medizinische Geräte, Kioske und Tankstellen, können durch Benachrichtigungen und entsprechende Interaktionsanfragen irritiert werden. • Wählen Sie **Ja** aus, um entsprechenden Benutzern Endpoint Application Control-Benachrichtigungen anzuzeigen. • Wählen Sie **Nein** aus, um die Anzeige von Benachrichtigungen zu verhindern und entsprechende Benutzerinteraktionen zu deaktivieren. **Wichtig** Wenn der Start einer Anwendung von Endpoint Application Control mit Hilfe der Methode auf Kernel-Ebene gesperrt oder verzögert wird, wird Windows-Benutzern unter Umständen folgende Benachrichtigung angezeigt:  **Abbildung 26-1. Windows-Sperrbenachrichtigung** Diese Benachrichtigung kann von Endpoint Application Control nicht ausgeblendet werden. Sie können diese Benachrichtigung vermeiden, indem Sie die Sperrung auf Benutzerebene anwenden.

Richtlinieneinstellung	Details
Neues Inventar erstellen	Endpunkte generieren Bestandslisten, um neue und gelöschte Anwendungen nachzuverfolgen. Endpoint Application Control sammelt in regelmäßigen Abständen Anwendungsbestandslisten von Endpunkten. Wählen Sie ein Zeitintervall aus, wie z. B. täglich oder wöchentlich.
Startzeit	Wählen Sie eine Startzeit für die Überprüfung der Bestandsliste aus.

Teil XI

Endpoint Encryption-Widgets und -Richtlinien

Kapitel 27

Endpoint Encryption-Dashboard-Widgets

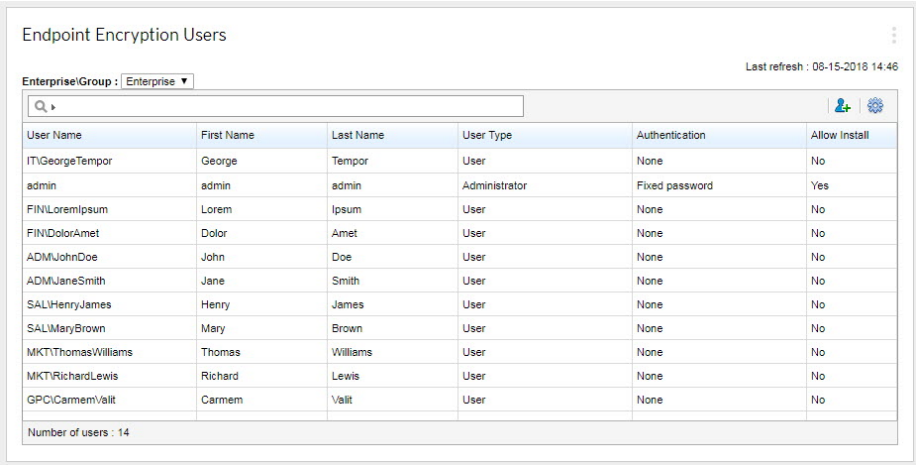
Dieser Abschnitt enthält Hilfethemen für Endpoint Encryption-Widgets, die im Trend Micro Apex Central-Dashboard unterstützt werden.

Es werden folgende Themen behandelt:

- *Endpoint Encryption Benutzer auf Seite 27-2*
- *Endpoint Encryption Geräte auf Seite 27-9*
- *Full Disk Encryption Status auf Seite 27-15*
- *Erfolglose Anmeldeversuche an Endpoint Encryption-Geräten auf Seite 27-18*
- *Erfolglose Anmeldeversuche von Endpoint Encryption-Benutzern auf Seite 27-20*
- *Endpoint Encryption Geräte-Sperre auf Seite 27-22*
- *Bericht über Verstöße gegen die Endpoint Encryption Sicherheit auf Seite 27-24*

Endpoint Encryption Benutzer

Das Widget **Endpoint Encryption Benutzer** bietet direkt im Apex Central-Dashboard Funktionen zur Benutzerverwaltung. Mit dem Widget **Endpoint Encryption Benutzer** können Sie Apex Central-Benutzerkonten hinzufügen oder entfernen, Kennwörter zurücksetzen, Berechtigungen ändern, die Priorität von Richtliniengruppen konfigurieren, den Import aus Active Directory durchführen und nach bestimmten Benutzerkonten suchen.



Vorgang	Beschreibung
Anzeigen	Wählen Sie aus, welche Benutzer angezeigt werden sollen: alle Benutzer im Unternehmen oder Benutzer in einer bestimmten Richtlinie.
Suchen ( )	Klicken Sie auf das Symbol , um zu filtern, welche Apex Central-Benutzer in der Tabelle angezeigt werden. Über das Suchfeld legen Sie Parameter für die Suche fest.
Einstellungen ( ) Anklicken eines Benutzers mit der rechten Maustaste	Klicken Sie auf das Symbol , um Benutzerattribute anzuzeigen oder Aktionen für ausgewählte Benutzer durchzuführen.

Vorgang	Beschreibung
Benutzer hinzufügen ( )	Klicken Sie auf das Symbol , um einzelne Benutzer hinzuzufügen, Benutzer aus einer CSV-Datei zu importieren oder Benutzer aus Active Directory-LDAP zu importieren.
Anzahl der Benutzer	Zeigt die Gesamtzahl der Benutzer im gesamten Unternehmen, in der ausgewählten Richtlinie oder in der angegebenen Suche an.

Benutzereinstellungen - Optionen

In der folgenden Tabelle werden die unter dem Einstellungssymbol verfügbaren Optionen erläutert.

Tabelle 27-1. Benutzereinstellungen - Optionen

Optionen	Beschreibung
Kennwort ändern	Geben Sie ein neues Kennwort für Benutzer an, die die feste Kennwortauthentifizierung verwenden. Das Widget bietet keine Unterstützung zum Ändern von Kennwörtern für den Domänenauthentifizierungstyp.
Benutzer löschen	Entfernt den ausgewählten Benutzer.
Benutzer ändern	Aktualisieren Sie die Eigenschaften des ausgewählten Benutzers. Die folgenden Eigenschaften können geändert werden: • Benutzername • Vorname • Nachname • Mitarbeiter-ID • E-Mail-Adresse • Einfrieren • Benutzertyp • Eine Richtlinie • Authentifizierungsmethode

Optionen	Beschreibung
Richtlinien auflisten	Zeigt die Richtlinien an, die dem ausgewählten Benutzer zugewiesen sind. Ist die Spalte **Installation zulassen** für den ausgewählten Benutzer auf **Ja** gesetzt, ist die Option zum Zulassen oder Verweigern der Installation ausgewählter Richtlinien sowie das Auswählen der Richtlinien mit höchster Priorität aktiviert.

Optionen zum Hinzufügen neuer Benutzer

In der folgenden Tabelle werden die Optionen erläutert, die verfügbar sind, wenn ein neuer Apex Central-Benutzer hinzugefügt wird.

Tabelle 27-2. Optionen zum Hinzufügen neuer Benutzer

Optionen	Beschreibung
Benutzername	Geben Sie den Namen des Benutzerkontos ein, den der Benutzer bei der Authentifizierung verwendet.
Vorname	Geben Sie den Vornamen des Benutzers an.
Nachname	Geben Sie den Nachnamen des Benutzers an.
Mitarbeiter-ID	Geben Sie die Mitarbeiter-ID des Benutzers (optional) an.
E-Mail-Adresse	Geben Sie die E-Mail-Adresse des Benutzers (optional) an.
Einfrieren	Wählen Sie **Ja**, um das Konto vorübergehend zu sperren. Ein gesperrtes Konto kann sich nicht bei Apex Central-Geräten anmelden.
Benutzertyp	Wählen Sie **Benutzer**, **Authentifizierer** oder **Administrator**.
Eine Gruppe	Wenn Sie **Ja** wählen, kann der Benutzer jeweils nur einer Richtlinie angehören. Der Benutzer kann zu keiner anderen Richtliniengruppe hinzugefügt werden. Wenn Sie diese Option auf **Ja** und den **Benutzertyp** auf **Authentifizierer** oder **Administrator** setzen, wird der Benutzer ein Gruppenauthentifizierer bzw. Gruppenadministrator.

Optionen	Beschreibung
Authentifizierungsmethode	Wählen Sie die Authentifizierungsmethode, die für den Benutzer verfügbar ist.

Richtlinienmitgliedschaft

In der folgenden Tabelle wird Grundlegendes zur Richtlinienmitgliedschaft von Apex Central-Benutzern erläutert.

Hinweis

Encryption Management for Apple FileVault und Encryption Management for Microsoft BitLocker erfordern keine Authentifizierung und sind nicht von Authentifizierungsrichtlinien betroffen. Client-, Anmeldung-, Kennwort- und Authentifizierungsrichtlinien oder die Möglichkeit, dass der Benutzer die Security Agent-Software deinstalliert, betreffen nur die Full Disk Encryption- und File Encryption-Agents.

Header	Beispiel	Beschreibung
Priorität	1, 2. 3	Zeigt die Reihenfolge an, in der Apex Central Richtlinien anwendet. Wenn eine Richtlinie ausgelöst wird, die einen Benutzer betrifft, führt Apex Central die Aktion durch. Danach wirken sich keine anderen Richtlinien für dieses Ereignis auf den Benutzer aus.
Name der Richtlinie	GP1	Zeigt den Namen aller Richtlinien an, denen der Benutzer gegenwärtig zugewiesen ist.
Beschreibung	Richtlinie zu temporären Mitarbeitern.	Zeigt die Beschreibung der Richtlinie an.
Installation zulassen	Ja, Nein	Zeigt an, ob der Benutzer neue Geräte installieren kann.

Benutzer aus einer CSV-Datei importieren

Hinweis

Der Import von Benutzern aus einer CSV-Datei wird nur für Benutzer mit fester Kennwortauthentifizierung unterstützt.

Formatieren Sie jede Zeile in der CSV-Datei wie folgt:

```
<Benutzer-ID (erforderlich)>, <Vorname>, <Nachname>,
<Mitarbeiter-ID>, <E-Mail-Adresse>
```

In Feldern ohne Daten verwenden Sie ein Komma als Platzhalter. Im Folgenden ist ein Beispiel-CSV-Eintrag aufgeführt:

```
beispiel_id, name,,, name@beispiel.com
```

Prozedur

1. Klicken Sie im Widget **Endpoint Encryption Benutzer** auf **Benutzer hinzufügen**, und wählen Sie anschließend **Benutzer aus einer CSV-Datei importieren**.

   Das Fenster **Benutzer aus einer CSV-Datei importieren** wird angezeigt.

2. Klicken Sie auf **Datei wählen**, um die CSV-Datei auszuwählen.

   Das Fenster **CSV-Datei öffnen** wird angezeigt.

3. Wählen Sie die Datei, und klicken Sie anschließend auf **Öffnen**.

4. Klicken Sie auf **Hinzufügen**.

   Die Benutzer in der CSV-Datei werden importiert.

Active Directory-Benutzer importieren

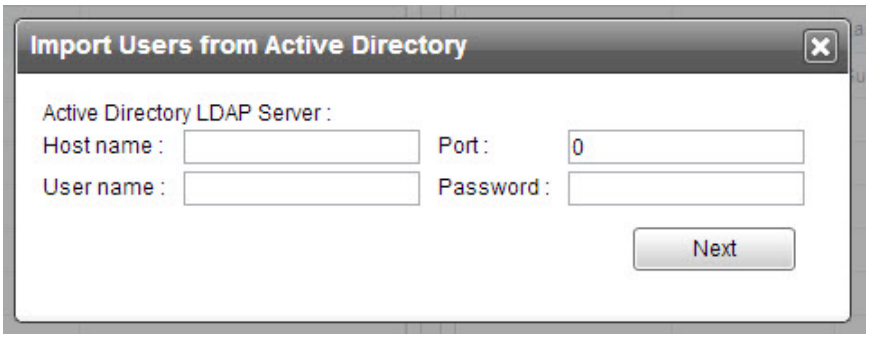
PolicyServer beinhaltet ein Benutzerverzeichnis getrennt von der Active Directory-Datenbank. Dies bietet PolicyServer absolute Sicherheit beim Zugriff auf alle Apex Central-Geräte, Benutzerrechte und Authentifizierungsmethoden.

Mithilfe des Widgets **Endpoint Encryption Benutzer** in Apex Central können Sie Active Directory-Benutzer importieren.

Prozedur

1. Melden Sie sich bei Apex Central an.
2. Navigieren Sie zum Widget **Endpoint Encryption Benutzer**.
3. Klicken Sie auf das -Symbol.
4. Wählen Sie **Benutzer aus Active Directory importieren**.

   Das Fenster **Benutzer aus Active Directory importieren** wird angezeigt.



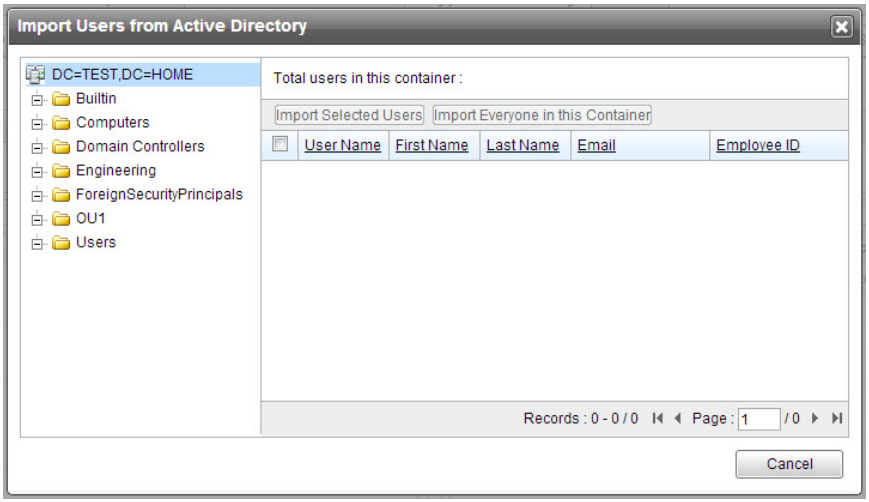
5. Geben Sie Ihre Anmeldedaten für den Active Directory LDAP-Server an.

Hinweis

Bei **Port** gibt der Wert „0“ den Standardport an. Der Standardport ist 389.

6. Klicken Sie auf **Weiter**.
7. Warten Sie, bis die angegebene Active Directory-Domäne mit Daten gefüllt wurde.

Die Active Directory-Struktur für die angegebene Domäne wird im linken Fensterbereich angezeigt.



8. Verwenden Sie im linken Fensterbereich die Navigationsstruktur, um den Container auszuwählen, aus dem Benutzer hinzugefügt werden sollen.

   Die verfügbaren Benutzer werden im rechten Fensterbereich angezeigt.

9. Wählen Sie eine der folgenden Optionen:

   - Wählen Sie einzelne Benutzer, und klicken Sie anschließend auf **Ausgewählte Benutzer importieren**.
   - Klicken Sie auf **Alle Benutzer in diesem Container importieren**.

10. Klicken Sie auf **OK**, um die Benutzer dem angegebenen Speicherort hinzuzufügen.

    Ein Bestätigungsfenster wird angezeigt.

11. Klicken Sie zum Bestätigen auf **OK**.

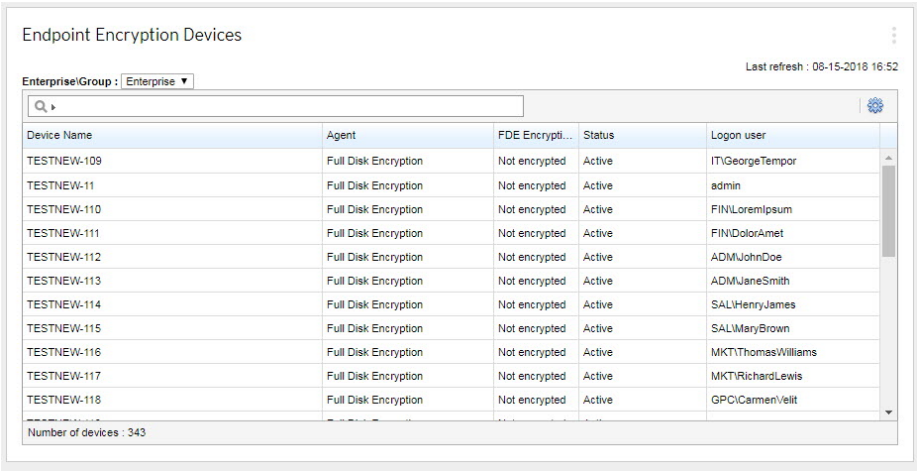
    Eine Importstatusmeldung wird angezeigt.

12. Klicken Sie auf **Schließen**, um den Schritt zu beenden, oder wiederholen Sie das Verfahren, um weitere Benutzer zum Importieren auszuwählen.

Endpoint Encryption Geräte

Endpoint Encryption-Geräte sind Endpoint Encryption-Agents, die bei PolicyServer registriert sind. Bei der Installation eines Endpoint Encryption-Agents wird der Endpunkt automatisch bei PolicyServer als neues Endpoint Encryption-Gerät registriert. Da möglicherweise mehrere Endpoint Encryption-Agents einen bestimmten Endpunkt schützen, wird ein einzelner Endpunkt möglicherweise als mehrere Endpoint Encryption-Geräte bei PolicyServer angezeigt.

Das Widget **Endpoint Encryption Geräte** bietet direkt im Apex Central-Dashboard Funktionen zur Verwaltung von Endpoint Encryption-Geräten. Mit dem Widget **Endpoint Encryption Geräte** können Sie Aktivitäten überwachen, nach Endpoint Encryption-Geräten suchen oder Endpunktdaten schützen, indem Sie lock- oder kill-Befehle ausführen, wenn ein Endpunkt verloren gegangen ist oder gestohlen wurde.



Optionen	Beschreibung
Anzeigen	Wählen Sie aus, welche Geräte angezeigt werden sollen: alle Geräte im Unternehmen oder Geräte in einer bestimmten Richtlinie.
Suchen ( )	Klicken Sie auf das Symbol , um den Security Agent auszuwählen und die in der Tabelle angezeigten Geräte zu filtern. Über das Suchfeld legen Sie Parameter für die Suche fest. Sie können nach allen Attributen suchen, die in den Geräteattributen aufgeführt werden.
Einstellungen ( ) Anklicken eines Geräts mit der rechten Maustaste	Wählen Sie ein Gerät aus und klicken Sie auf das Symbol oder klicken Sie mit der rechten Maustaste auf ein Gerät, um Geräteattribute anzuzeigen oder Aktionen für das ausgewählte Gerät durchzuführen.
Anzahl der Geräte	Zeigt die Gesamtzahl der Geräte im gesamten Unternehmen, in der ausgewählten Richtlinie oder in der angegebenen Suche an.

Geräteaktionen

Wählen Sie ein Gerät und klicken Sie auf das Symbol oder klicken Sie mit der rechten Maustaste auf ein Gerät, um die folgenden Aktionen durchzuführen:

Aktion	Beschreibung
Gerät löschen	Durch das Löschen eines Apex Central-Geräts aus dem Unternehmen wird das Gerät auch aus allen Richtliniengruppen entfernt. Das gelöschte Apex Central-Gerät funktioniert so lange weiter, wie die Verbindung und die Kennwortrichtlinien auf dem Gerät aktuell sind. Der Agent kann seine Richtlinien nicht mit PolicyServer synchronisieren. **Warnung!** Bevor Sie ein Full Disk Encryption Gerät löschen, entschlüsseln Sie Ihre Festplatte und deinstallieren Sie den Full Disk Encryption Agent. Falls Sie ein Full Disk Encryption Gerät löschen, ohne den Agent zu löschen, kann sich der Full Disk Encryption Preboot möglicherweise nicht bei PolicyServer authentifizieren, und die Daten können möglicherweise nicht abgerufen werden.
Soft-Token	Durch das Generieren eines „Software-Token“ wird eine eindeutige Zeichenfolge erstellt, mit der Sie Apex Central-Geräte entsperren können und Apex Central-Benutzer vergessene Kennwörter zurücksetzen können. Das Software-Token ist nur in der Vollversion von Full Disk Encryption verfügbar, nicht in Encryption Management for Apple FileVault oder Encryption Management for Microsoft BitLocker.
Wiederherstellungsschlüssel	Wenn Sie einen „Wiederherstellungsschlüssel“ generieren, können Benutzer eine Festplatte entschlüsseln, wenn der Benutzer das ursprüngliche Kennwort oder den ursprünglichen Schlüssel vergessen hat. Der Wiederherstellungsschlüssel ist nur für die Encryption Management for Apple FileVault und die Encryption Management for Microsoft BitLocker Agents verfügbar, weil diese keine der anderen verfügbaren Wiederherstellungsmethoden in Full Disk Encryption verwenden.
Geräteattribute	Zeigt einen aktuellen Snapshot des ausgewählten Geräts an.

Aktion	Beschreibung
Gerät auslöschen	Mit einem „Beenden“-Befehl werden alle Apex Central-Gerätedaten gelöscht. Die gelöschten Daten sind unterschiedlich, je nach dem Bereich der Daten, den der zugeordnete Security Agent verwaltet. Wenn Sie beispielsweise einen „Beenden“-Befehl auf ein Full Disk Encryption Gerät ausführen, werden alle Daten vom Endpunkt gelöscht. Führen Sie dagegen einen „Beenden“-Befehl auf ein File Encryption Gerät aus, werden alle Dateien und Ordner auf dem lokalen Datenträger und auf den Wechselmedien gelöscht, die vom File Encryption Agent geschützt werden. Der „Beenden“-Befehl wird ausgegeben, wenn der Security Agent mit PolicyServer kommuniziert. **Warnung!** Das Auslöschen eines Geräts kann nicht rückgängig gemacht werden. Sichern Sie alle Daten, bevor Sie einen kill-Befehl ausführen.
Gerät sperren	Durch das Ausführen eines „sperren“-Befehls auf dem Apex Central-Gerät wird der Benutzerzugriff so lange verhindert, bis eine Authentifizierung mittels Remote-Hilfe durchgeführt wurde. Beim Sperren eines Geräts wird der Endpunkt neu gestartet und in einen Status gezwungen, der Remote-Hilfe erfordert. Der lock-Befehl wird ausgegeben, wenn der Security Agent mit PolicyServer kommuniziert.
Warmstart	Wenn Sie einen „Warmstart“-Befehl geben, wird der Endpunkt neu gestartet. Der Befehl wird das nächste Mal ausgeführt, wenn der Agent mit PolicyServer kommuniziert.

Geräteattribute

In der folgenden Tabelle sind die Apex Central-Geräteattribute beschrieben.

Attributname	Beispiel	Beschreibung
AD-NetBIOS-Name	Enterprise	Der dem AD-NetBIOS zugewiesene Name.
AD-Objekt-GUID	6629bdeb-99a8-456b-b7c5-dbbc50ad13d0	Die dem AD-Objekt zugewiesene GUID.
Akkuanzahl	2	Die Anzahl der installierten Akkus.

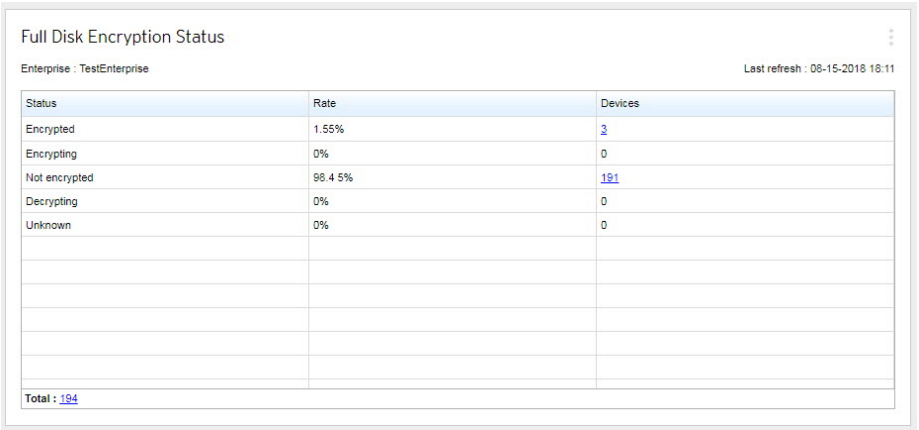
Attributname	Beispiel	Beschreibung
.NET-Version	2.0.50727.3620	Die Versions- und Build-Nummer für das installierte .NET-Framework.
Build-Nummer des Common Framework	5.0.0.84	Der Security Agent verwendet ein übliches Framework für die Verschlüsselung. Die Build-Nummer wird dazu verwendet, um festzustellen, ob der Agent auf dem neuesten Stand ist.
Modell der Festplatte	VMware Virtual IDE	Das Festplattenmodell.
Festplattenname	`\\.\PHYSICALDRIVE0`	Der Name der Festplatte.
Seriennummer der Festplatte		Die Seriennummer der Festplatte.
Festplattenpartitionen	1	Die Anzahl der Partitionen auf der Festplatte, auf der der Agent installiert ist.
Größe der Festplatte	10733990400	Die Gesamtkapazität der Festplatte (in Byte).
Domänenname	WORKGROUP	Die Domäne, zu der der Endpunkt gehört.
Endpunkt-ID	85b1e3e2a3c25d882540ef6e4818c3e4	Die eindeutige ID des Endpunkts, der zur Integration von Apex Central verwendet wird.
Version der File Encryption	6.0.0.1039	Die auf dem Endpunkt installierte Version von File Encryption.
Hostname	TREND-4136D2DB3	Der Host-Name des Endpunkts.
IP-Adresse	`10.1.152.219`	Die IP-Adresse des Endpunkts.
Sprache	Deutsch (Deutschland)	Die vom Endpunkt verwendete Sprache.
Gebietsschema	en-US	Das vom Endpunkt verwendete Gebietsschema.
MAC-Adresse	00-50-56-01-xx-xx	Die MAC-Adresse des Endpunkts.

Attributname	Beispiel	Beschreibung
Computername	TREND-4136D2DB3	Der Computername, den der Endpunkt verwendet.
Hersteller	VMware, Inc.	Der Hersteller der Festplatte.
Modell	Virtuelle VMware-Plattform	Das Modell der Festplatte.
Betriebssystem	Microsoft Windows NT 5.1.2600 Service Pack 3	Das Betriebssystem, das auf derselben Festplatte wie der Agent installiert ist.
Name des Betriebssystems	Microsoft Windows XP Professional	Der allgemeine Name des Betriebssystems, das auf derselben Festplatte wie der Agent installiert ist.
Service Pack des Betriebssystems	Service Pack 3	Die Service Pack-Nummer des Betriebssystems, das auf derselben Festplatte wie der Agent installiert ist.
Version des Betriebssystems	5.1.2600.196608	Die Versionsnummer des Betriebssystems, das auf derselben Festplatte wie der Agent installiert ist.
Partitionsschema	Klassischer MBR	Das Partitionsschema für die Festplatte.
Prozessor	x86 Family 6 Modell 30 Stepping 5, Genuine Intel	Das Prozessorfabrikat und -modell des Endpunkts.
Prozessoranzahl	2	Die Anzahl der Prozessoren im Endpunkt.
Prozessorrevision	1e05	Die Prozessorrevisionsnummer.
Zeitzone	Taipei Standardzeit	Die Zeitzone, in der sich der Endpunkt befindet.
Gesamter physischer Arbeitsspeicher	2.047MB	Der im Endpunkt installierte oder dem Endpunkt zugewiesene Gesamtarbeitsspeicher.
Typ	X86-basierter PC	Der Prozessortyp des Endpunkts.

Attributname	Beispiel	Beschreibung
Windows Benutzername	TREND-4136D2DB3\admin	Der Benutzername des Windows-Kontos, das sich zuletzt am Endpunkt angemeldet hat.
<Agent> Benutzer	john_smith	Der Benutzername des zuletzt angemeldeten Benutzers.
<Agent> Version	5.0.0.260	Die Versions- und die Build-Nummer für die Agent-Installation.

Full Disk Encryption Status

Das **Full Disk Encryption Status**-Widget zeigt den aktuellen Verschlüsselungsstatus jedes Geräts in Ihrem Netzwerk an.



Spalte	Beschreibung
Status	Der Status des Endpunkts. Enthaltene Statusangaben: • **Verschlüsselt**: Der Endpunkt ist zu 100 % verschlüsselt. • **Wird verschlüsselt**: Der Endpunkt ist zurzeit dabei, die Festplatte zu verschlüsseln. Der Status ändert sich in „Vollständig verschlüsselt“, sobald die Verschlüsselung abgeschlossen ist und der Endpunkt neu gestartet wird. • **Nicht verschlüsselt**: Der Endpunkt ist zu 0 % verschlüsselt. • **Wird entschlüsselt**: Der Endpunkt ist zurzeit dabei, die Festplatte zu entschlüsseln. Der Status ändert sich in "Nicht verschlüsselt", sobald die Entschlüsselung abgeschlossen ist und der Endpunkt neu gestartet wird. • **Unbekannt**: Der Endpunkt ist synchronisiert, PolicyServer kann jedoch den Verschlüsselungsstatus nicht ermitteln.
Bewerten	Der Prozentsatz, zu dem der Endpunkt verschlüsselt ist.
Geräte	Die Anzahl der Endpunkte mit diesem aktuellen Status. Klicken Sie auf die Zahl, um den Endpoint Encryption-Gerätebericht anzuzeigen.

Hinweis

Klicken Sie am unteren Rand des Widgets auf die Zahl neben **Gesamt**, um den Verschlüsselungsstatusbericht der vollständigen Festplatte anzuzeigen.

Bericht "Full Disk Encryption Status"

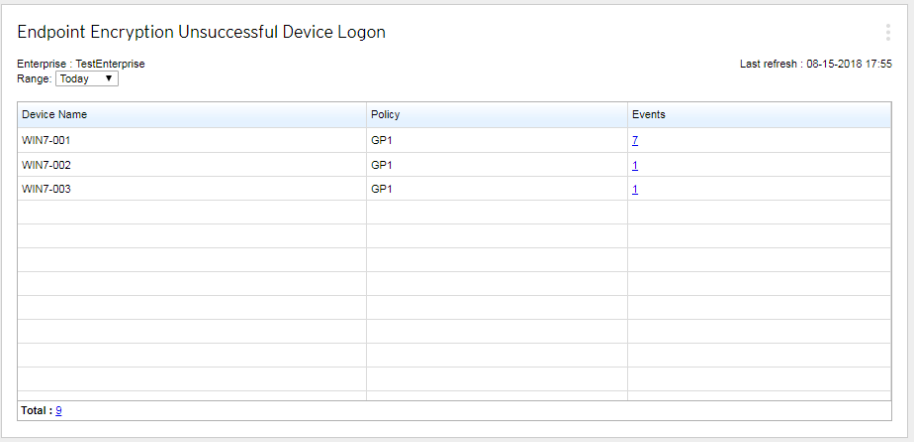
In der folgenden Tabelle wird der Bericht **Full Disk Encryption Status** beschrieben. Die Angaben sollen Ihnen helfen, die Details im Bericht zu verstehen.

TABELLE 27-3. Bericht "Full Disk Encryption Status" – Beispiel

HEADER	BEISPIEL	BESCHREIBUNG
Richtlinie	GP1	Der Titel der Richtlinie zur Steuerung des Endpunkts.
Gerätename	TREND-4136D2DB3	Der vom Endpunkt verwendete Computername.
Geräte-ID	1fabfbff-0001-06e5-000c-2970 85710000	Die eindeutige ID, die eingerichtet wurde, nachdem der Security Agent auf dem Endpunkt installiert wurde und ein neuer Endpunkt bei PolicyServer registriert wurde.
Agent	Vollständige Datenträgerverschlüsselung	Der zurzeit installierte Security Agent.
Status	Nicht verschlüsselt	Der aktuelle Zustand des Endpunkts.
Datum der letzten Synchronisierung	07.10.2013 11:05	Der Zeitstempel, wann der Endpunkt zuletzt Richtlinien über PolicyServer aktualisiert hat.
Letzte Richtliniendurchsetzung	07.10.2013 11:05	Der Zeitstempel, wann der Apex Central zuletzt Richtlinienänderungen auf PolicyServer erzwungen hat.

Erfolglose Anmeldeversuche an Endpoint Encryption-Geräten

Das **Erfolglose Anmeldeversuche an Endpoint Encryption-Geräten**-Widget zeigt alle Geräte (verwaltete Endpunkte), bei denen Benutzer erfolglose Anmeldeversuche unternommen haben. Erfolgslose Geräteanmeldeereignisse können einen Sicherheitsverstoß darstellen oder der Benutzer hat möglicherweise seine Anmeldeinformationen vergessen.



Spalte	Beschreibung
Gerätename	Der Computername des Endpunkts.
Richtlinie	Richtlinie, die den Endpunkt verwaltet.
Ereignisse	Die Anzahl der fehlgeschlagenen Anmeldeversuche. Klicken Sie auf die Nummer, um den Bericht **Erfolglose Anmeldeversuche an Endpoint Encryption-Geräten** anzuzeigen.

Bericht "Erfolglose Anmeldeversuche am Gerät"

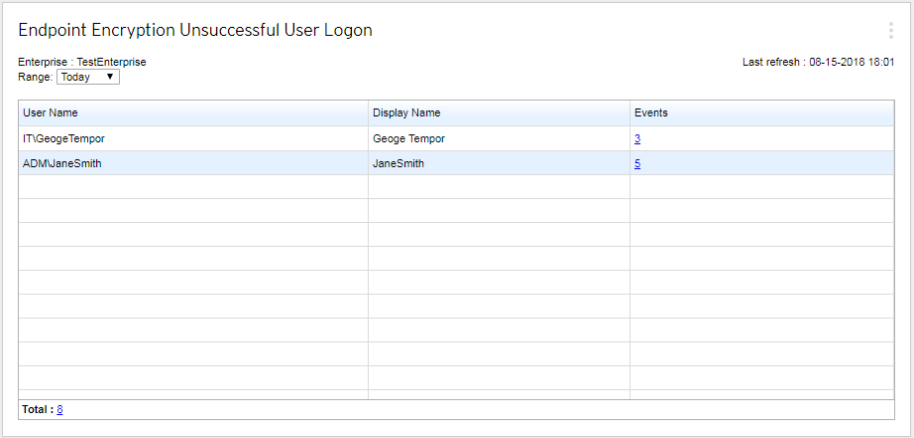
In der folgenden Tabelle wird der Bericht **Erfolglose Anmeldeversuche am Endpoint Encryption Gerät** beschrieben. Die Angaben sollen Ihnen helfen, die Details im Bericht zu verstehen.

TABELLE 27-4. Beispiel für eine erfolglose Anmeldung am Endpoint Encryption-Gerät

HEADER	BEISPIEL	BESCHREIBUNG
Ereigniszeitstempel	02.07.2012 13:56	Wann das Ereignis aufgetreten ist.
Richtlinie	GP1	Der Titel der Richtlinie zur Steuerung des Endpunkts.
Gerätename	TREND-4136D2DB3	Der vom Endpunkt verwendete Computername.
Geräte-ID	1fabfbff-0001-06e5-000c-297085710000	Die eindeutige ID, die eingerichtet wurde, nachdem der Security Agent auf dem Endpunkt installiert wurde und ein neuer Endpunkt bei PolicyServer registriert wurde.
IP-Adresse	`10.1.152.219`	Die IP-Adresse des Endpunkts.
Agent	Vollständige Datenträgerverschlüsselung	Der zurzeit installierte Security Agent.
Benutzername	user325	Der Name des Benutzers, der versucht hat, sich bei dem Endpunkt anzumelden.
Anzeigename	Mary Jones	Der Vor- und Nachname des Apex Central-Benutzerkontos. Wenn der angegebene Benutzername kein gültiger Apex Central-Benutzername ist, enthält die Spalte die Angabe „Nicht aufgezeichnet“.
Ereignis	Erfolglose Anmeldung mit festem Kennwort	Das protokollierte Ereignis, das die Authentifizierungsmethode enthält.

Erfolglose Anmeldeversuche von Endpoint Encryption-Benutzern

Das **Erfolglose Anmeldeversuche von Endpoint Encryption-Benutzern**-Widget zeigt alle fehlgeschlagenen Anmeldeversuche von Benutzern an jedem verwalteten Endpunkt im Apex Central-Netzwerk.



Spalte	Beschreibung
Benutzername	Der Name des Benutzers, der versucht hat, sich bei dem Endpunkt anzumelden.
Anzeigename	Der Anzeigename des Benutzerkontos an, das versucht hat, sich am Endpunkt anzumelden.
Ereignisse	Die Anzahl der Authentifizierungsversuche. Klicken Sie auf die Nummer, um den Bericht **Erfolglose Anmeldeversuche von Endpoint Encryption-Benutzern** anzuzeigen.

Bericht "Erfolglose Anmeldeversuche des Benutzers"

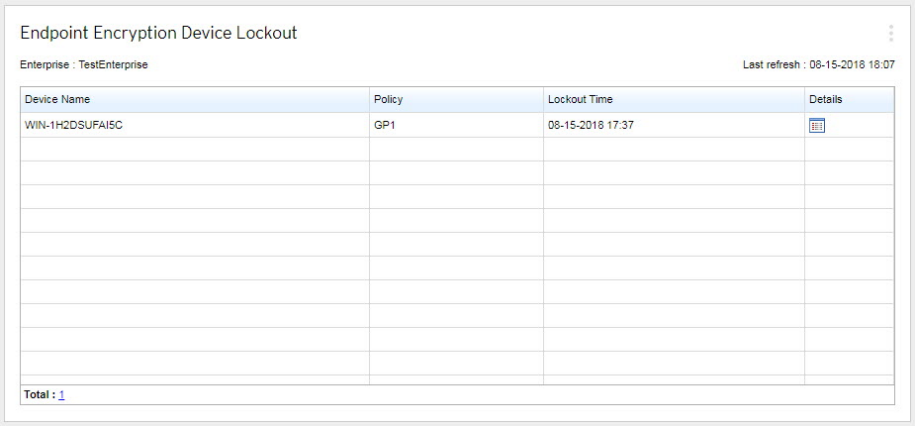
In der folgenden Tabelle wird der Bericht **Erfolglose Anmeldeversuche des Endpoint Encryption Benutzers** beschrieben. Die Angaben sollen Ihnen helfen, die Details im Bericht zu verstehen.

TABELLE 27-5. Beispiel für den Bericht „Erfolglose Anmeldeversuche des Endpoint Encryption-Benutzers“

HEADER	BEISPIEL	BESCHREIBUNG
Ereigniszeitstempel	02.07.2012 13:56	Wann das Ereignis aufgetreten ist.
Richtlinie	GP1	Der Titel der Richtlinie zur Steuerung des Endpunkts.
Gerätename	TREND-4136D2DB3	Der vom Endpunkt verwendete Computername.
Geräte-ID	1fabfbff-0001-06e5-000c-297085710000	Die eindeutige ID, die eingerichtet wurde, nachdem der Security Agent auf dem Endpunkt installiert wurde und ein neuer Endpunkt bei PolicyServer registriert wurde.
IP-Adresse	`10.1.152.219`	Die IP-Adresse des Endpunkts.
Agent	Vollständige Datenträgerverschlüsselung	Der zurzeit installierte Security Agent.
Benutzername	user325	Der Name des Benutzers, der versucht hat, sich bei dem Endpunkt anzumelden.
Anzeigename	Mary Jones	Der Vor- und Nachname des Apex Central-Benutzerkontos. Wenn der angegebene Benutzername kein gültiger Apex Central-Benutzername ist, enthält die Spalte die Angabe „Nicht aufgezeichnet“.
Ereignis	Erfolglose Anmeldung mit festem Kennwort	Das protokollierte Ereignis, das die Authentifizierungsmethode enthält.

Endpoint Encryption Geräte-Sperre

Das **Endpoint Encryption Geräte-Sperre**-Widget zeigt Apex Central-Geräte, die aufgrund von Richtlinieneinschränkungen gesperrt sind.



Header	Beschreibung
Gerätename	Der Computername, der vom Endpunkt verwendet wird.
Richtlinie	Der Titel der Richtlinie zur Steuerung des Endpunkts.
Sperrzeit	Der Zeitpunkt, als PolicyServer den Befehl zum Sperren des Geräts gegeben hat. Der Endpunkt wird erst gesperrt, nachdem der Endpoint Encryption-Agent Richtlinien mit PolicyServer synchronisiert hat.
Details	Klicken Sie auf das Detailsymbol, um den Bericht **Endpoint Encryption Geräte-Sperre** anzuzeigen.

Klicken Sie unten im Widget auf die Zahl neben **Gesamt**, um den Bericht anzuzeigen.

Bericht zur Gerätesperrung

In der folgenden Tabelle wird der Bericht **Endpoint Encryption Gerätesperrung** beschrieben. Die Angaben sollen Ihnen helfen, die Details im Bericht zu verstehen.

Tabelle 27-6. Bericht zur Gerätesperrung für Endpoint Encryption – Beispiel

Header	Beispiel	Beschreibung
Ereigniszeitstempel	02.07.2012 13:56	Wann das Ereignis aufgetreten ist.
Richtlinie	GP1	Der Titel der Richtlinie zur Steuerung des Endpoint Encryption-Geräts.
Gerätename	TREND-4136D2DB3	Der vom Endpoint Encryption-Gerät verwendete Computername.
Geräte-ID	1fabfbff-0001-06e5-000c-297085710000	Die eindeutige ID, die eingerichtet wurde, nachdem der Endpoint Encryption-Agent auf dem Endpunkt installiert wurde und ein neues Endpoint Encryption-Gerät bei PolicyServer registriert wurde.
IP-Adresse	`10.1.152.219`	Die IP-Adresse des Endpoint Encryption-Geräts.
Agent	Vollständige Datenträgerverschlüsselung	Der zurzeit installierte Endpoint Encryption-Agent.
Benutzername	user325	Der Name des Benutzers, der versucht hat, sich bei dem Endpoint Encryption-Gerät anzumelden.

Header	Beispiel	Beschreibung
Anzeigename	Mary Jones	Der Vor- und Nachname des Endpoint Encryption-Benutzerkontos. Wenn der angegebene Benutzername kein gültiger Endpoint Encryption-Benutzername ist, enthält die Spalte die Angabe „Nicht aufgezeichnet“.
Ereignis	Das Gerät wurde aufgrund einer Verletzung durch einen ungültigen Anmeldeversuch gesperrt.	Das protokollierte Ereignis, das die Authentifizierungsmethode enthält.

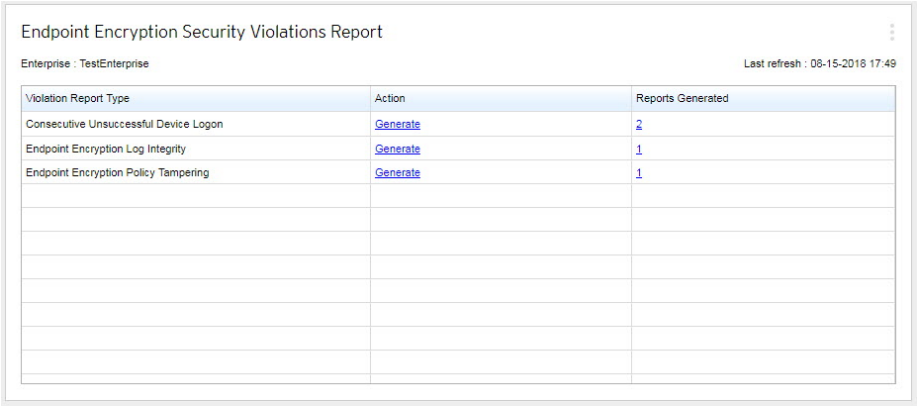
Bericht über Verstöße gegen die Endpoint Encryption Sicherheit

Das Widget **Endpoint Encryption - Bericht zu Sicherheitsverstößen** zeigt die Sicherheitsverstöße aus folgenden Berichten an:

- **Endpoint Encryption - Aufeinanderfolgende erfolglose Anmeldeversuche am Gerät**
- **Endpoint Encryption - Richtlinienmanipulation**
- **Endpoint Encryption - Protokollintegrität**

Beim Generieren eines Berichts werden alle Sicherheitsverstöße erfasst, die momentan von PolicyServer protokolliert wurden. Klicken Sie nach der

Generierung auf die Zahl in der Spalte **Berichte**, um die generierten Berichte für diesen Verstoß anzuzeigen.



Header	Beschreibung
Typ des Berichts zu Verstößen	Die verfügbaren Berichttypen für verschiedene Verstöße.
Aktion	Klicken Sie auf **Generieren**, um einen neuen Bericht zu erstellen.
Berichte	Die Gesamtzahl der generierten Berichte für diesen Verstoß. Klicken Sie auf die Zahl, um die verfügbaren Berichte anzuzeigen.

Hinweis

Zur Angabe der Anzahl erfolgloser Anmeldeversuche, die noch nicht als Sicherheitsverletzung betrachtet werden, klicken Sie auf ▼, um das Fenster **Widget-Einstellungen** zu öffnen, geben einen Wert im Textfeld **Aufeinanderfolgende erfolglose Anmeldungen** ein und klicken dann auf **Speichern**.

Bericht zu aufeinanderfolgenden erfolglosen Anmeldeversuchen am Gerät

In der folgenden Tabelle wird der Bericht **Endpoint Encryption - Aufeinanderfolgende erfolglose Anmeldeversuche am Gerät** beschrieben. Verwenden Sie diese, um zu verstehen, wann der Anmeldeversuch stattgefunden hat, welches Endpoint Encryption-Gerät betroffen ist und wie oft der Benutzer versucht hat, sich bei dem Endpoint Encryption-Gerät anzumelden.

TABELLE 27-7. Endpoint Encryption – Bericht über aufeinanderfolgende fehlgeschlagene Geräteanmeldungen – Beispiel

EINTRAG	BEISPIEL	BESCHREIBUNG
Ereigniszeitstempel	02.07.2012 13:56	Wann das Ereignis aufgetreten ist.
Gerätename	TREND-4136D2DB3	Der vom Endpoint Encryption-Gerät verwendete Computername.
Versuche	5	Wie oft ein Benutzer versucht hat, sich beim Endpoint Encryption-Gerät anzumelden.

Bericht zu Richtlinienmanipulationen

In der folgenden Tabelle wird der Bericht **Endpoint Encryption - Bericht zu Richtlinienmanipulationen** beschrieben. Die Angaben sollen Ihnen helfen, die Details im Bericht zu verstehen.

TABELLE 27-8. Endpoint Encryption – Bericht zu Richtlinienmanipulationen: Beispiel

HEADER	BEISPIEL	BESCHREIBUNG
Ereigniszeitstempel	02.07.2012 13:56	Wann das Ereignis aufgetreten ist.

Header	Beispiel	Beschreibung
Ereignis	Integritätsprüfung des Richtlinienwerts fehlgeschlagen	Das protokollierte Ereignis, das die Authentifizierungsmethode enthält.

Bericht zur Protokollintegrität

In der folgenden Tabelle wird der Bericht **Endpoint Encryption - Bericht zur Protokollintegrität** beschrieben. Die Angaben sollen Ihnen helfen, die Details im Bericht zu verstehen.

Tabelle 27-9. Protokollintegritätsbericht für Endpoint Encryption – Beispiel

Header	Beispiel	Beschreibung
Ereigniszeitstempel	02.07.2012 13:56	Wann das Ereignis aufgetreten ist.
Ereignis	Audit-Protokoll-Datensatz fehlt	Das protokollierte Ereignis, das die Authentifizierungsmethode enthält.

Kapitel 28

Endpoint Encryption-Richtlinieneinstellungen

In diesem Abschnitt wird erläutert, wie Endpoint Encryption-Richtlinien in der Apex Central-Konsole konfiguriert werden.

Es werden folgende Themen behandelt:

Authentifizierungsübersicht

Die primäre Form von Schutz, die Endpoint Encryption bietet, ist die Verhinderung von unbefugtem Benutzerzugriff auf verschlüsselte Endpunkte und Geräte. Durch die ordnungsgemäße Konfiguration von Endpoint Encryption-Geräten, -Benutzern und -Richtliniengruppen wird das Risiko von Datenverlusten durch versehentliche Informationsfreigabe oder zielgerichtete Sabotage verhindert.

Geräte auf Seite 28-2	Endpoint Encryption zählt die Anzahl der aufeinanderfolgenden Anmeldeversuche auf einem bestimmten Gerät und wie viel Zeit seit der letzten Kommunikation mit PolicyServer in einem bestimmten Zeitraum vergangen ist. Wenn ein Gerät gegen die Kriterien der Richtlinie verstößt, kann Endpoint Encryption die Festplatte zurücksetzen, sperren oder löschen.
Benutzer auf Seite 28-3	Zusätzlich zur Überprüfung der Authentifizierungsversuche auf einem Gerät wird von Endpoint Encryption auch die Anzahl der aufeinanderfolgenden Anmeldeversuche durch ein bestimmtes Benutzerkonto gezählt. Wenn der Benutzer gegen die Kriterien der Richtlinie verstößt, kann Endpoint Encryption die Festplatte zurücksetzen, sperren oder löschen.
Gruppen auf Seite 28-5	Gruppen fungieren als Behälter für Benutzer für die Richtlinienverwaltung. Administratoren und Authentifizierer innerhalb einer Gruppe haben jene besonderen Berechtigungen nur innerhalb dieser Gruppe, nicht zugewiesene Administratoren und Authentifizierer haben diese Rolle über das gesamte Unternehmen hinweg inne.

Geräte

Endpoint Encryption-Geräte sind Endpoint Encryption-Agents, die bei PolicyServer registriert sind. Bei der Installation eines Endpoint Encryption-Agents wird der Endpunkt automatisch bei PolicyServer als neues Endpoint Encryption-Gerät registriert. Da möglicherweise mehrere Endpoint Encryption-Agents einen bestimmten Endpunkt schützen, wird ein einzelner Endpunkt möglicherweise als mehrere Endpoint Encryption-Geräte bei PolicyServer angezeigt.

Abhängig von den Richtlinieneinstellungen führt Endpoint Encryption eine der folgenden Aktionen durch, wenn Benutzer mehrere aufeinanderfolgende fehlgeschlagene Anmeldeversuche auf dem Gerät durchführen:

- Den nächsten Authentifizierungsversuch verzögern
- Das Gerät sperren
- Alle Daten auf dem Gerät löschen

Hinweis

Verwenden Sie zum Konfigurieren der Endpoint Encryption-Geräte das Widget **Endpoint Encryption Geräte**. Weitere Informationen finden Sie unter *Endpoint Encryption Geräte auf Seite 27-9*.

Benutzer

Bei Endpoint Encryption-Benutzern handelt es sich um beliebige Benutzerkonten, die manuell zum PolicyServer hinzugefügt oder mit Active Directory synchronisiert wurden.

Endpoint Encryption verfügt über verschiedene Kontorollen und Authentifizierungsmethoden für umfassende identitätsbasierte Authentifizierung und Verwaltung. Mit Hilfe der Endpoint Encryption- oder PolicyServer-MMC können Sie je nach Bedarf Benutzerkonten hinzufügen oder importieren, die Authentifizierung steuern, Synchronisierungen mit Active Directory durchführen und Gruppenmitgliedschaften von Richtlinien verwalten.

In der folgenden Tabelle werden die Endpoint Encryption-Benutzerrollen beschrieben:

Rolle	Beschreibung
Administrator	Administratoren können auf die Management-Konsolen zugreifen und beliebige Konfigurationen innerhalb ihrer Domäne durchführen. Diese Rolle weist je nach Stufe, auf der die Administratorrolle hinzugefügt wird, verschiedene Rechte auf: • Unternehmensadministrator: Diese Administratoren steuern alle Richtlinien, Gruppen, Benutzer und Geräte im Unternehmen. • Gruppenadministrator: Diese Administratoren steuern Benutzer und Geräte, die sich innerhalb einer bestimmten Gruppe authentifizieren. Endpoint Encryption erstellt eine Gruppe für jede Richtlinie, weshalb diese Administratoren auch „Richtlinienadministratoren“ genannt werden.
Authentifizierer	Authentifizierer bieten Remote-Unterstützung, wenn Benutzer ihre Endpoint Encryption-Kennwörter vergessen oder technische Probleme haben. Diese Rolle weist je nach Stufe, auf der die Authentifiziererrolle hinzugefügt wird, verschiedene Rechte auf: • Unternehmensauthentifizierer: Diese Authentifizierer können alle Benutzer im Unternehmen unterstützen. • Gruppenauthentifizierer: Diese Authentifizierer können alle Benutzer innerhalb einer bestimmten Gruppe unterstützen. Endpoint Encryption erstellt eine Gruppe für jede Richtlinie, weshalb diese Authentifizierer auch „Richtlinienauthentifikatoren“ genannt werden.
Benutzer	Einfache Endbenutzer weisen keine besonderen Berechtigungen auf. Mit dieser Benutzerrolle ist eine Anmeldung an den Endpoint Encryption-Management-Konsolen unter Umständen nicht möglich. Die Benutzerrolle darf auch keine Wiederherstellungstools verwenden, es sei denn, der PolicyServer lässt dies zu.

Hinweis

Verwenden Sie zur Konfiguration von Endpoint Encryption-Benutzern das Widget **Endpoint Encryption Benutzer**. Weitere Informationen finden Sie unter *Endpoint Encryption Benutzer auf Seite 27-2*.

Gruppen

Apex Central verwaltet Richtlinien nach Benutzergruppen. Die Gruppenverwaltung ist bei PolicyServer MMC und Apex Central unterschiedlich. Nach dem Ändern von Richtlinien und Gruppen synchronisiert PolicyServer die Gruppen in beiden Konsolen.

Wichtig

Apex Central hat bei der Richtlinien- und Gruppenzuweisung immer Vorrang vor PolicyServer MMC. Alle Änderungen an der Gruppenzuweisung in PolicyServer MMC werden automatisch überschrieben, wenn Apex Central das nächste Mal mit PolicyServer synchronisiert wird.

KONSOLE	GRUPPENVERWALTUNG
Apex Central	Apex Central erstellt automatisch jedes Mal dann eine Gruppe, wenn eine Richtlinie mit bestimmten Zielen verteilt wird. Ändern Sie nach der Verteilung die Gruppen, in denen sich ein Benutzer befindet, über das Widget **Endpoint Encryption Benutzer**. Ändern Sie dann die Benutzer in der Richtlinie im Fenster **Richtlinienverwaltung**.

Konsole	Gruppenverwaltung
PolicyServer MMC	Gruppen können im linken Bereich von PolicyServer MMC direkt hinzugefügt und geändert werden. Gruppen in PolicyServer MMC können wie folgt zugewiesen werden: • **Top-Gruppe**: Top-Gruppen befinden sich auf der höchsten Ebene unter dem Unternehmen. Jede Top-Gruppe hat einen eindeutigen Knoten unterhalb des Unternehmens. • **Untergruppe**: Untergruppen werden innerhalb von Top-Gruppen erstellt. Bei der Erstellung von Untergruppen übernehmen diese die Richtlinien der Top-Gruppe. An der Top-Gruppe vorgenommene Änderungen werden jedoch nicht übernommen. Untergruppen dürfen nicht schwächer einschränkend sein als die Top-Gruppe. **Hinweis** Sie müssen Geräte und Benutzer jeder Untergruppe manuell zuweisen. Durch das Hinzufügen von Apex Central-Benutzern zu einer Untergruppe werden die Benutzer nicht automatisch der Top-Gruppe hinzugefügt. Sie können Benutzer jedoch sowohl der Top-Gruppe als auch der Untergruppe hinzufügen.

Hinweis

Um die Benutzer innerhalb einer Richtliniengruppe in Apex Central zu konfigurieren, verwenden Sie das Widget **Endpoint Encryption Benutzer**.

Informationen zur Konfiguration der Benutzer innerhalb einer Richtliniengruppe auf PolicyServer MMC finden Sie im *Endpoint Encryption PolicyServer MMC Handbuch*.

Endpoint Encryption Benutzerregeln konfigurieren

Im folgenden Verfahren werden die konfigurierbaren Optionen für Richtlinienregeln erläutert, die die Authentifizierung und die Benutzerkonten von Endpoint Encryption betreffen.

Prozedur

1. Erstellen Sie eine neue Endpoint Encryption Richtlinie.
2. Klicken Sie auf **Benutzer**.

   Das Fenster zu den Richtlinienregeleinstellungen **Benutzer** wird angezeigt.

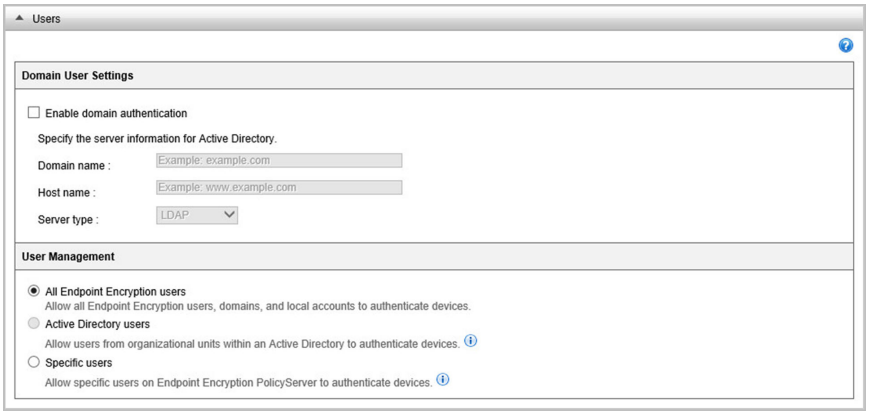


ABBILDUNG 28-1. Endpoint Encryption Benutzer Richtlinienregeln

3. Wenn Benutzer Domänenauthentifizierung benötigen, wählen Sie die Option **Domänenauthentifizierung aktivieren** unter **Domänenbenutzereinstellungen** aus.

   Geben Sie bei Auswahl von **Domänenauthentifizierung aktivieren** die Serverinformationen für Ihr Active Directory (AD)-Konto an.

   a. Konfigurieren Sie den AD-Domänennamen.

   b. Konfigurieren Sie den Host-Namen des AD-Servers.

   c. Wählen Sie den Servertyp aus:

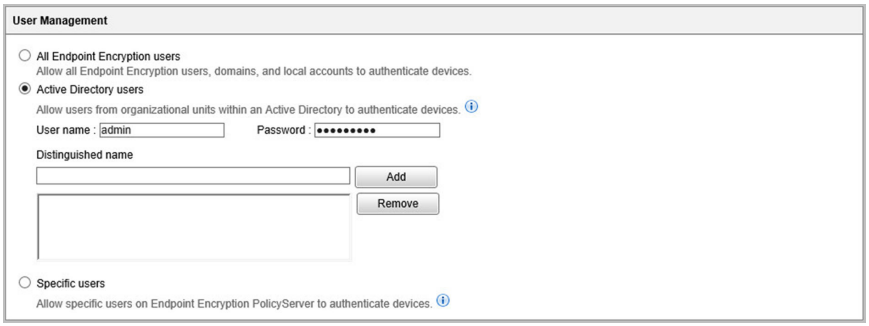
   - **LDAP**
   - **LDAP-Proxy**

4. Konfigurieren Sie unter **Benutzerverwaltung** den Benutzerzugriff.

Option	Bezeichnung
Alle Endpoint Encryption Benutzer	Alle Benutzer, Domänenkonten und lokalen Konten dürfen Geräte authentifizieren.
Active Directory-Benutzer	Alle Benutzer aus Organisationseinheiten (OE) innerhalb eines AD dürfen Geräte authentifizieren. **Hinweis** Wählen Sie **Domänenauthentifizierung aktivieren** aus, um die Option **Active Directory-Benutzer** zu aktivieren.
Bestimmte Benutzer auswählen	Legen Sie fest, welche bereits hinzugefügten Benutzer bei verwalteten Endpunkten authentifiziert werden können. **Hinweis** Um bestimmte Benutzer mit dieser Option auszuwählen, müssen Sie die Benutzerliste auffüllen. Fügen Sie Organisationseinheiten mit der Option **Active Directory-Benutzer** hinzu oder fügen Sie Benutzer mit dem Endpoint Encryption Benutzer-Widget hinzu.

5. Wenn Sie **Active Directory-Benutzer** ausgewählt haben, fügen Sie der Richtlinie Organisationseinheiten nach ihrem eindeutigen Namen hinzu.

   Nach Auswahl von **Active Directory-Benutzer** werden die folgenden zusätzlichen Optionen angezeigt:



Option	Bezeichnung
Benutzername	Geben Sie Ihren Active Directory-Benutzernamen ein.
Kennwort	Geben Sie Ihr Active Directory-Kennwort ein.
Eindeutiger Name	Legen Sie jede Organisationseinheit gemäß der Reihenfolge der relativen eindeutigen Namen getrennt durch Kommas fest. Beispiel: OU=TW, DC=mycompany, DC=com Wenn Sie den eindeutigen Namen für die Organisationseinheit festgelegt haben, klicken Sie auf **OK**. **Wichtig** Apex Central unterstützt bis zu 12 OE pro Richtlinie.

Full Disk Encryption Regeln konfigurieren

Im folgenden Verfahren werden die konfigurierbaren Optionen für Richtlinienregeln erläutert, die Full Disk Encryption-Geräte betreffen.

Hinweis

Encryption Management for Apple FileVault und Encryption Management for Microsoft BitLocker erfordern keine Authentifizierung und sind nicht von Authentifizierungsrichtlinien betroffen. Client-, Anmeldung-, Kennwort- und Authentifizierungsrichtlinien oder die Möglichkeit, dass der Benutzer die Endpoint Encryption Agent-Software deinstalliert, betreffen nur die Full Disk Encryption- und File Encryption-Agents.

Prozedur

1. Erstellen Sie eine neue Endpoint Encryption Richtlinie.
2. Klicken Sie auf **Full Disk Encryption**.

Die Einstellungen für Richtlinien vom Typ **Full Disk Encryption** werden angezeigt.

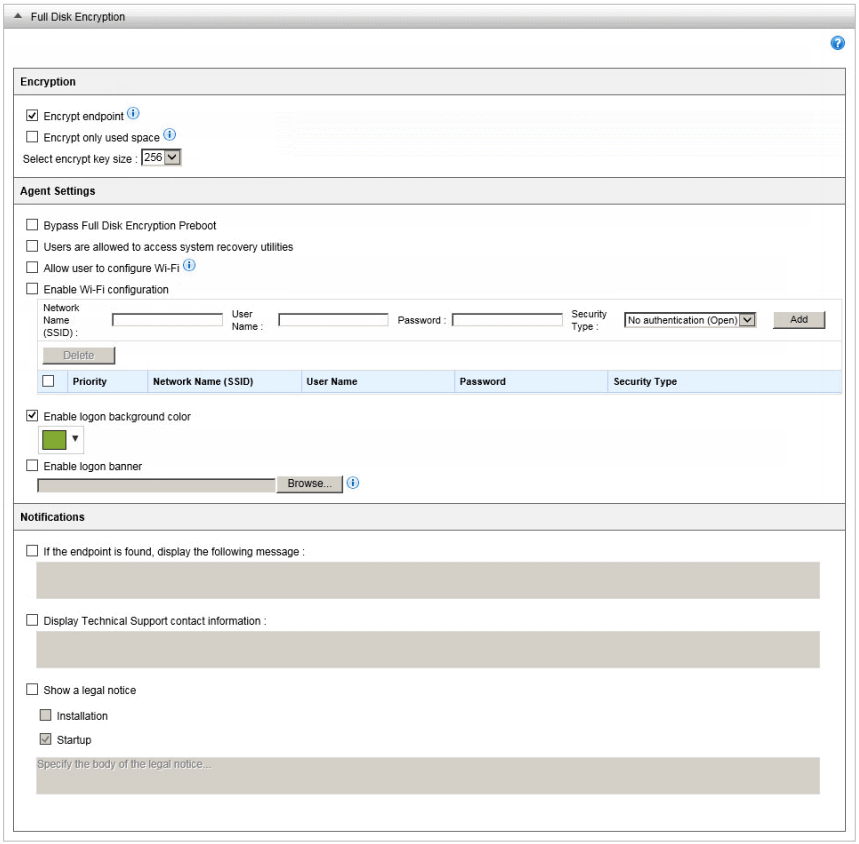


ABBILDUNG 28-2. Full Disk Encryption – Richtlinienregeln

3. Wählen Sie unter **Verschlüsselung** die folgenden Optionen aus:

   - Wählen Sie **Gerät verschlüsseln** aus, um die vollständige Festplattenverschlüsselung zu starten, wenn der Endpoint Encryption-Agent Richtlinien mit PolicyServer synchronisiert.

Warnung!

Verteilen Sie die Verschlüsselung nicht auf Full Disk Encryption-Agents, ohne das Festplattenlaufwerk des Endpunkts zunächst vorzubereiten.

Weitere Informationen zum Vorbereiten des Festplattenlaufwerks finden Sie unter *Überblick über die Full Disk Encryption Verteilung* im *Endpoint Encryption Installationshandbuch*.

- Wählen Sie **Nur verwendeten Speicherplatz verschlüsseln** aus, um nur den verwendeten Speicherplatz zu verschlüsseln.
- Wählen Sie **Größe des Verschlüsselungsschlüssels auswählen** aus, um die Größe des Verschlüsselungsschlüssels eines Geräts in Bit anzugeben.

4. Wählen Sie unter **Agent-Einstellungen** die folgenden Optionen aus:
   - Wählen Sie **Full Disk Encryption Preboot umgehen** aus, um dem Benutzer die direkte Authentifizierung in Windows ohne die Preboot-Authentifizierung zu gestatten.
   - Wählen Sie **Benutzern den Zugriff auf Dienstprogramme für die Systemwiederherstellung auf diesem Gerät gestatten** aus, um Benutzern den Zugriff auf die Wiederherstellungskonsole zu gestatten.
   - Wählen Sie **Konfiguration von WLAN durch Benutzer zulassen** aus, damit Benutzer während des Preboots WLAN-Richtlinien auf dem Gerät konfigurieren können.
   - Wählen Sie **WLAN-Konfiguration aktivieren** aus, um während des Preboots eine vordefinierte WLAN-Konfiguration zu verwenden. Geben Sie die folgenden Informationen an:
     - Netzwerkname (SSID)
     - Benutzername
     - Kennwort

- Sicherheitstyp

- Wählen Sie **Hintergrundfarbe für Anmeldung aktivieren** aus, um die Hintergrundfarbe bei der Anmeldung anzugeben.
- Wählen Sie **Anmeldebanner aktivieren** aus, um ein Anmeldebannerbild anzugeben.

  Das Bild sollte 128 KB nicht überschreiten und 512 x 64 Pixel aufweisen. Akzeptierte Dateiformate sind PNG mit Transparenz (empfohlen), JPG und GIF

5. Konfigurieren Sie unter **Benachrichtigungen** die folgenden Optionen:
   - Wählen Sie **Wenn gefunden, die folgende Meldung auf dem Gerät anzeigen** aus, um eine Meldung anzuzeigen, wenn die Richtlinie **Wenn gefunden** aktiv ist.
   - Wählen Sie **Kontaktinformationen des technischen Supports anzeigen** aus, um eine Meldung anzuzeigen, nachdem sich der Benutzer beim Full Disk Encryption-Agent angemeldet hat.
   - Wählen Sie **Rechtlichen Hinweis anzeigen** aus, um den rechtlichen Hinweis beim Start oder erst nach der Installation des Full Disk Encryption-Agents anzuzeigen.

File Encryption Regeln konfigurieren

Das folgende Verfahren beschreibt die konfigurierbaren Optionen für Richtlinienregeln, die sich auf File Encryption Geräte auswirken.

Prozedur

1. Erstellen Sie eine neue Endpoint Encryption Richtlinie.
2. Klicken Sie auf "File Encryption".

Das Fenster mit den Einstellungen für **File Encryption** Richtlinienregeln wird angezeigt.

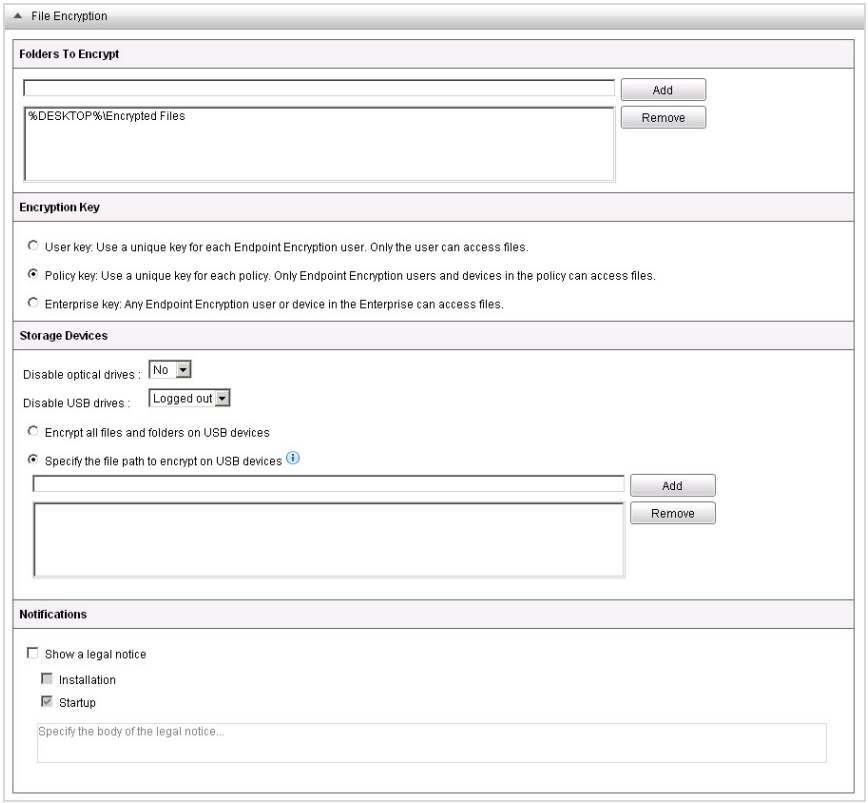


ABBILDUNG 28-3. File Encryption Richtlinienregeln

3. Legen Sie unter **Zu verschlüsselnde Ordner** die Ordner fest, die auf dem Endpunkt automatisch erstellt und verschlüsselt werden, wenn der File Encryption Agent Richtlinien synchronisiert.
4. Wählen Sie unter **Verschlüsselungsschlüssel** die Verschlüsselung für den verschlüsselten File Encryption Ordner.
    - **Benutzerschlüssel**: Verwenden Sie einen eindeutigen Schlüssel für jeden Endpoint Encryption-Benutzer. Nur der Benutzer

von Endpoint Encryption kann Dateien entschlüsseln, die er verschlüsselt hat.

- **Richtlinienschlüssel**: Verwenden Sie einen eindeutigen Schlüssel für jede Richtlinie. Nur Endpoint Encryption-Benutzer und -Geräte in der Richtlinie können Dateien entschlüsseln.
- **Unternehmensschlüssel**: Alle Endpoint Encryption-Benutzer oder -Geräte im Unternehmen können die Dateien entschlüsseln.

Hinweis

Durch die Auswahl von **Richtlinienschlüssel** oder **Unternehmensschlüssel** steuern Sie den Austausch des gemeinsamen Schlüssels für File Encryption.

5. Konfigurieren Sie die folgenden Optionen unter **Speichergeräte**:
   - Wählen Sie **Optisches Laufwerk deaktivieren**, um festzulegen, ob der Zugriff auf Wechselmedien vom Endpunkt aus möglich ist.
   - Wählen Sie **USB-Laufwerk deaktivieren**, um festzulegen, ob USB-Ports deaktiviert sind. Folgende Optionen sind möglich:
     - **Immer**
     - **Abgemeldet**
     - **Nie**
   - Wählen Sie **Alle Dateien und Ordner auf USB-Geräten verschlüsseln**, um automatisch alle Dateien und Ordner auf Wechselmedien zu verschlüsseln, wenn diese mit dem Endpunkt verbunden sind.
   - Wählen Sie **Zu verschlüsselnden Dateipfad auf USB-Geräten angeben**, um verschlüsselte Ordner auf USB-Laufwerken hinzuzufügen oder zu entfernen. Nicht vorhandene Ordner werden erstellt. Wenn kein Laufwerksbuchstabe angegeben wird, gilt diese Regel für alle USB-Geräte.

6. Wählen Sie unter **Benachrichtigungen** die Option **Rechtlichen Hinweis anzeigen**, um einen bestimmten rechtlichen Hinweis beim Start oder nur nach der Installation von File Encryption Agent anzuzeigen.

Hinweis

Benachrichtigungen werden nur von Trend Micro Dateiverschlüsselungsagenten der Versionen 3.1.3 und früher unterstützt.

Allgemeine Regeln für Richtlinien konfigurieren

Dieser Abschnitt erklärt die konfigurierbaren Optionen für Richtlinienregeln, die sich auf alle Endpoint Encryption Geräte auswirken.

Prozedur

1. Erstellen Sie eine neue Endpoint Encryption Richtlinie.
2. Klicken Sie auf **Allgemein**.

Das Fenster zu den Richtlinienregeleinstellungen **Allgemein** wird angezeigt.

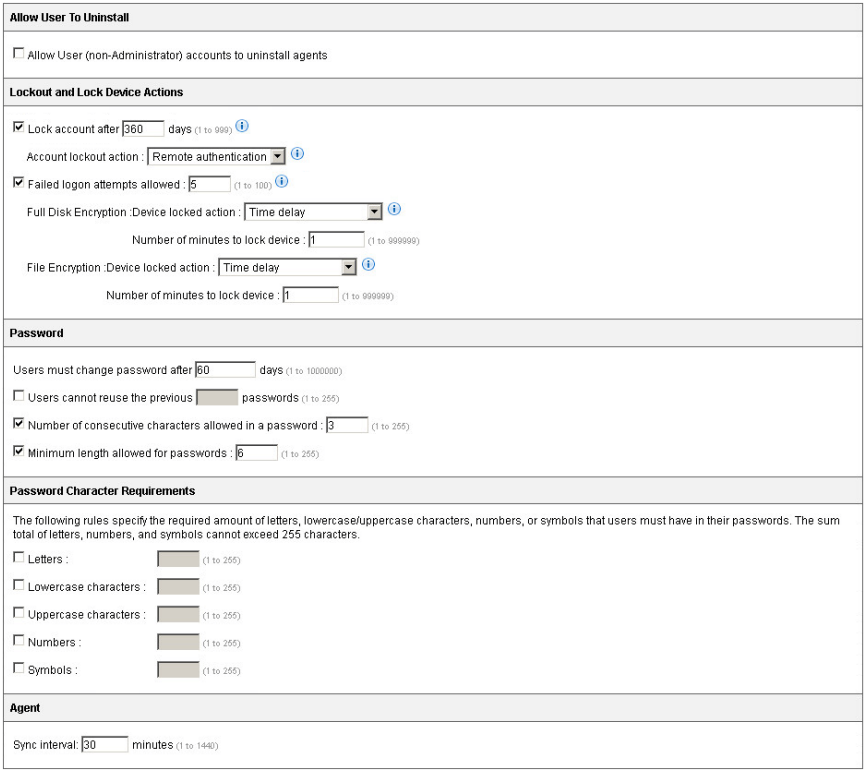


ABBILDUNG 28-4. Allgemeine Richtlinienregeln

3. Unter **Benutzer das Deinstallieren erlauben** wählen Sie **Benutzerkonten (nicht-Administrator) erlauben, Agentensoftware zu deinstallieren**, um jedem Endpoint Encryption-Benutzer das Deinstallieren des Agents zu erlauben.

Hinweis

Standardmäßig können nur Administratorkonten Endpoint Encryption Agents deinstallieren.

4. Konfigurieren Sie unter **Aktionen zum Sperren von Geräten** die folgenden Optionen:

   - Wählen Sie **Konto nach <number> Tagen sperren** aus, um anzugeben, für wie viele Tage das Endpoint Encryption Gerät gesperrt wird, wenn es die Richtlinien nicht synchronisiert.
     - Geben Sie mit **Kontosperraktion** an, ob bei einer Sperrung die Remote-Authentifizierung oder Löschung aktiviert werden soll.

     Hinweis

     Weitere Informationen zu Sperroptionen finden Sie unter *Sperraktionen auf Seite 28-18*

   - Wählen Sie die Option **Fehlgeschlagene Anmeldeversuche erlaubt** aus, um anzugeben, wie oft ein Benutzer versuchen kann, sich zu authentifizieren, bevor das Endpoint Encryption-Gerät gesperrt wird.
   - Konfigurieren Sie für Full Disk Encryption oder File Encryption Geräte Folgendes separat:
     - Geben Sie mit **Aktion zur Gerätesperrung** an, ob bei einer Sperrung die „Remote-Authentifizierung“ oder die „Löschung“ aktiviert werden soll.

     Hinweis

     Weitere Informationen zu Sperroptionen finden Sie unter *Sperraktionen auf Seite 28-18*

     - Verwenden Sie die Option **Anzahl der Minuten bis zur Sperrung des Geräts**, um die Dauer der Zeitverzögerung vor dem Sperren des Endpoint Encryption-Geräts ab der Authentifizierung anzugeben

5. Konfigurieren Sie unter **Kennwort** die folgenden Optionen:
   - Wählen Sie **Benutzer muss das Kennwort nach <Anzahl> Tagen ändern**, um anzugeben, wenn ein Benutzer aufgefordert wird, das Kennwort zu aktualisieren.
   - Wählen Sie **Benutzer darf die vorherigen <Anzahl> Kennwörter nicht wiederverwenden**, um anzugeben, wie viele vorherige Kennwörter der Benutzer nicht verwenden darf.
   - Wählen Sie **Anzahl der zulässigen aufeinanderfolgenden Zeichen in einem Kennwort**, um anzugeben, wie viele gleiche Zeichen ein Kennwort enthalten darf.
   - Wählen Sie **Zulässige Mindestlänge für Kennwörter**, um anzugeben, aus wie vielen Zeichen ein Kennwort mindestens bestehen muss.
6. Legen Sie unter **Kennwortvoraussetzungen** die Einschränkungen in Bezug auf Zeichen in Kennwörtern fest.
   - **Buchstaben**
   - **Kleinbuchstaben**
   - **Großbuchstaben**
   - **Zahlen**
   - **Symbole**

   Wichtig

   Die Gesamtzahl der Buchstaben, Ziffern und Symbole kann höchstens 255 betragen.
7. Geben Sie unter **Agent** das **Synchronisierungsintervall** in Minuten ein.

Sperraktionen

Einige Richtlinien verfügen über Einstellungen zum Sperren eines Benutzerkontos oder eines Geräts auf Grundlage bestimmter Kriterien.

Konto- und Gerätesperraktionen wirken sich auf das Endpoint Encryption-Gerät aus, unabhängig davon, ob der Agent Richtlinien mit PolicyServer synchronisiert oder nicht. Wenn der Endpoint Encryption-Agent beispielsweise eine bestimmte Zeit lang nicht mit PolicyServer kommuniziert, sperrt der Endpoint Encryption-Agent automatisch das Endpoint Encryption-Gerät. Die nachfolgende Tabelle vermittelt Ihnen ein Verständnis der verfügbaren Aktionen zur Sperrung von Konten und Geräten.

In der folgenden Tabelle wird beschrieben, wann die Sperraktionen auftreten:

Typ	Beschreibung
Kontosperrung	Kontosperraktionen werden wirksam, wenn der Endpoint Encryption-Agent eine gemäß der Richtlinie festgelegte bestimmte Zeit lang nicht mit PolicyServer kommuniziert.
Gerätesperrung bei Full Disk Encryption	Full Disk Encryption-Gerätesperraktionen werden wirksam, wenn der Endpoint Encryption-Benutzer die gemäß der Richtlinie festgelegte Anzahl der fehlgeschlagenen Anmeldeversuche bei dem Full Disk Encryption-Gerät überschreitet.
Gerätesperrung bei File Encryption	File Encryption-Gerätesperraktionen werden wirksam, wenn der Endpoint Encryption-Benutzer die gemäß der Richtlinie festgelegte Anzahl der fehlgeschlagenen Anmeldeversuche bei dem File Encryption-Gerät überschreitet.

Für Sperraktionen gibt es die folgenden Optionen:

Aktion	Beschreibung
Löschen	PolicyServer löscht alle Daten, die von dem zugeordneten Endpoint Encryption-Agent gesteuert werden. **Warnung!** Die Benutzer von Endpoint Encryption können die gelöschten Daten nicht wiederherstellen.

Aktion	Beschreibung
Remote-Authentifizierung	PolicyServer sperrt das Endpoint Encryption-Gerät, bis die Endpoint Encryption-Benutzerkontakte eine Authentifizierung mittels Remote-Hilfe von einem Authentifizierer oder vom Support erhalten.
Zeitverzögerung	PolicyServer sperrt das Endpoint Encryption-Gerät vorübergehend und benachrichtigt die Benutzer von Endpoint Encryption, dass das Gerät gesperrt ist. Die Möglichkeit zur Authentifizierung oder zum Zurücksetzen des Kennworts ist während der Zeitverzögerung deaktiviert. Die Dauer der Zeitverzögerung wird von der Richtlinie bestimmt. Sobald die Zeitverzögerung abgelaufen ist, ist es dem Benutzer gestattet, sich zu authentifizieren.

Gruppen zu Apex Central migrieren

Mit dem folgenden Verfahren können Sie vorhandene Gruppen von PolicyServer MMC zu Apex Central hinzufügen.

Prozedur

1. Melden Sie sich bei PolicyServer MMC an.
2. Sammeln Sie folgenden Informationen:
   - Die Gesamtzahl der Gruppen, deren Namen und Untergruppen
   - Alle Benutzer, die den jeweiligen Gruppen zugeordnet sind
   - Die Richtlinienkonfiguration der jeweiligen Gruppen
3. Melden Sie sich bei Apex Central an.
4. Konfigurieren Sie für jede Gruppe in PolicyServer MMC eine neue Richtlinie, die der entsprechenden Gruppenrichtlinienkonfiguration entspricht.

Hinweis

Untergruppen werden in Apex Central nicht unterstützt. Erstellen Sie zum Replizieren der Richtlinieneinstellungen für Untergruppen eine separate Richtlinie für jede Untergruppe.

5. Fügen Sie jeder entsprechenden neuen Richtlinie Benutzer hinzu.
6. Verteilen Sie jede Richtlinie.

Teil XII

Endpoint Sensor-Widgets und Richtlinien

Kapitel 29

Trend Micro Endpoint Sensor-Dashboard-Widgets

Dieser Abschnitt enthält Hilfethemen für die Trend Micro Endpoint Sensor-Dashboard-Widgets, die in Trend Micro Apex Central unterstützt werden.

Es werden folgende Themen behandelt:

Endpoint Sensor-Untersuchung

Das Widget **Endpoint Sensor-Untersuchung** stellt eine Verbindung mit einem Trend Micro Endpoint Sensor-Remote-Server her, um eine Untersuchung zu starten und die Ergebnisse der Untersuchung direkt im Apex Central-Dashboard anzuzeigen.

Klicken Sie auf **Neue Untersuchung starten**, um eine neue Untersuchung zu starten, und wählen Sie anschließend eine Untersuchungsmethode aus:

- **Verlaufsdaten**, um historische Ereignisse basierend auf benutzerdefinierten Kriterien zu untersuchen
- **Systemsnapshot**, um den aktuellen Status der ausgewählten Endpunkte zu untersuchen

Sobald die Seite **Neue Untersuchung** angezeigt wird, geben Sie die erforderlichen Kriterien ein. Die folgenden Untersuchungstypen sind verfügbar:

Untersuchungstyp	Beschreibung
Verlaufsdaten – Retro-Suche	Verlaufsereignisse basierend auf benutzerdefinierten Kriterien untersuchen
Verlaufsdaten – IOC-Regel	Verlaufsereignisse mit Hilfe einer IOC-Regel untersuchen
Systemsnapshot – Registrierung durchsuchen	Windows-Registrierung untersuchen
Systemsnapshot – YARA-Regel	Speicherresidente Bedrohungen mit Hilfe einer YARA-Regel untersuchen
Systemsnapshot – IOC-Regel	Ereignisse mit Hilfe einer IOC-Regel untersuchen
Systemsnapshot – IOC-Regel Festplatte	Dateien mit Hilfe einer IOC-Regel untersuchen

Untersuchungstyp	Beschreibung
Systemsnapshot – Systemprüfung	Alle aktiven Prozesse, Dienste und Module untersuchen

Klicken Sie auf **Untersuchen**, um die Untersuchung zu starten. Um eine laufende Untersuchung zu beenden, klicken Sie auf **Abbrechen**.

Das Widget wird in regelmäßigen Abständen aktualisiert und zeigt den Fortschritt der Untersuchung an. Das Widget zeigt ein Ringdiagramm an, das eine grafische Darstellung der Gesamtzahl der Endpunkte bietet, die wie folgt klassifiziert sind:

- **Übereinstimmung**: Zeigt die Anzahl der Endpunkte an, auf denen ein übereinstimmendes Objekt gefunden wurde.
- **Sicher**: Gibt die Anzahl der Endpunkte an, auf denen kein übereinstimmendes Objekt gefunden wurde.
- **Ausstehend**: Gibt die Anzahl der Endpunkte an, die noch nicht untersucht wurden.
- **Abgebrochen**: Gibt die Anzahl der Endpunkte an, die eines der folgenden Kriterien erfüllen:
  - Bei der auf dem Endpunkt durchgeführten Untersuchung ist ein Fehler aufgetreten
  - Der Endpunkt ist offline, oder alle an den Endpunkt gesendeten Befehle führen zu einer Zeitüberschreitung
  - Die Untersuchung des Endpunkts wurde durch den Benutzer manuell unterbrochen

Auf der rechten Seite des Ringdiagramms ist eine Aufschlüsselung der Gesamtzahlen angegeben. Klicken Sie auf den Zähler für jede Klassifizierung, um das Fenster **Untersuchungsergebnisse** anzuzeigen. Dieses Fenster enthält weitere Informationen zu den neuesten Untersuchungsergebnissen, die von Apex Central ermittelt wurden.

Hinweis

- Nachdem ein Server hinzugefügt wurde, aktualisieren Sie das Widget, um Daten von dem neuen Server abzurufen.
- Wenn mehrere Server hinzugefügt werden, zeigt das Widget das aggregierte Ergebnis sämtlicher Daten des Servers an.

Intelligente Überwachung, Übersicht nach Host

Dieses Widget zeigt einen Überblick über die Endpunkte an, auf denen zuletzt eine Überwachungsregel ausgelöst wurde. Die Daten werden aus dem Widget **Intelligente Überwachung, Übersicht nach Host** im Trend Micro Endpoint Sensor-Server-Dashboard abgerufen.

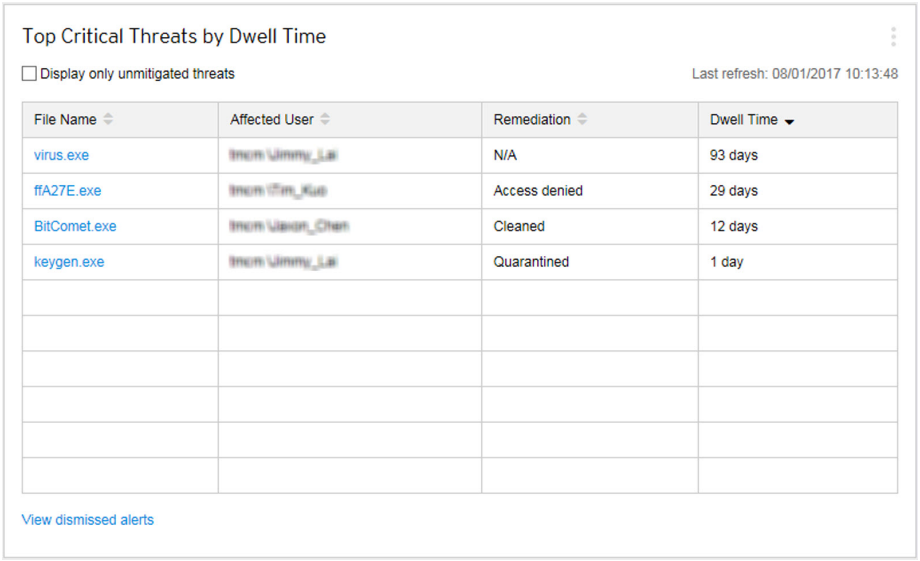
Name der Spalte	Beschreibung
Host-Name	Der Hostname des Endpunkts
Trefferanzahl	Anzahl der auf dem Endpunkt ausgelösten übereinstimmenden Regeln Klicken Sie hierauf, um Details zu den auf dem Endpunkt ausgelösten Regeln anzuzeigen.
Regelkategorie	Klassifizierung basierend auf sechs Stufen eines zielgerichteten Angriffs
Zeitpunkt der Erkennung	Datum und Uhrzeit, zu dem bzw. der die Regel zuletzt auf dem Endpunkt ausgelöst wurde

Der Standardzeitraum ist **Letzte 24 Stunden**. Ändern Sie den Zeitraum entsprechend Ihrer Präferenzen.

Hinweis

- Das Widget benötigt eine vorhandene Verbindung zu einem Trend Micro Endpoint Sensor-Server. Nachdem ein Server hinzugefügt wurde, aktualisieren Sie das Widget, um Daten von dem neuen Server abzurufen.
- Wenn mehrere Server hinzugefügt werden, zeigt das Widget das aggregierte Ergebnis sämtlicher Daten des Servers an.

Kritischste Bedrohungen nach Verweilzeit – Widget



Dieses Widget zeigt einen Überblick über die kritischsten Bedrohungen basierend auf der Dauer an, die eine Bedrohung bereits auf dem Endpunkt des betroffenen Benutzers vorhanden ist.

Wichtig

Dieses Widget benötigt einen registrierten Trend Micro Endpoint Sensor-Server. Das Widget zeigt die Ergebnisse der vom Trend Micro Endpoint Sensor-Server durchgeführten Auswirkungsbewertung basierend auf den SHA-1 Werten von Dateien an, die als kritische Bedrohungen gelten.

Sie können **Nur uneingeschränkte Bedrohungen anzeigen** auswählen, um nur die kritischen Bedrohungen anzuzeigen, die behoben werden müssen.

Klicken Sie auf die Spaltenüberschriften, um die Daten in der Tabelle zu sortieren.

Spalte	Beschreibung
Dateiname	Zeigt den Dateinamen der erkannten kritischen Bedrohung an Klicken Sie auf den **Dateiname**, um zusätzliche Bedrohungsinformationen anzuzeigen oder um eine weitere Untersuchung durchzuführen.
Betroffene Benutzer	Zeigt den Namen des betroffenen Benutzers an
Wiederherstellung	Zeigt die von einem Trend Micro Produkt durchgeführte Wartungsaktion an
Verweilzeit	Zeigt an, wie lange die Bedrohung auf dem Endpunkt des betroffenen Benutzers beibehalten wurde

Klicken Sie auf **Abgelehnte Warnungen anzeigen**, um das Fenster **Verworfene Warnungen** zu öffnen und ausschließlich Informationen über Warnungen für kritische Bedrohungen anzuzeigen, die von einem Apex Central-Benutzerkonto manuell abgewiesen wurden.

Spalte	Beschreibung
Verworfen	Zeigt den Zeitpunkt an, an dem die Warnung für kritische Bedrohungen abgewiesen wurde

Spalte	Beschreibung
Dateiname	Zeigt den Dateinamen der erkannten kritischen Bedrohung an Klicken Sie auf den **Dateiname**, um zusätzliche Bedrohungsinformationen anzuzeigen oder um eine weitere Untersuchung durchzuführen.
Betroffene Benutzer	Zeigt den Namen des betroffenen Benutzers an
Verweilzeit	Zeigt an, wie lange die Bedrohung auf dem Endpunkt des betroffenen Benutzers beibehalten wurde
Verworfen von	Zeigt das Apex Central Benutzerkonto an, das die Warnung für kritische Bedrohungen abgewiesen hat

Kapitel 30

Trend Micro Endpoint Sensor Server-Integration und Richtlinieneinstellungen

Der folgende Inhalt erklärt, wie Trend Micro Endpoint Sensor in Apex Central integriert wird und wie Richtlinien über die Apex Central-Konsole verwaltet werden.

Es werden folgende Themen behandelt:

Endpoint Sensor-Integration

Die Integration von Apex Central mit eigenständigen Endpoint Sensor-Servern ermöglicht die folgenden Funktionen und Fähigkeiten:

- Hochgeladene IOC-Dateien in Apex Central verwenden, um Untersuchungen direkt für Endpoint Sensor über die Apex Central-Konsole einzuleiten.
- Registrierung mehrerer Endpoint Sensor-Server. Apex Central können gleichzeitige Untersuchungen auf mehreren Endpoint Sensor-Servern starten.
- Daten aus Endpoint Sensor-Untersuchungsergebnissen abrufen. Die Daten werden dann in einem Apex Central-Widget angezeigt.
- Richtlinien erstellen und an bei Apex Central registrierte Endpoint Sensor-Server verteilen.
- Überwachungsregeln in Apex Central verwalten.
- **Einreichungseinstellungen** konfigurieren und an bei Apex Central registrierte Endpoint Sensor-Server verteilen.

Bei Apex Central registrieren

Prozedur

1. Öffnen Sie die Trend Micro Apex Central Management-Konsole.

   Um die Trend Micro Apex Central-Konsole auf einem beliebigen Endpunkt im Netzwerk zu öffnen, öffnen Sie einen Webbrowser und geben Sie Folgendes ein:

   ```
   https:// <Apex Central server name> /Webapp/index.html
   ```

   `<Apex Central server name>` steht für die IP-Adresse oder den Host-Namen des Trend Micro Apex Central Servers

2. Navigieren Sie zu **Administration** > **Verwaltete Server** > **Serverregistrierung**.

3. Wählen Sie im daraufhin angezeigten Fenster **Trend Micro Endpoint Sensor** als **Servervariante** aus und klicken Sie auf **Hinzufügen**.
4. Geben Sie im Fenster **Server hinzufügen** folgende Informationen ein:
   - Server
   - Anzeigename
   - Benutzername
   - Kennwort
5. Klicken Sie auf **Speichern**, um den Server zur Liste hinzuzufügen. Wiederholen Sie diese Schritte, um einen weiteren Server hinzuzufügen.

Endpoint Sensor-Widgets hinzufügen

Prozedur

1. Öffnen Sie die Trend Micro Apex Central Management-Konsole.

   Um die Trend Micro Apex Central-Konsole auf einem beliebigen Endpunkt im Netzwerk zu öffnen, öffnen Sie einen Webbrowser und geben Sie Folgendes ein:

   ```
   https:// <Apex Central server name> /Webapp/index.html
   ```

   `<Apex Central server name>` steht für die IP-Adresse oder den Host-Namen des Trend Micro Apex Central Servers
2. Navigieren Sie zu **Administration** > **Verwaltete Server** > **Serverregistrierung**.
3. Wählen Sie im daraufhin angezeigten Fenster **Trend Micro Endpoint Sensor** als **Servervariante** aus und klicken Sie auf **Hinzufügen**.
4. Geben Sie die Details des hinzuzufügenden Servers an und klicken Sie auf **Speichern**.
5. Navigieren Sie zum **Dashboard**.

6. Wählen Sie eine vorhandene Registerkarte aus oder erstellen Sie eine neue Registerkarte.
7. Klicken Sie rechts neben der Registerkartenanzeige auf die Schaltfläche **Einstellungen**.
8. Klicken Sie auf **Widgets hinzufügen**.
9. Wählen Sie im daraufhin angezeigten Fenster die Kategorie **Endpoint Sensor** in der Dropdown-Liste aus.

   Die folgenden Widgets sind verfügbar:

TABELLE 30-1. Endpoint Sensor-Widgets

WIDGET-NAME	BESCHREIBUNG
Intelligente Überwachung, Übersicht nach Host	Zeigt die Endpunkte an, die eine Überwachungsregel auslösten. Aktualisieren Sie das Widget manuell, um die aktuellen Daten anzuzeigen. Klicken Sie zum Konfigurieren der Widget-Einstellungen auf ▼.
Endpoint Sensor-Untersuchung	Führen Sie eine Untersuchung durch und zeigen Sie einen kurzen Überblick über die neueste, von Apex Central gestartete Trend Micro Endpoint Sensor-Untersuchung an. Standardmäßig wird das Widget alle 2 Minuten aktualisiert. Klicken Sie zum Konfigurieren der Widget-Einstellungen auf ▼. Weitere Informationen finden Sie im *Trend Micro Endpoint Sensor Administratorhandbuch*.

10. Wählen Sie ein Widget oder beide Widgets aus und klicken Sie auf **Hinzufügen**.

    Hinzugefügte Widgets werden im **Dashboard** angezeigt. Diese Widgets zeigen einen Überblick über die neue#sten Untersuchungen und die Überwachungsergebnisse aller registrierten Server an.

Hinweis

Nach der Registrierung eines Endpoint Sensor-Servers aktualisieren Sie die Widgets **Endpoint Sensor-Untersuchung** und **Intelligente Überwachung, Übersicht nach Host**, um die Inhalte der Widgets mit Daten von dem neuen Server zu aktualisieren.

Apex Central zur Statusüberprüfung verwenden

Verwenden Sie die Widgets **Verbindungsstatus des Produkts** und **Verbindungsstatus des Agents**, um den Status der registrierten Endpoint Sensor-Server oder -Agents zu überprüfen. In diesen Widgets werden Informationen der Endpoint Sensor-Server angezeigt, die über das Fenster **Administration** > **Verwaltete Server** > **Serverregistrierung** hinzugefügt wurden.

Prozedur

1. Navigieren Sie zum **Dashboard**.
2. Klicken Sie auf die Registerkarte **Konformität**, um die folgenden Widgets anzuzeigen:

   Hinweis

   Der **Verbindungsstatus des Produkts** steht auch auf der Registerkarte **Zusammenfassung** zur Verfügung.

   - **Verbindungsstatus des Produkts**: Zeigt den Serverstatus in der Spalte **Server** an

     Klicken Sie auf **Details anzeigen**, um detaillierte Informationen über die Server anzuzeigen.

   - **Verbindungsstatus des Agents**: Zeigt die Gesamtzahl der Agents, Online- und Offline-Agents für alle Server an

     Klicken Sie auf die Anzahl in der Spalte **Online**, **Offline** oder **Gesamt**, um ausführliche Informationen zu den Agents anzeigen.

3. So fügen Sie die Widgets zu einer Registerkarte hinzu:
   a. Wechseln Sie zu einer vorhandenen Registerkarte oder erstellen Sie eine neue.
   b. Klicken Sie rechts neben der Registerkartenanzeige auf die Schaltfläche **Einstellungen**.
   c. Klicken Sie auf **Widgets hinzufügen**.
   d. Wählen Sie im Fenster **Widgets hinzufügen** die Kategorie **Konformität** aus.
   e. Wählen Sie **Verbindungsstatus des Agents** oder **Verbindungsstatus des Produkts** aus.
   f. Klicken Sie auf **Hinzufügen**.

      Das hinzugefügte Widget wird auf der aktuellen Registerkarte angezeigt.

Widget „Endpoint Sensor-Untersuchung“ verwenden

Prozedur

1. Management-Konsole von Apex Central öffnen.
2. Navigieren Sie zu der Registerkarte, der das Widget „Endpoint Sensor Untersuchung“ hinzugefügt wurde.
3. Klicken Sie im Widget „Endpoint Sensor Untersuchung“ auf **Neue Untersuchung starten** und dann je nach Typ der auszuführenden Untersuchung auf **Verlaufsdaten** oder **Systemsnapshot**.
4. Geben Sie im angezeigten Fenster die entsprechenden Informationen an.

   Das Widget „Endpoint Sensor Untersuchung“ unterstützt auch den Import von C&C-Callback-Ereignissen als Untersuchungskriterien.

a. Klicken Sie im Widget „Endpoint Sensor Untersuchung“ auf **Neue Untersuchung starten** > **Verlaufsdaten**.

b. Wählen Sie **Retro-Suche** als Untersuchungsmethode aus.

c. Klicken Sie auf **Import aus C&C-Callback-Ereignissen**.

d. Wählen Sie im angezeigten Fenster die C&C-Callback-Ereignisse aus, die untersucht werden müssen, und klicken Sie auf **OK**. Die Ereignisse werden als Untersuchungskriterien hinzugefügt.

5. Klicken Sie auf **Untersuchen**.

   Das Fenster wird aktualisiert und zeigt den Fortschritt der Untersuchung an.

   Hinweis

   Um eine laufende Untersuchung zu beenden, klicken Sie auf **Abbrechen**.

6. Nach Abschluss der Untersuchung wird im Widget die Anzahl der Endpunkte angezeigt, die während der Untersuchung als **Passend**, **Sicher**, **Ausstehend** oder **Abgebrochen** klassifiziert wurden. Klicken Sie auf das Ergebnis der jeweiligen Klassifizierung, um weitere Informationen anzuzeigen.

Automatische Updates verwenden

Zur Verwendung von Apex Central als lokalen Update-Server für Endpoint Sensor führen Sie die folgenden Schritte durch:

Prozedur

1. Einrichten automatischer Updates in Apex Central.

   a. Management-Konsole von Apex Central öffnen.

   b. Navigieren Sie zu **Administration** > **Updates** > **Zeitgesteuertes Update**.

   c. Suchen Sie nach den folgenden Pattern:

- Endpoint Sensor Ausnahme-Pattern
- Pattern für vertrauenswürdigen Endpoint Sensor
- Angriffserkennungs-Pattern

d. Klicken Sie für jedes Pattern auf den Pattern-Namen und wählen Sie **Zeitgesteuerte Downloads aktivieren** aus. Behalten Sie für alle anderen Einstellungen die Standardwerte bei.

Hinweis

Einstellungen für die automatische Verteilung wird für die Endpoint Sensor-Integration nicht unterstützt.

e. Klicken Sie auf **Save**.

2. Konfigurieren Sie Endpoint Sensor zur Verwendung von Apex Central als Update-Adresse.

a. Öffnen Sie die Management-Konsole des Endpoint Sensor-Servers.

b. Klicken Sie auf **Administration** > **Updates**.

c. Aktivieren Sie **Überwachungsregeln aus folgender Quelle herunterladen**.

d. Wählen Sie **Andere Update-Adresse** aus und geben Sie Folgendes im unten angezeigten Textfeld ein:

```
http://<Apex Central server Name>/TVCSDownload/
Activeupdate
```

e. Klicken Sie auf **Save**.

Apex Central bezieht die Endpoint Sensor Pattern während des nächsten zeitgesteuerten Updates mit ein. Endpoint Sensor lädt diese Pattern dann während des nächsten zeitgesteuerten Endpoint Sensor-Updates aus Apex Central herunter.

Trend Micro Endpoint Sensor-Richtlinie

Trend Micro Apex Central beinhaltet eine Funktion zur Richtlinienverwaltung, mit der Administratoren Überwachungsregeln remote aktualisieren und Übermittlungseinstellungen auf registrierten Servern bereitstellen können.

Hinweis

Mehrere Endpoint Sensor-Richtlinien können erstellt werden, jeder Server kann aber nur jeweils eine Richtlinie ausgeben.

Weitere Informationen finden Sie in der Dokumentation zu Trend Micro Apex Central unter:

http://docs.trendmicro.com/de-de/enterprise/apex-central.aspx

Server für die Richtlinienbereitstellung vorbereiten

Standardmäßig werden neu hinzugefügte Endpoint Sensor-Server im Ordner **Neue Entität** abgelegt. Die Server müssen in einen anderen Ordner verschoben werden, um für die Richtlinienbereitstellung sichtbar zu sein.

Prozedur

1. Management-Konsole von Apex Central öffnen.
2. Navigieren Sie zu **Verzeichnisse** > **Produkte** und klicken Sie auf **Verzeichnisverwaltung**.
3. Erweitern Sie in der Verzeichnis den Ordner **Neue Entität** und suchen Sie nach dem zu verwaltenden Server.
4. Führen Sie folgende Aktionen durch:
   - Ziehen Sie den Server in einen anderen Ordner und legen Sie ihn dort ab

- Klicken Sie auf **Ordner hinzufügen**, um einen neuen Ordner zu erstellen. Verschieben Sie den Server dann per Drag & Drop in den neuen Ordner.

Richtlinien erstellen und verteilen

Prozedur

1. Öffnen Sie die Trend Micro Apex Central Management-Konsole.
2. Navigieren Sie zu **Richtlinien** > **Richtlinienverwaltung**.
3. Wählen Sie in der Dropdown-Liste **Produkt** den Eintrag **Trend Micro Endpoint Sensor** aus.
4. Klicken Sie auf **Erstellen**.
5. Klicken Sie auf **Ziel(e) festlegen** und wählen Sie aus, auf welchen Endpoint Sensor-Servern Sie die Verteilung vornehmen möchten.
6. Konfigurieren Sie im Abschnitt **Überwachungseinstellungen** die Überwachungsregeln und die Übermittlungseinstellungen für die neue Richtlinie.
7. Klicken Sie auf **Verteilen**, um sofort mit der Richtlinienverteilung zu beginnen.

   Anschließend erzwingt Trend Micro Apex Central alle 24 Stunden alle nachfolgenden Updates für die Richtlinie auf den Endpoint Sensor-Zielservern.

   Weitere Informationen finden Sie in der Dokumentation zu Trend Micro Apex Central unter:

   http://docs.trendmicro.com/de-de/enterprise/apex-central.aspx

Überwachungsregeln verwalten

Beachten Sie dabei Folgendes:

- Überwachungsregeln verwalten:

Auf der Registerkarte **Überwachungsregeln** werden nur benutzerdefinierte Regeln angezeigt. Während Überwachungsregeln in allen Richtlinien verwendet werden, ist der Status einer Überwachungsregel (Aktiviert/Deaktiviert/Entfernen) für jede Richtlinie unabhängig. Administratoren können Richtlinien anpassen, indem sie auswählen, welche Überwachungsregeln für jede Richtlinie aktiviert, deaktiviert oder entfernt werden. Neue Überwachungsregeln sind standardmäßig deaktiviert.

Apex Central ist auf die Remote-Steuerung von Überwachungsregeln in Endpoint Sensor-Servern beschränkt, bei denen die Regeln Teil einer Endpoint Sensor-Richtlinie sind.

Wenn ein neuer Endpoint Sensor-Server registriert wird, übernimmt Apex Central den neuen Endpoint Sensor-Server automatisch in den Verteilungsplan für Regeln. Sobald die nächste Bereitstellung fällig ist, lädt Apex Central alle aktiven Überwachungsregeln auf den neu registrierten Server hoch.

- Überwachungsregeln hochladen:

  Um eine Überwachungsregel hochzuladen, klicken Sie auf **Richtlinien** > **Richtlinienverwaltung** und wählen Sie **Trend Micro Endpoint Sensor** als **Produkt** aus. Klicken Sie auf **Erstellen**, um eine neue Richtlinie zu erstellen, oder klicken Sie auf eine vorhandene Richtlinie, um den **Richtlinie erstellen / bearbeiten**-Bildschirm zu öffnen. Erweitern Sie **Überwachungseinstellungen**, klicken Sie auf **IOC-Regel hochladen** > **Datei auswählen** und navigieren Sie zum Speicherort der Überwachungsregel. Klicken Sie auf **Öffnen**, um die Überwachungsregel automatisch hochzuladen. Nach Abschluss des Uploads klicken Sie auf **Speichern** oder **Verteilen**.

Hinweis

- Es wird empfohlen, die zielseitigen Endpoint Sensor-Server anzugeben, bevor Sie die Regel hochladen.
- Die Funktion **IOC-Regel hochladen** wird nur dann aktiviert, wenn mindestens ein Endpoint Sensor-Server bei Apex Central registriert ist.

Das Hochladen derselben Überwachungsregel sowohl auf einem Apex Central-Server als auch auf einem Endpoint Sensor-Server, der bei Apex Central registriert ist, kann zu Konflikten führen. Behalten Sie über das Fenster **Überwachungseinstellungen** stets den Überblick über die hochgeladenen Überwachungsregeln, um Duplizierungen zu vermeiden.

Wenn eine doppelte Überwachungsregel gefunden wird, wird die folgende Meldung angezeigt: 'Die Datei konnte nicht hochgeladen werden. Die Datei ist bereits im Endpoint Sensor Server vorhanden. Entfernen Sie die Datei zuerst in der Endpoint Sensor Management-Konsole, und versuchen Sie es dann erneut.'

- Status einer Überwachungsregel ändern:

  Um den Status einer Überwachungsregel zu ändern, klicken Sie auf **Status umschalten** und wählen Sie **Aktivieren** oder **Deaktivieren** aus. Aktualisieren Sie anschließend die Remote-Regel der als Ziele in dieser Richtlinie angegebenen Endpoint Sensor-Server.

  Der Status einer Überwachungsregel ist für jede Richtlinie unabhängig.

- Überwachungsregeln entfernen:

  Um eine Regel zu entfernen, wählen Sie die Regel aus und klicken Sie auf **Entfernen**. Der Status der entfernen Regel ändert sich in **Entfernen**. Klicken Sie auf **Speichern** oder **Verteilen**, um den Prozess abzuschließen.

Warnung!

- Durch das Entfernen einer Überwachungsregel wird diese aus allen anderen Endpoint Sensor-Richtlinien entfernt.
- Wenn die gleiche Regel erneut in eine neue Richtlinie hochgeladen wird, wird die Regel bei der zeitgesteuerten Ausführung erneut aus der alten Richtlinie entfernt.

Wenn das Problem weiterhin besteht, wenden Sie sich zwecks Unterstützung an den Support von Trend Micro.

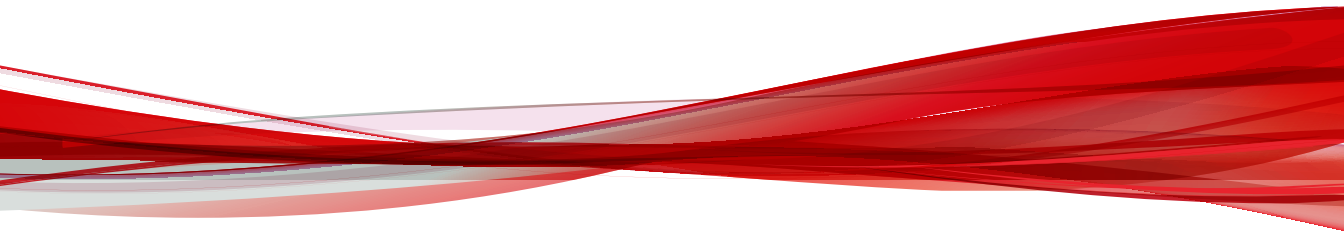
Übermittlungseinstellungen verwalten

Auf der Registerkarte **Übermittlungseinstellungen** können Sie angeben, ob die gesammelten Dateien an einen lokalen Dateiserver oder zur weiteren Analyse an Deep Discovery Analyzer gesendet werden.

Apex Central kann keine Proxy-Verbindung zwischen Endpoint Sensor-Endpunkten und Deep Discovery Analyzer konfigurieren. Verwenden Sie zum Konfigurieren einer Proxy-Verbindung zwischen Endpoint Sensor-Endpunkten und Deep Discovery Analyzer das Fenster **Proxy** des Endpoint Sensor-Servercomputers.

Teil XIII

InterScan-Sicherheitsrichtlinien



Kapitel 31

Richtlinieneinstellungen für InterScan Messaging Security Suite

In diesem Abschnitt wird erläutert, wie Richtlinieneinstellungen für InterScan Messaging Security Suite in Trend Micro Apex Central konfiguriert werden.

Es werden folgende Themen behandelt:

IMSS-Regeln

IMSS (InterScan Messaging Security Suite) wertet *Daten in einer E-Mail-Nachricht* anhand verschiedener definierter Regeln aus. Regeln bestimmen die Daten, die vor einer unbefugten Übertragung geschützt werden müssen, sowie die Aktion, die IMSS durchführt, wenn eine Übertragung erkannt wird.

IMSS-Regeln haben die folgenden Komponenten:

- Mail-Route: Eine Reihe von Absender- und Empfänger-E-Mail-Adressen oder -Gruppen oder ein LDAP-Benutzer oder eine LDAP-Gruppe, auf die die Richtlinie angewendet wird. Mit dem Sternchen (*) können Sie Platzhalterausdrücke erstellen und die Routenkonfiguration vereinfachen.
- Filter: Eine Regel oder eine Gruppe von Regeln, die auf eine bestimmte Route angewendet werden. In Trend Micro Apex Central können Sie Regeln zum Schutz vor Datenverlust mit Hilfe von Vorlagen festlegen.
- Aktion: Die Aktion, die IMSS durchführt, wenn die Filterbedingungen erfüllt sind.

IMSS-Regeln hinzufügen

Das Erstellen einer Regel umfasst die folgenden Schritte:

- Schritt 1: Regelnamen festlegen
- Schritt 2: Empfänger und Absender auswählen
- Schritt 3: Vorlagen auswählen
- Schritt 4: Aktionen auswählen

Prozedur

1. Klicken Sie unter **Einstellungen** auf **Hinzufügen**.

   Das Fenster **Regel hinzufügen** wird angezeigt.

Schritt 1: Regelnamen festlegen

Prozedur

1. Geben Sie einen Namen für die Regel ein. Der Name darf eine Länge von 122 Byte nicht überschreiten.
2. Weisen Sie dem Namen eine Nummer zu, um seine Position innerhalb der Regelhierarchie anzugeben.
3. Klicken Sie auf **Weiter**.

   Das Fenster **Empfänger und Absender auswählen** wird angezeigt.

Schritt 2: Empfänger und Absender auswählen

Legen Sie die E-Mail-Adressen der Absender und Empfänger oder Gruppen oder einen LDAP-Benutzer oder eine LDAP-Gruppe fest, auf die die Regel angewendet wird. Sie können auch Ausnahmen für eine E-Mail-Route konfigurieren.

Prozedur

1. Klicken Sie auf den Link neben **An:** oder **Von:**.

   Das Fenster **Empfänger festlegen** oder **Absender festlegen** wird angezeigt.
2. Wählen Sie eine der folgenden Optionen:
   - **Jeder**: Wählen Sie diese Option aus, um etwaige Beschränkungen für die Empfänger oder Absender zu entfernen.
   - **Eine der ausgewählten Adressen**
3. Bei Auswahl von **Eine der ausgewählten Adressen** verwenden Sie eine der folgenden Optionen aus dem Listenfeld:
   - **E-Mail-Adresse eingeben**: Geben Sie die E-Mail-Adresse ein, die hinzugefügt werden soll.

- **Nach LDAP-Benutzern oder -Gruppen suchen**: Geben Sie den Namen des LDAP-Benutzers oder der LDAP-Gruppe ein und klicken Sie auf **Suchen**. Die Ergebnisse werden im Listenfeld angezeigt.
- **Adressgruppen auswählen**: Alle vorhandenen Adressgruppen werden in der Liste angezeigt.

Bei Auswahl einer LDAP-Gruppe als Empfänger oder Absender können Sie Platzhalterzeichen am Anfang und/oder am Ende der LDAP-Gruppe verwenden, wenn Sie Microsoft Active Directory oder Sun iPlanet Directory als LDAP-Server angegeben haben.

Für weitere Informationen siehe *Verwendung des Asterisk-Platzhalters auf Seite 31-5*.

4. Wenn Sie eine E-Mail-Adresse hinzufügen, klicken Sie auf **Hinzufügen >**. Wenn Sie einen LDAP-Benutzer, eine LDAP-Gruppe oder eine Adressgruppe hinzufügen möchten, klicken Sie auf das Listenfeld und dann auf **Hinzufügen >**.
5. Klicken Sie auf **Save**.
6. Klicken Sie auf **Weiter**.

   Das Fenster **Schritt 3: Vorlage auswählen** wird angezeigt.

Ausnahmen konfigurieren

Sie können eine Route konfigurieren, die für eine große Gruppe von Absendern oder Empfängern gilt, mit Ausnahme bestimmter Benutzer, für die die Regel nicht gilt.

Prozedur

1. Klicken Sie auf **Absender und Empfänger** neben **Ausnahmen**.

   Das Fenster **Ausnahmen festlegen** wird angezeigt.
2. Unter **Adressen auswählen** wählen Sie eine der folgenden Optionen für beide Adressen **Von (Absender)** und **An (Empfänger)** aus:

- **E-Mail-Adresse eingeben**: Geben Sie die E-Mail-Adresse ein, die hinzugefügt werden soll.
- **Nach LDAP-Benutzern oder -Gruppen suchen**: Geben Sie den LDAP-Benutzer- oder -Gruppennamen ein und klicken Sie auf 'Suchen'. Die Ergebnisse werden im Listenfeld angezeigt.
- **Adressgruppen auswählen**: Alle vorhandenen Adressgruppen werden in der Liste angezeigt.

3. Wenn Sie eine E-Mail-Adresse hinzufügen, klicken Sie auf **Hinzufügen >**. Wenn Sie einen LDAP-Benutzer, eine LDAP-Gruppe oder eine Adressgruppe hinzufügen möchten, klicken Sie auf das Listenfeld und dann auf **Hinzufügen >**.
4. Klicken Sie auf **Save**.

Sternchen als Platzhalterzeichen verwenden

Sie können das Sternchen (*) als Platzhalterzeichen in E-Mail-Adressen verwenden, wenn Sie Routen definieren.

Platzhalter können in den Namens- oder Domänenabschnitten einer E-Mail-Adresse angezeigt werden. Bei Folgendem handelt es sich um gültige Beispiele:

- *@*: Gültige Darstellung aller E-Mail-Adressen.
- *@domain.tld, name@*.tld: Gültige Darstellung des gesamten Namens oder der Domäne (nicht die Domäne der höchsten Ebene (Top Level Domain, TLD)).
- *@*.tld: Gültige Darstellung des Namens und der Domäne (nicht die TLD).

Platzhalter können nicht in einer Unterdomäne oder der Domäne der höchsten Ebene angezeigt werden. Platzhalter können auch nicht mit anderen Buchstaben versehen werden. Sie müssen einzeln verwendet werden. Bei Folgendem handelt es sich um ungültige Beispiele:

- name@domain.*.tld: Ungültige Darstellung einer Unterdomäne.

- name@domain.*: Ungültige Darstellung einer TLD.
- *name@domain.tld: Ungültige Verwendung in Verbindung mit einem Namen.

Schritt 3: Vorlagen auswählen

Mit Vorlagen wird verhindert, dass digitale Assets (wie z. B. Sozialversicherungs- und Kreditkartennummern) Ihr Unternehmensnetzwerk verlassen. Darüber hinaus sorgen sie für die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz.

Prozedur

1. Wählen Sie Vorlagen aus der Liste **Verfügbar** Vorlagen, und klicken Sie dann auf **>>**.

   Tipp
   Wählen Sie mehrere Vorlagen aus, indem Sie die STRG-Taste gedrückt halten und gleichzeitig die Vorlagen auswählen.

2. Klicken Sie auf **Weiter**.

   Das Fenster **Schritt 4: Aktionen auswählen** wird angezeigt.

Schritt 4: Aktionen auswählen

IMSS führt eine oder mehrere Aktionen durch, wenn es einen Versuch zur Übertragung digitaler Assets erkennt.

Prozedur

1. Wählen Sie eine der folgenden Aktionen aus:
   - **Quarantäne**: Weist IMSS an, die Nachrichten abzufangen und somit zu verhindern, dass sie die Empfänger erreichen.
   - **Benachrichtigungen senden**: Weist IMSS an, eine E-Mail-Benachrichtigung an einen oder mehrere Empfänger zu senden.

2. Wenn Sie **Benachrichtigungen senden** ausgewählt haben, wählen Sie den Benachrichtigungstyp aus, den Sie aus der Dropdown-Liste verwenden möchten. Die verfügbaren Benachrichtigungen hängen von den ausgewählten Zielen ab.
3. Klicken Sie auf **Fertig stellen**.

Vorhandene IMSS-Regeln ändern

Prozedur

1. Klicken Sie auf den Namen der zu bearbeitenden Regel.

   Das Fenster **Übersicht** für die Regel wird angezeigt.
2. Klicken Sie im **Regel**-Tab auf **Bearbeiten** für **Falls Empfänger und Absender**.
3. Konfigurieren Sie die Routing-Einstellungen.

   Für weitere Informationen siehe *Schritt 2: Empfänger und Absender auswählen auf Seite 31-3*.
4. Klicken Sie auf **Bearbeiten** für **Und Suchbedingungen übereinstimmen**.
5. Konfigurieren Sie die Vorlageneinstellungen.
6. Klicken Sie auf **Bearbeiten** für **Dann erfolgt die Aktion**.
7. Konfigurieren Sie die Aktionseinstellungen.

   Hinweis

   Wenn Trend Micro Apex Central keine Verbindung zu den ausgewählten Zielen herstellen kann, sind einige Aktionen möglicherweise nicht mehr verfügbar.
8. Klicken Sie auf **Save**.

IMSS-Regeln löschen

Prozedur

1. Aktivieren Sie das Kontrollkästchen neben der Regel, die gelöscht werden soll.
2. Klicken Sie auf **Löschen**.

Kapitel 32

Richtlinieneinstellungen für InterScan Messaging Security Virtual Appliance

In diesem Abschnitt wird erläutert, wie Richtlinieneinstellungen für InterScan Messaging Security Virtual Appliance in Apex Central konfiguriert werden.

Es werden folgende Themen behandelt:

IMSVA-Regeln

IMSVA (InterScan Messaging Security Virtual Appliance) wertet Daten in einer E-Mail-Nachricht anhand verschiedener definierter Regeln aus. Regeln bestimmen die Daten, die vor einer unbefugten Übertragung geschützt werden müssen, sowie die Aktion, die IMSVA durchführt, wenn eine Übertragung erkannt wird.

IMSVA-Regeln haben die folgenden Komponenten:

- Mail-Route: Eine Reihe von Absender- und Empfänger-E-Mail-Adressen oder -Gruppen oder ein LDAP-Benutzer oder eine LDAP-Gruppe, auf die die Richtlinie angewendet wird. Mit dem Sternchen (*) können Sie Platzhalterausdrücke erstellen und die Routenkonfiguration vereinfachen.
- Filter: Eine Regel oder eine Gruppe von Regeln, die auf eine bestimmte Route angewendet werden. In Apex Central können Sie Regeln zum Schutz vor Datenverlust mit Hilfe von Vorlagen festlegen.
- Aktion: Die Aktion, die IMSVA durchführt, wenn die Filterbedingungen erfüllt sind.

IMSVA-Regeln hinzufügen

Das Erstellen einer Regel umfasst die folgenden Schritte:

- Schritt 1: Regelnamen festlegen
- Schritt 2: Empfänger und Absender auswählen
- Schritt 3: Vorlagen auswählen
- Schritt 4: Aktionen auswählen

Prozedur

1. Klicken Sie unter **Einstellungen** auf **Hinzufügen**.

   Das Fenster **Regel hinzufügen** wird angezeigt.

Schritt 1: Regelnamen festlegen

Prozedur

1. Geben Sie einen Namen für die Regel ein. Der Name darf eine Länge von 122 Byte nicht überschreiten.
2. Weisen Sie dem Namen eine Nummer zu, um seine Position innerhalb der Regelhierarchie anzugeben.
3. Klicken Sie auf **Weiter**.

   Das Fenster **Empfänger und Absender auswählen** wird angezeigt.

Schritt 2: Empfänger und Absender auswählen

Legen Sie die E-Mail-Adressen der Absender und Empfänger oder Gruppen oder einen LDAP-Benutzer oder eine LDAP-Gruppe fest, auf die die Regel angewendet wird. Sie können auch Ausnahmen für eine E-Mail-Route konfigurieren.

Prozedur

1. Klicken Sie auf den Link neben **An:** oder **Von:**.

   Das Fenster **Empfänger festlegen** oder **Absender festlegen** wird angezeigt.
2. Wählen Sie eine der folgenden Optionen:
   - **Jeder**: Wählen Sie diese Option aus, um etwaige Beschränkungen für die Empfänger oder Absender zu entfernen.
   - **Eine der ausgewählten Adressen**
3. Bei Auswahl von **Eine der ausgewählten Adressen** verwenden Sie eine der folgenden Optionen aus dem Listenfeld:
   - **E-Mail-Adresse eingeben**: Geben Sie die E-Mail-Adresse ein, die hinzugefügt werden soll.

- **Nach LDAP-Benutzern oder -Gruppen suchen**: Geben Sie den Namen des LDAP-Benutzers oder der LDAP-Gruppe ein und klicken Sie auf **Suchen**. Die Ergebnisse werden im Listenfeld angezeigt.
- **Adressgruppen auswählen**: Alle vorhandenen Adressgruppen werden in der Liste angezeigt.

Bei Auswahl einer LDAP-Gruppe als Empfänger oder Absender können Sie Platzhalterzeichen am Anfang und/oder am Ende der LDAP-Gruppe verwenden, wenn Sie Microsoft Active Directory oder Sun iPlanet Directory als LDAP-Server angegeben haben. Weitere Informationen finden Sie unter „Verwenden des Sterns als Platzhalter“.

4. Wenn Sie eine E-Mail-Adresse hinzufügen, klicken Sie auf **Hinzufügen >**. Wenn Sie einen LDAP-Benutzer, eine LDAP-Gruppe oder eine Adressgruppe hinzufügen möchten, klicken Sie auf das Listenfeld und dann auf **Hinzufügen >**.
5. Klicken Sie auf **Save**.
6. Klicken Sie auf **Weiter**.

   Das Fenster **Schritt 3: Vorlage auswählen** wird angezeigt.

Ausnahmen konfigurieren

Sie können eine Route konfigurieren, die für eine große Gruppe von Absendern oder Empfängern gilt, mit Ausnahme bestimmter Benutzer, für die die Regel nicht gilt.

Prozedur

1. Klicken Sie auf den Link neben **Ausnahmen**.

   Das Fenster **Ausnahmen festlegen** wird angezeigt.
2. Wählen Sie unter **Adressen auswählen** eine der folgenden Optionen für die Felder 'Von' und 'An':
   - **E-Mail-Adresse eingeben**: Geben Sie die E-Mail-Adresse ein, die hinzugefügt werden soll.

- **Nach LDAP-Benutzern oder -Gruppen suchen**: Geben Sie den LDAP-Benutzer- oder -Gruppennamen ein und klicken Sie auf 'Suchen'. Die Ergebnisse werden im Listenfeld angezeigt.
- **Adressgruppen auswählen**: Alle vorhandenen Adressgruppen werden in der Liste angezeigt.

3. Wenn Sie eine E-Mail-Adresse hinzufügen, klicken Sie auf **Hinzufügen >**. Wenn Sie eine LDAP- oder Adressgruppe hinzufügen, klicken Sie in das Listenfeld und klicken Sie dann auf **Hinzufügen >**.
4. Klicken Sie auf **Save**.

Sternchen als Platzhalterzeichen verwenden

Sie können das Sternchen (*) als Platzhalterzeichen in E-Mail-Adressen verwenden, wenn Sie Routen definieren.

Platzhalter können in den Namens- oder Domänenabschnitten einer E-Mail-Adresse angezeigt werden. Bei Folgendem handelt es sich um gültige Beispiele:

- *@*: Gültige Darstellung aller E-Mail-Adressen.
- *@domain.tld, name@*.tld: Gültige Darstellung des gesamten Namens oder der Domäne (nicht die Domäne der höchsten Ebene (Top Level Domain, TLD)).
- *@*.tld: Gültige Darstellung des Namens und der Domäne (nicht die TLD).

Platzhalter können nicht in einer Unterdomäne oder der Domäne der höchsten Ebene angezeigt werden. Platzhalter können auch nicht mit anderen Buchstaben versehen werden. Sie müssen einzeln verwendet werden. Bei Folgendem handelt es sich um ungültige Beispiele:

- name@domain.*.tld: Ungültige Darstellung einer Unterdomäne.
- name@domain.*: Ungültige Darstellung einer TLD.
- *name@domain.tld: Ungültige Verwendung in Verbindung mit einem Namen.

Schritt 3: Vorlagen auswählen

Mit Vorlagen wird verhindert, dass digitale Assets (wie z. B. Sozialversicherungs- und Kreditkartennummern) Ihr Unternehmensnetzwerk verlassen. Darüber hinaus sorgen sie für die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz.

Prozedur

1. Wählen Sie Vorlagen in der Liste „Verfügbare Vorlagen“ aus und klicken Sie dann auf **>>**.

   Wählen Sie mehrere Vorlagen aus, indem Sie die Strg-Taste gedrückt halten und gleichzeitig die Vorlagen auswählen.

2. Klicken Sie auf **Weiter**.

   Das Fenster **Schritt 4: Aktionen auswählen** wird angezeigt.

Schritt 4: Aktionen auswählen

IMSVA führt eine oder mehrere Aktionen durch, wenn es einen Versuch zur Übertragung digitaler Assets erkennt.

Prozedur

1. Wählen Sie eine der folgenden Aktionen aus:

   - **Quarantäne**: Weist IMSVA an, die Nachrichten abzufangen und somit zu verhindern, dass sie die Empfänger erreichen.
   - **Benachrichtigungen senden**: Weist IMSVA an, eine E-Mail-Benachrichtigung an einen oder mehrere Empfänger zu senden.

2. Bei Auswahl von **Benachrichtigungen senden** legen Sie den Typ der zu verwendenden E-Mail-Benachrichtigung in der Dropdown-Liste fest.

   Die verfügbaren Benachrichtigungen richten sich nach den ausgewählten Zielen.

3. Klicken Sie auf **Fertig stellen**.

Vorhandene IMSVA-Regeln ändern

Prozedur

1. Klicken Sie auf den Namen der zu bearbeitenden Regel.

   Das Fenster **Übersicht** für die Regel wird angezeigt.

2. Klicken Sie auf der Registerkarte **Regel** für **Falls Empfänger und Absender** auf **Bearbeiten**.

3. Konfigurieren Sie die Routing-Einstellungen.

   Weitere Informationen finden Sie unter *Schritt 2: Empfänger und Absender auswählen auf Seite 32-3*.

4. Klicken Sie für **Und Suchbedingungen übereinstimmen** auf **Bearbeiten**.

5. Konfigurieren Sie die Vorlageneinstellungen.

6. Klicken Sie für **Dann erfolgt die Aktion** auf **Bearbeiten**.

7. Konfigurieren Sie die Aktionseinstellungen.

   Hinweis

   Wenn Trend Micro Apex Central keine Verbindung zu den ausgewählten Zielen herstellen kann, sind einige Aktionen möglicherweise nicht mehr verfügbar.

8. Klicken Sie auf **Save**.

IMSVA-Regeln löschen

Prozedur

1. Aktivieren Sie das Kontrollkästchen neben der Regel, die gelöscht werden soll.

2. Klicken Sie auf **Löschen**.

Kapitel 33

Richtlinieneinstellungen für InterScan Web Security Suite

In diesem Abschnitt wird erläutert, wie Richtlinieneinstellungen für InterScan Web Security Suite in Apex Central konfiguriert werden.

Es werden folgende Themen behandelt:

Regelliste für die Funktion 'Prävention vor Datenverlust'

Wenn Sie die Option 'Prävention vor Datenverlust' aktivieren, können Sie auch einzelne Regeln für 'Prävention vor Datenverlust' aktivieren oder deaktivieren. Das grüne Häkchen zeigt an, dass die Regel aktiviert ist. Das rote 'x' bedeutet, dass die Regel deaktiviert ist. Sie können auf das Symbol klicken, um zwischen aktiviertem und deaktiviertem Status umzuschalten.

Die folgenden Optionen sind in diesem Fenster verfügbar:

Regel: Klicken, um die Regel zu bearbeiten.

Hinzufügen: Öffnet das Fenster **Regel hinzufügen**, in dem Sie eine neue Regel konfigurieren können.

Kopieren: Ermöglicht Ihnen, eine ausgewählte Regel aus der Liste zu kopieren.

Löschen: Ermöglicht Ihnen, eine Regel aus der Liste zu löschen.

Priorität: Klicken Sie auf den Pfeil, um die Regelpriorität zu ändern.

Status: Klicken Sie auf das Symbol, um die Regel zu aktivieren oder zu deaktivieren.

Speichern: Klicken Sie hierauf, um die Regel zu speichern.

Schritt 1: Regelnamen festlegen

Nachfolgend finden Sie eine kurze Beschreibung der in diesem Fenster verfügbaren Optionen.

- **Aktivieren**: Wählen, um die Regel zu aktivieren.
- **Regelname**: Geben Sie einen Namen an, der für diese Regel angezeigt werden soll.
- **Weiter >**: Klicken Sie, um den Vorgang fortzusetzen.

Schritt 2: Konten auswählen

Nachfolgend finden Sie eine kurze Beschreibung der in diesem Fenster verfügbaren Optionen.

Hinweis

Es sind nicht alle Optionen verfügbar, wenn Entwurfsregeln erstellt werden. Geben Sie einen Server an, um alle Optionen zu aktivieren.

- Geben Sie IP-Adressen für die Konten an, auf die die Regel angewendet wird.
  - Geben Sie einen IP-Bereich in **Von** und **An**, eine spezifische Konto-IP-Adresse oder einen Host-Namen in **IP/Hostname** oder ein IP-Subnetz in **Adresse** und **Präfixlänge** ein.
  - Klicken Sie auf **Hinzufügen**, um ein oder mehrere Konten in der Tabelle auf der rechten Seite zu erstellen.
  - Klicken Sie auf **Löschen**, um ein oder mehrere Konten aus der Tabelle auf der rechten Seite zu entfernen.
- **< Zurück**: Klicken Sie hierauf, um zur vorherigen Seite zurückzukehren.
- **Weiter >**: Klicken Sie, um den Vorgang fortzusetzen.

Schritt 3: Zu sperrende Vorlagen zur Einhaltung von Richtlinien auswählen

Nachfolgend finden Sie eine kurze Beschreibung der in diesem Fenster verfügbaren Optionen.

- **Geben Sie die Vorlagen zur Einhaltung von Richtlinien an, die mit dieser Regel gesperrt werden sollen.**
  - **Verfügbare Vorlage(n)**: Die aufgeführten Vorlagen können mit der Regel verwendet werden.
  - **Ausgewählte Vorlage(n) zum Sperren**: Die zu sperrende Regel wird auf die Vorlagen in der Liste angewendet.

Tipp

Wählen Sie mehrere Vorlagen aus, indem Sie bei gedrückter Umschalt- oder Strg-Taste auf die Namen der Konten klicken.

- **>>**: Klicken Sie hierauf, um verfügbare Vorlagen zur Liste der ausgewählten Vorlagen hinzuzufügen.
- **<<**: Klicken Sie hierauf, um Vorlagen aus der Liste der ausgewählten Vorlagen zu entfernen.

- **< Zurück**: Klicken Sie hierauf, um zur vorherigen Seite zurückzukehren.
- **Weiter >**: Klicken Sie, um den Vorgang fortzusetzen.

Schritt 4: Zu überwachende Vorlagen zur Einhaltung von Richtlinien auswählen

Nachfolgend finden Sie eine kurze Beschreibung der in diesem Fenster verfügbaren Optionen.

- **Geben Sie die Vorlagen zur Einhaltung von Richtlinien an, die mit dieser Regel überwacht werden sollen.**
  - **Verfügbare Vorlage(n)**: Die aufgeführten Vorlagen können mit der Regel verwendet werden.
  - **Ausgewählte Vorlage(n) zur Überwachung**: Die Regel zur Überwachung wird auf die Vorlagen in der Liste angewendet.

Tipp

Wählen Sie mehrere Vorlagen aus, indem Sie bei gedrückter Umschalt- oder Strg-Taste auf die Namen der Konten klicken.

  - **>>**: Klicken Sie hierauf, um verfügbare Vorlagen zur Liste der ausgewählten Vorlagen hinzuzufügen.
  - **<<**: Klicken Sie hierauf, um Vorlagen aus der Liste der ausgewählten Vorlagen zu entfernen.
- **< Zurück**: Klicken Sie hierauf, um zur vorherigen Seite zurückzukehren.

- **Fertig stellen**: Klicken Sie hierauf, um zur Liste der Regeln zurückzukehren.

Kapitel 34

Richtlinieneinstellungen für InterScan Web Security Virtual Appliance

In diesem Abschnitt wird erläutert, wie Richtlinieneinstellungen für InterScan Web Security Virtual Appliance in Apex Central konfiguriert werden.

Es werden folgende Themen behandelt:

Regelliste für die Funktion 'Prävention vor Datenverlust'

Wenn Sie die Option 'Prävention vor Datenverlust' aktivieren, können Sie auch einzelne Regeln für 'Prävention vor Datenverlust' aktivieren oder deaktivieren. Das grüne Häkchen zeigt an, dass die Regel aktiviert ist. Das rote 'x' bedeutet, dass die Regel deaktiviert ist. Sie können auf das Symbol klicken, um zwischen aktiviertem und deaktiviertem Status umzuschalten.

Die folgenden Optionen sind in diesem Fenster verfügbar:

Regel: Klicken, um die Regel zu bearbeiten.

Hinzufügen: Öffnet das Fenster **Regel hinzufügen**, in dem Sie eine neue Regel konfigurieren können.

Kopieren: Ermöglicht Ihnen, eine ausgewählte Regel aus der Liste zu kopieren.

Löschen: Ermöglicht Ihnen, eine Regel aus der Liste zu löschen.

Priorität: Klicken Sie auf den Pfeil, um die Regelpriorität zu ändern.

Status: Klicken Sie auf das Symbol, um die Regel zu aktivieren oder zu deaktivieren.

Speichern: Klicken Sie hierauf, um die Regel zu speichern.

Schritt 1: Regelnamen festlegen

Nachfolgend finden Sie eine kurze Beschreibung der in diesem Fenster verfügbaren Optionen.

- **Aktivieren**: Wählen, um die Regel zu aktivieren.
- **Regelname**: Geben Sie einen Namen an, der für diese Regel angezeigt werden soll.
- **Weiter >**: Klicken Sie, um den Vorgang fortzusetzen.

Schritt 2: Konten auswählen

Nachfolgend finden Sie eine kurze Beschreibung der in diesem Fenster verfügbaren Optionen.

Hinweis

Es sind nicht alle Optionen verfügbar, wenn Entwurfsregeln erstellt werden. Geben Sie einen Server an, um alle Optionen zu aktivieren.

- Geben Sie IP-Adressen für die Konten an, auf die die Regel angewendet wird.
  - Geben Sie einen IP-Bereich in **Von** und **An**, eine spezifische Konto-IP-Adresse oder einen Host-Namen in **IP/Hostname** oder ein IP-Subnetz in **Adresse** und **Präfixlänge** ein.
  - Klicken Sie auf **Hinzufügen**, um ein oder mehrere Konten in der Tabelle auf der rechten Seite zu erstellen.
  - Klicken Sie auf **Löschen**, um ein oder mehrere Konten aus der Tabelle auf der rechten Seite zu entfernen.
- **< Zurück**: Klicken Sie hierauf, um zur vorherigen Seite zurückzukehren.
- **Weiter >**: Klicken Sie, um den Vorgang fortzusetzen.

Schritt 3: Zu sperrende Vorlagen zur Einhaltung von Richtlinien auswählen

Nachfolgend finden Sie eine kurze Beschreibung der in diesem Fenster verfügbaren Optionen.

- **Geben Sie die Vorlagen zur Einhaltung von Richtlinien an, die mit dieser Regel gesperrt werden sollen.**
  - **Verfügbare Vorlage(n)**: Die aufgeführten Vorlagen können mit der Regel verwendet werden.
  - **Ausgewählte Vorlage(n) zum Sperren**: Die zu sperrende Regel wird auf die Vorlagen in der Liste angewendet.

Tipp

Wählen Sie mehrere Vorlagen aus, indem Sie bei gedrückter Umschalt- oder Strg-Taste auf die Namen der Konten klicken.

- **>>**: Klicken Sie hierauf, um verfügbare Vorlagen zur Liste der ausgewählten Vorlagen hinzuzufügen.
- **<<**: Klicken Sie hierauf, um Vorlagen aus der Liste der ausgewählten Vorlagen zu entfernen.

- **< Zurück**: Klicken Sie hierauf, um zur vorherigen Seite zurückzukehren.
- **Weiter >**: Klicken Sie, um den Vorgang fortzusetzen.

Schritt 4: Zu überwachende Vorlagen zur Einhaltung von Richtlinien auswählen

Nachfolgend finden Sie eine kurze Beschreibung der in diesem Fenster verfügbaren Optionen.

- **Geben Sie die Vorlagen zur Einhaltung von Richtlinien an, die mit dieser Regel überwacht werden sollen.**
  - **Verfügbare Vorlage(n)**: Die aufgeführten Vorlagen können mit der Regel verwendet werden.
  - **Ausgewählte Vorlage(n) zur Überwachung**: Die Regel zur Überwachung wird auf die Vorlagen in der Liste angewendet.

Tipp

Wählen Sie mehrere Vorlagen aus, indem Sie bei gedrückter Umschalt- oder Strg-Taste auf die Namen der Konten klicken.

  - **>>**: Klicken Sie hierauf, um verfügbare Vorlagen zur Liste der ausgewählten Vorlagen hinzuzufügen.
  - **<<**: Klicken Sie hierauf, um Vorlagen aus der Liste der ausgewählten Vorlagen zu entfernen.
- **< Zurück**: Klicken Sie hierauf, um zur vorherigen Seite zurückzukehren.

- **Fertig stellen**: Klicken Sie hierauf, um zur Liste der Regeln zurückzukehren.

Teil XIV

ScanMail for Microsoft Exchange – Richtlinien

Kapitel 35

ScanMail for Microsoft Exchange – Richtlinieneinstellungen

In diesem Abschnitt wird erläutert, wie Sie die Richtlinieneinstellungen von ScanMail for Microsoft Exchange in der Apex Central-Konsole konfigurieren.

Es werden folgende Themen behandelt:

Richtlinie für die Prävention vor Datenverlust konfigurieren

Richtlinien für 'Prävention vor Datenverlust' regeln die Maßnahmen, die Trend Micro Apex Central ergreift, wenn sensible Informationen in E-Mail-Nachrichten entdeckt werden.

Erstellen Sie eine neue Richtlinie, indem Sie auf **Prävention vor Datenverlust** > **DLP-Richtlinien** > **Hinzufügen** klicken.

Ändern Sie eine bestehende Richtlinie, indem Sie auf **Prävention vor Datenverlust** > **DLP-Richtlinien** > **[DLP-Richtlinienname]** klicken.

Konfigurieren Sie Richtlinien für „Prävention vor Datenverlust“, indem Sie die folgenden fünf Schritte durchführen:

1. *Konten auswählen auf Seite 35-2*
2. *DLP-Ziele konfigurieren auf Seite 35-3*
3. *DLP-Aktionen konfigurieren auf Seite 35-4*
4. *DLP-Benachrichtigungen konfigurieren auf Seite 35-5*
5. *DLP-Richtlinie aktivieren auf Seite 35-6*

Konten auswählen

Prozedur

1. Gehen Sie zum Bildschirm **Richtlinien für 'Prävention vor Datenverlust'**, indem Sie zu **Prävention vor Datenverlust** > **DLP-Richtlinien** navigieren.
2. Fügen Sie eine Richtlinie oder Ausnahme hinzu oder bearbeiten Sie sie:
   - Für neue Richtlinien oder Ausnahmen:

     Klicken Sie auf **Hinzufügen**.
   - Für bereits vorhandene Richtlinien oder Ausnahmen:
     a. Klicken Sie auf den Namen der Richtlinie oder Ausnahme.

b. Klicken Sie auf die Registerkarte **Konten**.

3. Wählen Sie eine der folgenden Optionen:
   - **Alle Benutzer**: Diese Richtlinie oder Ausnahme wird auf alle Benutzer angewendet.
   - **Bestimmte Konten**: Zur Auswahl stehen Active Directory-Gruppen oder spezielle Trend Micro Apex Central-Gruppen.
4. Suchen Sie nach AD-Benutzern, -Gruppen, -Kontakten oder speziellen AD-Gruppen, markieren Sie sie und fügen Sie sie zur Liste „Ausgewählte Konten“ hinzu.
5. Suchen Sie nach AD-Users/Groups/Contacts/Special-Gruppen, markieren Sie sie und fügen Sie sie zur Liste „Ausgewählte Konten“ auf dem Bildschirm **Konten ausschließen** hinzu.

DLP-Ziele konfigurieren

Prozedur

1. Gehen Sie zum Bildschirm **Richtlinien für 'Prävention vor Datenverlust'**, indem Sie wie folgt navigieren:
   - Für Echtzeitsuche: **Prävention vor Datenverlust** > **DLP-Richtlinien**
   - Für manuelle Scans: **Manuelle Suche** > **Prävention vor Datenverlust**
   - Für zeitgesteuerte Suchläufe: **Zeitgesteuerte Suche** > **[Hinzufügen oder Bearbeiten]** > **Prävention vor Datenverlust**
2. Fügen Sie eine Richtlinie oder Ausnahme hinzu oder bearbeiten Sie sie:
   - Für neue Richtlinien oder Ausnahmen:
     a. Klicken Sie auf **Hinzufügen**.
     b. Wechseln Sie zum Fenster **Regel angeben**.
   - Für bereits vorhandene Richtlinien oder Ausnahmen:

a. Klicken Sie auf den Namen der Richtlinie oder Ausnahme.

b. Klicken Sie auf die Registerkarte **Ziel**.

3. Aktivieren Sie die Kontrollkästchen für die Zielbereiche der zu durchsuchenden E-Mail-Nachricht.

   Verfügbare Ziele sind:

   - **Header** (**Von**, **An** und **Cc**)
   - **Betreff**
   - **Text**
   - **Anhang**

4. Wählen Sie Vorlagen aus der Liste der verfügbaren Vorlagen aus und klicken Sie auf **Hinzufügen >>**, um die Vorlagen auf die Richtlinie anzuwenden.

   Hinweis

   Eine Richtlinie für Prävention vor Datenverlust erfordert die Auswahl mindestens einer Vorlage vor der Aktivierung.

5. Klicken Sie auf der Symbolleiste „Verfügbare DLP-Vorlage(n)“ auf **Hinzufügen**, um eine neue Vorlage zu erstellen, oder auf **Importieren**, um eine Vorlagendatei zu importieren.

DLP-Aktionen konfigurieren

Prozedur

1. Gehen Sie zum Bildschirm **Richtlinien für 'Prävention vor Datenverlust'**, indem Sie wie folgt navigieren:

   - Für Echtzeitsuche: **Prävention vor Datenverlust** > **DLP-Richtlinien**
   - Für manuelle Scans: **Manuelle Suche** > **Prävention vor Datenverlust**

- Für zeitgesteuerte Suchläufe: **Zeitgesteuerte Suche** > **[Hinzufügen oder Bearbeiten]** > **Prävention vor Datenverlust**

2. Fügen Sie eine Richtlinie oder Ausnahme hinzu oder bearbeiten Sie sie:
   - Für neue Richtlinien oder Ausnahmen:
     a. Klicken Sie auf **Hinzufügen**.
     b. Wechseln Sie zum Fenster **Aktion angeben**.
   - Für bereits vorhandene Richtlinien oder Ausnahmen:
     a. Klicken Sie auf den Namen der Richtlinie oder Ausnahme.
     b. Klicken Sie auf die Registerkarte **Aktion**.
3. Wählen Sie eine von Trend Micro Apex Central durchzuführende Aktion aus, wenn unerwünschter Inhalt gefunden wird.
4. So benachrichtigen Sie bestimmte Personen:
   - Aktivieren Sie das Kontrollkästchen **An den Vorgesetzten des Absenders weiterleiten**.
   - Aktivieren Sie das Kontrollkästchen **Weiterleiten an bestimmte E-Mail-Adresse(n)** und geben Sie die E-Mail-Adresse der Empfänger ein.
5. Geben Sie an, ob im Fall einer durchgeführten Aktion Benachrichtigungen gesendet werden sollen, indem Sie **Benachrichtigen** oder **Nicht benachrichtigen** auswählen.
6. Konfigurieren Sie **Erweiterte Optionen** nach Bedarf.

DLP-Benachrichtigungen konfigurieren

Prozedur

1. Gehen Sie zum Bildschirm **Richtlinien für 'Prävention vor Datenverlust'**, indem Sie wie folgt navigieren:

- Für Echtzeitsuche: **Prävention vor Datenverlust** > **DLP-Richtlinien**
- Für manuelle Scans: **Manuelle Suche** > **Prävention vor Datenverlust**
- Für zeitgesteuerte Suchläufe: **Zeitgesteuerte Suche** > **[Hinzufügen oder Bearbeiten]** > **Prävention vor Datenverlust**

2. Fügen Sie eine Richtlinie oder Ausnahme hinzu oder bearbeiten Sie sie:
   - Für neue Richtlinien oder Ausnahmen:
     a. Klicken Sie auf **Hinzufügen**.
     b. Wechseln Sie zum Fenster **Benachrichtigung angeben**.
   - Für bereits vorhandene Richtlinien oder Ausnahmen:
     a. Klicken Sie auf den Namen der Richtlinie oder Ausnahme.
     b. Klicken Sie auf die Registerkarte **Benachrichtigung**.
3. Aktivieren Sie die Kontrollkästchen für die Personen, die von Trend Micro Apex Central benachrichtigt werden.
4. Klicken Sie auf **Details anzeigen**, um die Benachrichtigung für den jeweiligen Empfänger anzupassen.
5. Treffen Sie eine Auswahl aus den Benachrichtigungsoptionen.
6. Klicken Sie auf **In das Windows-Ereignisprotokoll schreiben**, damit Trend Micro Apex Central die Benachrichtigung in ein Windows-Ereignisprotokoll schreibt.

DLP-Richtlinie aktivieren

Prozedur

1. Gehen Sie zum Bildschirm **Richtlinien für 'Prävention vor Datenverlust'**, indem Sie wie folgt navigieren:
   - Für Echtzeitsuche: **Prävention vor Datenverlust** > **DLP-Richtlinien**

- Für manuelle Scans: **Manuelle Suche** > **Prävention vor Datenverlust**
- Für zeitgesteuerte Suchläufe: **Zeitgesteuerte Suche** > **[Hinzufügen oder Bearbeiten]** > **Prävention vor Datenverlust**

2. Fügen Sie eine Richtlinie hinzu oder bearbeiten Sie sie, bevor Sie Folgendes aktivieren:
   - Für neue Richtlinien:
     a. Klicken Sie auf **Hinzufügen**.
     b. Navigieren Sie zum Fenster **Name und Priorität**.
   - Für bereits vorhandene Richtlinien:

     Klicken Sie auf den Namen der Richtlinie.
3. Aktivieren Sie diese Richtlinie oder Ausnahme.
4. Geben Sie den Namen Ihrer Richtlinie in das Feld **Name der Richtlinie** ein.
5. Geben Sie die Priorität an.
   - Für neue Richtlinien:

     Geben Sie die Priorität der Richtlinie im Bereich **Priorität** an.
   - Für bereits vorhandene Richtlinien:
     a. Aktivieren Sie das Kontrollkästchen neben dem Namen der Richtlinie oder Ausnahme in der Liste.
     b. Klicken Sie auf **Neu ordnen**.
     c. Geben Sie eine Prioritätsnummer in das Feld **Priorität** ein.
     d. Klicken Sie auf **Neue Anordnung speichern**.
6. Klicken Sie auf **Save**.

Teil XV

Widgets für Smart Protection Server

Kapitel 36

Dashboard-Widgets für Smart Protection Server

Dieser Abschnitt enthält Hilfethemen für die im Trend Micro Apex Central unterstützten Smart Protection Server-Dashboard-Widgets.

Es werden folgende Themen behandelt:

Aktive Benutzer der File Reputation

Das Widget 'Aktive Benutzer' zeigt die Anzahl der Benutzer an, die File Reputation-Abfragen an den Smart Protection Server gesendet haben. Jeder einzelne Clientcomputer zählt als aktiver Benutzer.

Hinweis

Dieses Widget zeigt Informationen in einer 2D-Grafik an und wird stündlich aktualisiert. Zum Aktualisieren der Daten können Sie auch jederzeit auf das Aktualisierungssymbol ( ) klicken.

TABELLE 36-1. Widget-Informationen

DATEN	BESCHREIBUNG
Benutzer	Anzahl der Benutzer, die Abfragen an Smart Protection Server Computer gesendet haben.
Datum	Datum der Abfrage.

Aktive Benutzer der Web Reputation

Das Widget 'Aktive Benutzer' zeigt die Anzahl der Benutzer an, die Web-Reputation-Abfragen an den Smart Protection Server gesendet haben. Jeder einzelne Clientcomputer zählt als aktiver Benutzer.

Hinweis

Dieses Widget zeigt Informationen in einer 2D-Grafik an und wird alle 5 Minuten aktualisiert. Sie können auch jederzeit auf das Symbol "Aktualisieren" ( ) klicken, um die Daten zu aktualisieren.

Tabelle 36-2. Widget-Informationen

Daten	Beschreibung
Benutzer	Anzahl der Benutzer, die Abfragen an Smart Protection Server Computer gesendet haben.
Datum	Datum der Abfrage.

Bericht über HTTP-Datenverkehr der File Reputation

Das Widget 'Bericht über HTTP-Datenverkehr' zeigt die Gesamtmenge des Netzwerkdatenverkehrs, der über von Clients generierte File Reputation-Abfragen an den Smart Protection Server gesendet wurde, in Kilobyte (KB) an. Die Daten in diesem Widget werden stündlich aktualisiert. Sie können auch jederzeit auf das Symbol zum Aktualisieren ( ) klicken, um die Daten zu aktualisieren.

Tabelle 36-3. Widget-Informationen

Daten	Beschreibung
Datenverkehr (KB)	Der durch Abfragen entstehende Datenverkehr im Netzwerk.
Datum	Datum der Abfragen.

Bericht über HTTP-Datenverkehr der Web Reputation

Das Widget 'Bericht über HTTP-Datenverkehr' zeigt die Gesamtmenge des Netzwerkdatenverkehrs, der über von Clients generierte Web-Reputation-Abfragen an den Smart Protection Server gesendet wurde, in Kilobyte (KB) an. Die Daten in diesem Widget werden stündlich aktualisiert. Sie können auch jederzeit auf das Symbol zum Aktualisieren ( ) klicken, um die Daten zu aktualisieren.

Tabelle 36-4. Widget-Informationen

Daten	Beschreibung
Datenverkehr (KB)	Der durch Abfragen entstehende Datenverkehr im Netzwerk.
Datum	Datum der Abfragen.

Echtzeitsuche - Status

Verwenden Sie das Widget „Echtzeitsuche - Status“, um den Status von Smart Protection Server zu überwachen.

Hinweis

Wenn dieses Widget in der Zusammenfassung angezeigt wird, läuft die Sitzung der Produktkonsole nicht ab. Der Computerstatus wird einmal pro Minute aktualisiert, was bedeutet, dass die Sitzung aufgrund der an den Server gesendeten Abfragen nicht abläuft. Die Sitzung läuft allerdings dennoch ab, wenn die Registerkarte ohne das Widget angezeigt wird.

Tabelle 36-5. Widget-Informationen

Daten	Beschreibung
Dienst	Vom Smart Protection Server bereitgestellte Dienste.
Protokoll	Hier werden die von Diensten unterstützten Protokolle angezeigt. File Reputation unterstützt HTTP- und HTTPS-Protokolle. Web Reputation unterstützt HTTP. HTTPS bietet eine sicherere Verbindung, während HTTP weniger Bandbreite benötigt.
Host	Adressen des File-Reputation- und Web-Reputation-Diensts. Diese Adressen werden mit Trend Micro-Produkten verwendet, die Smart Protection Server-Computer unterstützen. Die Adressen werden zum Konfigurieren von Verbindungen mit Smart Protection Server-Computern verwendet.

Daten	Beschreibung
Computerstatus	Die folgenden Punkte werden unter "Status" angezeigt: • **File-Reputation-Abfrage**: Zeigt an, ob File Reputation erwartungsgemäß funktioniert. • **Web-Reputation-Abfrage**: Zeigt an, ob Web Reputation erwartungsgemäß funktioniert. • **ActiveUpdate**: Zeigt an, ob ActiveUpdate erwartungsgemäß funktioniert. • **Durchschnittliche CPU-Auslastung**: Zeigt die durchschnittliche, vom Kernel generierte Computerauslastung während der letzten 1, 5 und 15 Minuten an. • **Freier Arbeitsspeicher**: Zeigt die verfügbare physische Speicherkapazität des Computers an. • **Belegung der Auslagerungsplatte**: Zeigt die Belegung der Auslagerungsplatte an. • **Freier Speicher**: Zeigt den verfügbaren Speicherplatz auf der Festplatte des Computers an.

Die 10 am häufigsten infizierten Computer für File Reputation

Dieses Widget zeigt die IP-Adressen der 10 häufigsten Computer an, die als infiziert klassifiziert wurden, nachdem der Smart Protection Server einen bekannten Virus aus der File-Reputation-Abfrage empfangen hat. Die Informationen in diesem Widget werden in einer Tabelle angezeigt, die die IP-Adresse des jeweiligen Computers und die Gesamtzahl der Funde auf jedem Computer enthält. Die Informationen in diesem Widget werden stündlich aktualisiert. Sie können aber auch jederzeit auf das Symbol zum Aktualisieren ( ) klicken, um die Informationen zu aktualisieren.

Mit diesem Widget ermitteln Sie, auf welchen Computern in Ihrem Netzwerk die meisten Virenvorfälle vorkommen.

Hinweis

Wenn Sie mehrere Smart Protection Server in diesem Widget aktivieren, berechnet das Widget die Gesamtzahl der Funde auf dem ausgewählten Smart Protection Server und zeigt die zehn am häufigsten infizierten Smart Protection Server Computer in der Liste an.

TABELLE 36-6. Widget-Informationen

DATEN	BESCHREIBUNG
IP	Die IP-Adresse des Computers.
Funde	Die Anzahl der von diesem Computer erkannten Sicherheitsbedrohungen.

Die 10 am häufigsten gesperrten Computer für Web Reputation

Dieses Widget zeigt die IP-Adressen der 10 häufigsten Computer an, die als gesperrt klassifiziert wurden, nachdem der Smart Protection Server eine URL für eine Web-Reputation-Abfrage empfangen hat. Die Informationen in diesem Widget werden in einer Tabelle angezeigt, die die IP-Adresse des jeweiligen Computers und die Gesamtzahl der gesperrten URLs auf jedem Computer enthält. Die Informationen in diesem Widget werden täglich aktualisiert. Sie können aber auch jederzeit auf das Symbol zum Aktualisieren ( ) klicken, um die Informationen zu aktualisieren.

Mit diesem Widget ermitteln Sie, von welchen Computern in Ihrem Netzwerk aus am häufigsten auf gesperrte Websites zugegriffen wird.

Hinweis

Wenn Sie mehrere Smart Protection Server in diesem Widget aktivieren, berechnet das Widget die Gesamtzahl der Funde auf dem ausgewählten Smart Protection Server und zeigt die zehn am häufigsten gesperrten Smart Protection Server Computer in der Liste an.

TABELLE 36-7. Widget-Informationen

DATEN	BESCHREIBUNG
IP	Die IP-Adresse des Computers.
Funde	Die Anzahl der auf diesem Computer gesperrten URLs.

Teil XVI

Trend Micro Mobile Security – Widgets und Richtlinien

Kapitel 37

Trend Micro Mobile Security Dashboard-Widgets

Dieser Abschnitt enthält Hilfethemen für die Dashboard-Widgets von Trend Micro Mobile Security, die in Trend Micro Apex Central unterstützt werden.

Es werden folgende Themen behandelt:

Zustandsstatus von Android-Geräten

Dieses Widget zeigt einen Überblick über den Zustandsstatus der registrierten Android-Mobilgeräte an.

Der Status **Nicht infiziert** gibt an, dass das Android-Mobilgerät beim Mobile Security Management Server angemeldet ist und dass alle Komponenten und Richtlinien auf dem Android-Mobilgerät auf dem neuesten Stand sind.

Status	Beschreibung
Nicht infiziert	Anzahl der nicht infizierten Android-Mobilgeräte
Infiziert	Anzahl der infizierten Android-Mobilgeräte

Wählen Sie **Alle** oder den Namen der Gruppe in der Dropdown-Liste aus, um die Informationen der entsprechenden Geräte anzuzeigen.

Verschlüsselungsstatus des Android Gerätes – Überblick – Widget

Dieses Widget zeigt einen Überblick über den Verschlüsselungsstatus registrierter Android-Mobilgeräte an.

Status	Beschreibung
Verschlüsselt	Anzahl der verschlüsselten Android-Mobilgeräte
Nicht verschlüsselt	Anzahl der nicht verschlüsselten Android-Mobilgeräte

Wählen Sie **Alle** oder den Namen der Gruppe in der Dropdown-Liste aus, um die Informationen der entsprechenden Geräte anzuzeigen.

Android-Betriebssystemversionen – Überblick – Widget

Dieses Widget zeigt einen Überblick über die auf registrierten Android-Mobilgeräten installierten Betriebssystemversionen.

Wählen Sie **Alle** oder den Namen der Gruppe in der Dropdown-Liste aus, um die Informationen der entsprechenden Geräte anzuzeigen.

Root-Status von Android-Geräten – Überblick – Widget

Dieses Widget zeigt einen Überblick über den Root-Status registrierter Android-Mobilgeräte an.

Status	Beschreibung
Mit Root-Zugriff	Anzahl der Mobilgeräte mit Root-Status
Kein Root-Zugriff	Anzahl der Mobilgeräte ohne Root-Status

Wählen Sie **Alle** oder den Namen der Gruppe in der Dropdown-Liste aus, um die Informationen der entsprechenden Geräte anzuzeigen.

Sicherheitsstatus von Android-Geräten – Widget

Dieses Widget zeigt einen Überblick über den Sicherheitsstatus der registrierten Android-Mobilgeräte an.

- Nicht durchsucht
- Gefährlich
- Geschützt
- Gefährlich

Wählen Sie **Alle** oder den Namen der Gruppe in der Dropdown-Liste aus, um die Informationen der entsprechenden Geräte anzuzeigen.

Android-Malware-Suche – Überblick – Widget

Dieses Widget zeigt einen Ergebnisüberblick zur Malware-Suche auf allen installierten Android-Anwendungen an.

In diesem Widget werden die Ergebnisse in den folgenden Kategorien gruppiert:

- Unbekannt
- Potenziell unerwünschte Objekte
- Normal
- Malware

Wählen Sie **Alle** oder den Namen der Gruppe in der Dropdown-Liste aus, um die Informationen der entsprechenden Geräte anzuzeigen.

Suche nach geänderten Android-Anwendungen – Überblick – Widget

Dieses Widget zeigt einen Überblick über die Suchergebnisse der geänderten Anwendungen im Rahmen aller installierten Android-Anwendungen an.

In diesem Widget werden die Ergebnisse in den folgenden Kategorien gruppiert:

- Unbekannt
- Geändert
- Nicht geändert

Wählen Sie **Alle** oder den Namen der Gruppe in der Dropdown-Liste aus, um die Informationen der entsprechenden Geräte anzuzeigen.

Android Datenschutz-Lecksuche – Überblick – Widget

Dieses Widget zeigt einen Überblick über die Ergebnisse der Datenschutzsuche aller installierten Android-Anwendungen an.

In diesem Widget werden die Ergebnisse in den folgenden Kategorien gruppiert:

- Unbekannt
- Potenziell unerwünschte Objekte

- Normal
- Malware

Wählen Sie **Alle** oder den Namen der Gruppe in der Dropdown-Liste aus, um die Informationen der entsprechenden Geräte anzuzeigen.

Android-Schwachstellensuche – Überblick – Widget

Dieses Widget zeigt einen Überblick über die Suchergebnisse zu Schwachstellen auf allen installierten Android-Anwendungen an.

In diesem Widget werden die Ergebnisse in den folgenden Kategorien gruppiert:

- Unbekannt
- Normal
- Hoch
- Mittel

Wählen Sie **Alle** oder den Namen der Gruppe in der Dropdown-Liste aus, um die Informationen der entsprechenden Geräte anzuzeigen.

Status des Komponenten-Updates – Widget

Dieses Widget zeigt einen Überblick über den Geräteaktualisierungsstatus registrierter Mobilgeräte an.

Spalte	Beschreibung
Aktuelle Version	Aktuelle Versionsnummer des Agents für Mobilgeräte oder der Komponenten auf dem Mobile Security Management Server
Auf dem neuesten Stand	Anzahl der Mobilgeräte mit aktualisierten Versionen des Agents für Mobilgeräte oder Komponenten
Nicht aktuell	Anzahl der Mobilgeräte, die nicht aktuelle Komponenten nutzen

Spalte	Beschreibung
Update-Rate	Prozentsatz der Mobilgeräte mit der neuesten Version der Komponenten
Aktualisiert	Anzahl der Mobilgeräte mit den neuesten Versionen des Agents für Mobilgeräte
Nicht aktualisiert	Anzahl der Mobilgeräte, die nicht aktualisiert wurden, um die neuesten Versionen des Agents für Mobilgeräte zu verwenden
Upgrade-Rate	Prozentsatz der Mobilgeräte mit den neuesten Agents für Mobilgeäte

Cybersicherheit für Mobilgeräte – Neuigkeiten – Widget

Dieses Widget zeigt von Trend Micro veröffentlichte Neuigkeiten zur Cybersicherheit in Bezug auf Mobilgeräte an.

iOS-Geräte – Überblick über den Verschlüsselungsstatus – Widget

Dieses Widget zeigt einen Überblick über den Verschlüsselungsstatus registrierter iOS-Mobilgeräte an.

Status	Beschreibung
Verschlüsselt	Die Anzahl der verschlüsselten iOS-Mobilgeräte
Nicht verschlüsselt	Die Anzahl der nicht verschlüsselten iOS-Mobilgeräte

Wählen Sie **Alle** oder den Namen der Gruppe in der Dropdown-Liste aus, um die Informationen der entsprechenden Geräte anzuzeigen.

Zustandsstatus von iOS-Geräten – Widget

Dieses Widget zeigt einen Überblick über den Zustandsstatus der registrierten iOS-Geräte an.

Der Status **Nicht infiziert** gibt an, dass das iOS-Mobilgerät beim Mobile Security Management Server angemeldet ist und dass alle Komponenten und Richtlinien auf dem iOS-Mobilgerät auf dem neuesten Stand sind.

Status	Beschreibung
Nicht infiziert	Die Anzahl der nicht infizierten iOS-Mobilgeräte
Infiziert	Die Anzahl der infizierten iOS-Mobilgeräte

Wählen Sie **Alle** oder den Namen der Gruppe in der Dropdown-Liste aus, um die Informationen der entsprechenden Geräte anzuzeigen.

Sicherheitsstatus von iOS-Geräten – Widget

Dieses Widget zeigt einen Überblick über den Sicherheitsstatus der registrierten iOS-Mobilgeräte an.

- Nicht durchsucht
- Gefährlich
- Geschützt
- Gefährlich

Wählen Sie **Alle** oder den Namen der Gruppe in der Dropdown-Liste aus, um die Informationen der entsprechenden Geräte anzuzeigen.

Jailbreak-Status von iOS-Geräten – Überblick – Widget

Dieses Widget zeigt einen Überblick über den Jailbreak-Status der registrierten iOS-Mobilgeräte an.

Status	Beschreibung
gehackt	Die Anzahl der Mobilgeräte mit Jailbreak
Kein Jailbreak	Die Anzahl der Mobilgeräte ohne Jailbreak

Wählen Sie **Alle** oder den Namen der Gruppe in der Dropdown-Liste aus, um die Informationen der entsprechenden Geräte anzuzeigen.

iOS-Betriebssystemversionen – Überblick – Widget

Dieses Widget zeigt einen Überblick über die auf registrierten iOS-Mobilgeräten installierten Betriebssystemversionen.

Wählen Sie **Alle** oder den Namen der Gruppe in der Dropdown-Liste aus, um die Informationen der entsprechenden Geräte anzuzeigen.

iOS-Malware-Suche – Überblick – Widget

Dieses Widget zeigt einen Überblick über die Malware-Suchergebnisse zu allen installierten iOS-Anwendungen an.

In diesem Widget werden die Ergebnisse in den folgenden Kategorien gruppiert:

- Unbekannt
- Malware
- Normal

Wählen Sie **Alle** oder den Namen der Gruppe in der Dropdown-Liste aus, um die Informationen der entsprechenden Geräte anzuzeigen.

Mobilgerät, App-Kontrollstatus – Überblick – Widget

Dieses Widget zeigt einen Überblick über den Anwendungskontrollstatus registrierter Mobilgeräte an.

Status	Beschreibung
Konform	Die Anzahl der Mobilgeräte, die die Konformitätsrichtlinie und die Anwendungskontrollrichtlinie von Mobile Security einhalten
Nicht konform	Die Anzahl der Mobilgeräte, die die Konformitätsrichtlinie und die Anwendungskontrollrichtlinie von Mobile Security nicht einhalten

Wählen Sie **Alle** oder den Namen der Gruppe in der Dropdown-Liste aus, um die Informationen der entsprechenden Geräte anzuzeigen.

Mobilgeräte – Überblick über den Verschlüsselungsstatus – Widget

Dieses Widget zeigt einen Überblick über den Verschlüsselungsstatus registrierter Mobilgeräte an.

Status	Beschreibung
Verschlüsselt	Anzahl der Mobilgeräte, die verschlüsselt sind
Nicht verschlüsselt	Anzahl der Mobilgeräte, die nicht verschlüsselt sind

Wählen Sie **Alle** oder den Namen der Gruppe in der Dropdown-Liste aus, um die Informationen der entsprechenden Geräte anzuzeigen.

Zustandsstatus von Mobilgeräten – Widget

Dieses Widget zeigt einen Überblick über den Zustandsstatus registrierter Mobilgeräte an.

Status	Beschreibung
Nicht infiziert	Das Gerät ist beim Mobile Security Management Server angemeldet, und die Komponenten und Richtlinien auf dem Mobilgerät sind auf dem neuesten Stand
Nicht konform	Das Gerät wurde beim Mobile Security Management Server angemeldet, entspricht aber nicht den Serverrichtlinien
Nicht synchronisiert	Das Gerät wurde beim Mobile Security Management Server angemeldet, aber entweder die Komponenten oder die Richtlinien sind nicht auf dem neuesten Stand
Inaktiv	Das Gerät wurde noch nicht beim Mobile Security Management Server angemeldet

Wählen Sie **Alle** oder den Namen der Gruppe in der Dropdown-Liste aus, um die Informationen der entsprechenden Geräte anzuzeigen.

Jailbreak-Status von Mobilgeräten – Überblick – Widget

Dieses Widget zeigt einen Überblick über den Jailbreak-Status der registrierten Mobilgeräte an.

Status	Beschreibung
gehackt	Die Anzahl der Mobilgeräte mit Jailbreak
Kein Jailbreak	Die Anzahl der Mobilgeräte ohne Jailbreak

Wählen Sie **Alle** oder den Namen der Gruppe in der Dropdown-Liste aus, um die Informationen der entsprechenden Geräte anzuzeigen.

Mobilgeräte-Betriebssystemversionen – Überblick – Widget

Dieses Widget zeigt einen Überblick über die auf registrierten Mobilgeräten installierten Betriebssystemversionen.

Betriebssystem	Beschreibung
Android	Anzahl der registrierten Android-Mobilgeräte
iOS	Anzahl der registrierten iOS-Mobilgeräte
Windows Phone	Anzahl der registrierten Windows Phone-Mobilgeräte

Wählen Sie **Alle** oder den Namen der Gruppe in der Dropdown-Liste aus, um die Informationen der entsprechenden Geräte anzuzeigen.

Suche nach Ransomware auf Mobilgeräten – Überblick – Widget

Dieses Widget zeigt einen Überblick über die Suchergebnisse zu Ransomware im Rahmen aller installierten Android-Anwendungen an.

Das Widget gruppiert die Ergebnisse nach mobilem Betriebssystem.

Wählen Sie **Alle** oder den Namen der Gruppe in der Dropdown-Liste aus, um die Informationen der entsprechenden Geräte anzuzeigen.

Sicherheitsstatus von Mobilgeräten – Widget

Dieses Widget zeigt einen Überblick über den Sicherheitsstatus registrierter Mobilgeräte an.

- Nicht durchsucht
- Gefährlich
- Geschützt
- Gefährlich

Wählen Sie **Alle** oder den Namen der Gruppe in der Dropdown-Liste aus, um die Informationen der entsprechenden Geräte anzuzeigen.

Mobilgeräteanbieter – Überblick – Widget

Dieses Widget zeigt einen Überblick über die Mobilgeräteanbieter für registrierte Mobilgeräte an.

Wählen Sie **Alle** oder den Namen der Gruppe in der Dropdown-Liste aus, um die Informationen der entsprechenden Geräte anzuzeigen.

Richtlinienaktualisierungsstatus – Überblick – Widget

Dieses Widget zeigt einen Überblick über den Richtlinienaktualisierungsstatus registrierter Mobilgeräte an.

Status	Beschreibung
Auf dem neuesten Stand	Anzahl der Mobilgeräte, die mit einer aktualisierten Version oder aktualisierten Komponenten des Agents für mobile Geräte ausgeführt werden
Nicht aktuell	Anzahl der Mobilgeräte, die mit veralteten Komponenten ausgeführt werden

Wählen Sie **Alle** oder den Namen der Gruppe in der Dropdown-Liste aus, um die Informationen der entsprechenden Geräte anzuzeigen.

Zustandsstatus der Serverkomponente – Überblick – Widget

Dieses Widget zeigt den Aktualisierungsstatus der Serverkomponenten und ihre Versionsnummern an.

Spalte	Beschreibung
Server	Name des Moduls
Adresse	Domänenname oder IP-Adresse des Computers, auf dem das Modul gehostet wird
Aktuelle Version	Versionsnummer der installierten Mobile Security Management Server-Module
Zuletzt aktualisiert	Datum und Uhrzeit des letzten Updates

Netzbetreiber – Überblick – Widget

Dieses Widget zeigt einen Überblick über die von registrierten Android-Mobilgeräten verwendeten Netzbetreiber an.

Wählen Sie **Alle** oder den Namen der Gruppe in der Dropdown-Liste aus, um die Informationen der entsprechenden Geräte anzuzeigen.

Die 10 am häufigsten installierten Anwendungen – Widget

Dieses Widget zeigt die Liste der zehn am häufigsten installierten Anwendungen auf registrierten Mobilgeräten an. Wählen Sie **Alle** oder den Namen der Gruppe in der Dropdown-Liste aus, um die Informationen der entsprechenden Geräte anzuzeigen.

Die fünf am häufigsten erkannten Android-Ransomware-Programme – Widget

Dieses Widget zeigt die Liste der fünf am häufigsten von Mobile Security erkannten Android-Ransomware-Programme basierend auf der Häufigkeit an, mit der die angegebene Ransomware erkannt wurde. Wählen Sie **Alle** oder den Namen der Gruppe in der Dropdown-Liste aus, um die Informationen der entsprechenden Geräte anzuzeigen.

Die 5 am häufigsten gesperrten Websites – Widget

Dieses Widget zeigt die Liste der fünf häufigsten von Mobile Security gesperrten Websites basierend auf der Häufigkeit an, mit der auf die jeweilige Site zugegriffen wurde. Wählen Sie **Alle** oder den Namen der Gruppe in der Dropdown-Liste aus, um die Informationen der entsprechenden Geräte anzuzeigen.

Fünf häufigste erkannte iOS-Ransomware-Programme

Dieses Widget zeigt die Liste der fünf am häufigsten von Mobile Security erkannten iOS-Ransomware-Programme basierend auf der Häufigkeit an, mit der die angegebene Ransomware erkannt wurde. Wählen Sie **Alle** oder den Namen der Gruppe in der Dropdown-Liste aus, um die Informationen der entsprechenden Geräte anzuzeigen.

Die 5 häufigsten Malware-Funde – Widget

Dieses Widget zeigt die Liste der fünf am häufigsten von Mobile Security erkannten Malware-Programme basierend auf der Häufigkeit an, mit der die angegebene Malware erkannt wurde. Wählen Sie **Alle** oder den Namen der Gruppe in der Dropdown-Liste aus, um die Informationen der entsprechenden Geräte anzuzeigen.

Windows Phone – Überblick über den Verschlüsselungsstatus von Geräten – Widget

Dieses Widget zeigt einen Überblick über den Verschlüsselungsstatus registrierter Windows Phone-Mobilgeräte an.

Status	Beschreibung
Verschlüsselt	Anzahl der verschlüsselten Windows Phone-Mobilgeräte
Nicht verschlüsselt	Anzahl der unverschlüsselten Windows Phone-Mobilgeräte

Wählen Sie **Alle** oder den Namen der Gruppe in der Dropdown-Liste aus, um die Informationen der entsprechenden Geräte anzuzeigen.

Zustandsstatus von Windows Phone-Geräten – Widget

Dieses Widget zeigt einen Überblick über den Zustandsstatus registrierter Windows Phone-Mobilgeräte an.

Der Status **Nicht infiziert** gibt an, dass das Windows Phone-Mobilgerät am Mobile Security-Management Server angemeldet ist und alle Komponenten und Richtlinien auf dem Windows Phone-Mobilgerät aktuell sind.

Status	Beschreibung
Nicht infiziert	Anzahl der nicht infizierten Windows Phone-Mobilgeräte
Infiziert	Anzahl der infizierten Windows Phone-Mobilgeräte

Wählen Sie **Alle** oder den Namen der Gruppe in der Dropdown-Liste aus, um die Informationen der entsprechenden Geräte anzuzeigen.

Windows Phone-Betriebssystemversionen – Überblick – Widget

Dieses Widget zeigt einen Überblick über die Betriebssystemversionen, die auf registrierten Windows Phone-Mobilgeräten installiert sind.

Wählen Sie **Alle** oder den Namen der Gruppe in der Dropdown-Liste aus, um die Informationen der entsprechenden Geräte anzuzeigen.

Kapitel 38

Trend Micro Mobile Security-Richtlinieneinstellungen

In diesem Abschnitt wird erläutert, wie Sicherheitsrichtlinien für Mobile Security über die Apex Central-Verwaltungskonsole konfiguriert werden.

Geräte mit Richtlinien schützen

Sie können Sicherheitsrichtlinien für eine Mobile Security-Gruppe auf dem Management Server konfigurieren. Diese Richtlinien gelten für alle Mobilgeräte in der Gruppe. Sie können Sicherheitsrichtlinien auf alle Mobile Security-Gruppen anwenden, indem Sie die Gruppe **Mobilgeräte** (die Stammgruppe) auswählen. Die folgende Tabelle enthält die in Mobile Security verfügbaren Sicherheitsrichtlinien.

TABELLE 38-1. Sicherheitsrichtlinien in Mobile Security

RICHTLINIENGRUPPE	RICHTLINIE	RECHERCHE
Allgemein	Allgemeine Richtlinie	Informationen zum Verteilungsmodus Vollversion finden Sie unter *Allgemeine Richtlinie im Verteilungsmodus der Vollversion auf Seite 38-4*. Informationen zum Verteilungsmodus Sicherheitssuche finden Sie unter *Allgemeine Richtlinie im Verteilungsmodus der Sicherheitssuche auf Seite 38-6*.
Bereitstellung	Wi-Fi-Richtlinie	Weitere Informationen finden Sie unter *Wi-Fi-Richtlinie auf Seite 38-6*.
	Exchange ActiveSync-Richtlinie	Weitere Informationen finden Sie unter *Exchange ActiveSync-Richtlinie auf Seite 38-7*.
	Zertifikatrichtlinie	Weitere Informationen finden Sie unter *Zertifikatrichtlinie auf Seite 38-7*.
	VPN-Richtlinie	Weitere Informationen finden Sie unter *VPN-Richtlinie auf Seite 38-7*.

Richtliniengruppe	Richtlinie	Recherche
	Allgemeine HTTP-Proxy-Richtlinie	Weitere Informationen finden Sie unter *Allgemeine HTTP-Proxy-Richtlinie auf Seite 38-7*.
	Single Sign-On-Richtlinie	Weitere Informationen finden Sie unter *Single Sign-On-Richtlinie auf Seite 38-7*.
	Mobilfunknetzrichtlinie	Weitere Informationen finden Sie unter *Mobilfunknetzrichtlinie auf Seite 38-9*.
	AirPlay/AirPrint-Richtlinie	Weitere Informationen finden Sie unter *AirPlay/AirPrint-Richtlinie auf Seite 38-9*.
	Design-Richtlinie	Weitere Informationen finden Sie unter *Design-Richtlinie auf Seite 38-9*.
	Richtlinie für verwaltete Domänen	Weitere Informationen finden Sie unter *Richtlinie für verwaltete Domänen auf Seite 38-9*.
Gerätesicherheit	Sicherheitsrichtlinie	Informationen zur Sicherheitsrichtlinie im Verteilungsmodus Vollversion finden Sie unter *Sicherheitsrichtlinie im Bereitstellungsmodus der Vollversion auf Seite 38-10*. Informationen zur Sicherheitsrichtlinie im Verteilungsmodus Sicherheitssuche finden Sie unter *Sicherheitsrichtlinie im Bereitstellungsmodus der Sicherheitssuche auf Seite 38-13*.
	Spamschutzrichtlinie	Weitere Informationen finden Sie unter *Spamschutzrichtlinie auf Seite 38-15*.

Richtliniengruppe	Richtlinie	Recherche
	Anruffilterrichtlinie	Weitere Informationen finden Sie unter *Anruffilterrichtlinie auf Seite 38-19*.
	Richtlinie zum Schutz vor Internet-Bedrohungen	Weitere Informationen finden Sie unter *Richtlinie zum Schutz vor Internet-Bedrohungen auf Seite 38-21*.
Geräte	Kennwortrichtlinie	Weitere Informationen finden Sie unter *Kennwortrichtlinie auf Seite 38-24*.
	Richtlinie zur Funktionssperre	Weitere Informationen finden Sie unter *Richtlinie zur Funktionssperre auf Seite 38-24*.
	Konformitätsrichtlinie	Weitere Informationen finden Sie unter *Konformitätsrichtlinie auf Seite 38-47*.
Anwendungsverwaltung	Richtlinie zur Anwendungsüberwachung und -kontrolle	Weitere Informationen finden Sie unter *Richtlinie zur Anwendungsüberwachung und -kontrolle auf Seite 38-48*.
	Richtlinie zum Volumenkaufprogramm	Weitere Informationen finden Sie unter *Richtlinie zum Volumenkaufprogramm auf Seite 38-51*.
Samsung KNOX	Container-Richtlinie	Weitere Informationen finden Sie unter *Container -Richtlinie auf Seite 38-53*.

Allgemeine Richtlinie im Verteilungsmodus der Vollversion

Die allgemeine Richtlinie bietet die gemeinsamen Sicherheitsrichtlinien für Mobilgeräte. Um allgemeine Sicherheitseinstellungen zu konfigurieren, klicken Sie auf **Richtlinien**, dann auf den Namen der Richtlinie und anschließend auf **Allgemeine Richtlinie**.

- **Benutzerrechte**: Sie können die Funktion, die es Benutzern ermöglicht, den Agent für Mobilgeräte zu deinstallieren, aktivieren oder deaktivieren. Darüber hinaus können Sie auswählen, ob Benutzer Einstellungen für den Mobile Security Geräte-Agent konfigurieren können sollen.

  Die folgende Liste enthält die Funktionen, die mit dem Deinstallationsschutz verbunden sind:

  - Deinstallationsschutz über die Verwaltungskonsole aktivieren/deaktivieren
  - Das Kennwort muss mindestens 6 und darf höchstens 12 Zeichen umfassen. Das Kennwort darf Ziffern, Buchstaben und/oder Symbole enthalten.
  - Das Kennwort kann für jede Gruppe über die Verwaltungskonsole eingerichtet werden.

  Wenn Sie das Kontrollkästchen **Ermöglicht Benutzern, Mobile Security-Client-Einstellungen zu konfigurieren** nicht auswählen, können Benutzer die Einstellungen des Mobile Device Agent nicht ändern. Die Filterlisten für **Spamschutzrichtlinie**, **Anruffilterrichtlinie** und **Richtlinie zum Schutz vor Internet-Bedrohungen** werden jedoch nicht beeinflusst, wenn diese Option ausgewählt ist. Weitere Informationen finden Sie unter *Spamschutzrichtlinie auf Seite 38-15*, *Anruffilterrichtlinie auf Seite 38-19* und *Richtlinie zum Schutz vor Internet-Bedrohungen auf Seite 38-21*.

- **Einstellungen für Updates**: Sie können festlegen, dass der Mobile Security Management Server die Agents für Mobilgeräte benachrichtigt, wenn eine neue Komponente zum Update verfügbar ist. Sie können auch festlegen, dass die Agents für Mobilgeräte automatisch in regelmäßigen Abständen prüfen, ob Komponenten- oder Konfigurations-Updates auf dem Mobile Security Management Server vorhanden sind.
- **Protokolleinstellungen**: Wenn Mobile-Geräte-Agenten ein Sicherheitsrisiko erkennen, wie beispielsweise eine Malware auf dem

Android-Betriebssystem, wird ein Protokoll auf dem mobilen Gerät erstellt.

Allgemeine Richtlinie im Verteilungsmodus der Sicherheitssuche

Die allgemeine Richtlinie bietet die gemeinsamen Sicherheitsrichtlinien für Mobilgeräte. Um allgemeine Sicherheitseinstellungen zu konfigurieren, klicken Sie auf **Richtlinien**, dann auf den Namen der Richtlinie und anschließend auf **Allgemeine Richtlinie**.

- **Benutzerrechte**:
  - Sie können auswählen, ob Benutzer Einstellungen für den Mobile Security Geräte-Agent konfigurieren können sollen.

    Wenn Sie das Kontrollkästchen **Ermöglicht Benutzern, Mobile Security-Client-Einstellungen zu konfigurieren** nicht aktivieren, können Benutzer die Einstellungen des Mobile Device Agent nicht ändern. Die Filterlisten für **Richtlinie zum Schutz vor Internet-Bedrohungen** werden jedoch nicht beeinflusst, wenn diese Option ausgewählt ist. Weitere Informationen finden Sie unter *Richtlinie zum Schutz vor Internet-Bedrohungen auf Seite 38-21*.
  - Sie können festlegen, dass die Agents für Mobilgeräte automatisch in regelmäßigen Abständen prüfen, ob Komponenten- oder Konfigurations-Updates auf dem Mobile Security Management Server vorhanden sind.

Wi-Fi-Richtlinie

Mit Wi-Fi-Richtlinien können Sie Wi-Fi-Netzwerkinformationen Ihres Unternehmens auf Android- und iOS-Mobilgeräten bereitstellen, einschließlich des Netzwerknamens, des Sicherheitstyps und Kennworts.

Zum Konfigurieren von Einstellungen für Wi-Fi-Richtlinien klicken Sie auf **Richtlinien**, dann auf den Namen der Richtlinie und anschließend auf **Wi-Fi-Richtlinie**.

Exchange ActiveSync-Richtlinie

Mit Hilfe der Exchange ActiveSync-Richtlinie können Sie eine entsprechende Richtlinie für Ihre Organisation erstellen und an iOS-Mobilgeräte liefern.

Um die Exchange ActiveSync-Richtlinieneinstellungen zu konfigurieren, klicken Sie auf **Richtlinien**, dann auf den Name der Richtlinie und anschließend auf **Exchange ActiveSync-Richtlinie**.

Zertifikatrichtlinie

Mit einer Zertifikatrichtlinie können Sie Zertifikate importieren, die Sie auf iOS-Mobilgeräte verteilen müssen.

Um Richtlinieneinstellungen für Zertifikate zu konfigurieren, klicken Sie auf **Richtlinien**, dann auf den Namen der Richtlinie und anschließend auf **Zertifikatrichtlinie**.

VPN-Richtlinie

Mit Hilfe von VPN-Richtlinieneinstellungen können Sie eine VPN-Richtlinie für Ihr Unternehmen erstellen und diese auf iOS-Mobilgeräten zur Verfügung stellen.

Zum Konfigurieren von VPN-Richtlinieneinstellungen klicken Sie auf **Richtlinien**, dann auf den Namen der Richtlinie und anschließend auf **VPN-Richtlinie**

Allgemeine HTTP-Proxy-Richtlinie

Die allgemeine HTTP-Proxy-Richtlinie ermöglicht es Ihnen, die Proxy-Informationen Ihrer Organisation an Mobilgeräte zu übermitteln. Diese Richtlinie gilt nur für iOS-Mobilgeräte im überwachten Modus.

Um allgemeine HTTP-Proxy-Richtlinieneinstellungen zu konfigurieren, klicken Sie auf **Richtlinien**, dann auf den Name der Richtlinie und anschließend auf **Allgemeine HTTP-Proxy-Richtlinie**

Single Sign-On-Richtlinie

Mit Hilfe der SSO-Richtlinie (Single Sign-On) können Benutzer dieselben Anmeldedaten für verschiedene Anwendungen verwenden, einschließlich

Mobile Security und Anwendung aus dem App Store. Jede neue, mit SSO-Zertifizierung konfigurierte Anwendung überprüft Benutzerberechtigungen für Unternehmensressourcen und meldet Benutzer an, ohne von ihnen die erneute Eingabe der Kennwörter zu fordern.

Die SSO-Richtlinie enthält folgende Informationen:

- **Name**: der Kerberos-Prinzipalname.
- **Bereich**: der Kerberos-Bereichsname.

  Achten Sie beim Kerberos-Bereichsnamen auf ordnungsgemäße Großschreibung.
- **URL-Präfixe** (Optional): Liste der URLs, die abgeglichen werden müssen, damit ein Konto für die Kerberos-Authentifizierung über HTTP verwendet werden kann. Wenn dieses Feld leer ist, kann das Konto alle HTTP- und HTTPS-URLs abgleichen. Die URL-Abgleichs-Patterns müssen entweder mit HTTP oder HTTPS beginnen.

  Jeder Eintrag in dieser Liste muss ein URL-Präfix enthalten. Nur die URLs, die mit einer der Zeichenfolgen in einem Konto beginnen, dürfen auf das Kerberos-Ticket zugreifen. URL-Abgleichs-Patterns müssen das Schema enthalten. Zum Beispiel http://www.example.com/. Wenn ein Abgleichs-Pattern nicht auf / endet, wird der URL automatisch ein Schrägstrich (/) hinzugefügt.
- **Anwendungsbezeichner** (Optional): Liste der Anwendungsbezeichner, die das Konto verwenden dürfen. Ist das Feld leer, kann dieses Konto von allen Anwendungsbezeichnern verwendet werden.

  Das Array **Anwendungsbezeichner** muss Zeichenfolgen enthalten, die Anwendungspaket-IDs entsprechen. Diese Zeichenfolgen können genau übereinstimmen (z. B. com.mycompany.myapp) oder einen Präfixabgleich in der Paket-ID mit Hilfe des Platzhalterzeichens * angeben. Das Platzhalterzeichen muss nach einem Punkt (.) und darf nur am Ende einer Zeichenfolge (z. B. com.mycompany.*) angezeigt werden. Bei Verwendung eines Platzhalters wird jeder Anwendung, deren Paket-ID mit dem Präfix beginnt, Zugriff auf das Konto gewährt.

Zum Konfigurieren einer Single Sign-On-Richtlinie für iOS-Einstellungen klicken Sie auf **Richtlinien**, dann auf den Namen der Richtlinie und anschließend auf **Single Sign-On-Richtlinie**.

Mobilfunknetzrichtlinie

Mit Richtlinieneinstellungen für Mobilfunknetze können Sie Mobilfunknetzeinstellungen für Ihre Organisation konfigurieren und an iOS-Mobilgeräte liefern.

Um die Richtlinieneinstellungen für Mobilfunknetze zu konfigurieren, klicken Sie auf **Richtlinien**, dann auf den Namen der Richtlinie und anschließend auf **Mobilfunknetzrichtlinie**.

AirPlay/AirPrint-Richtlinie

AirPlay/AirPrint-Richtlinieneinstellungen ermöglichen Ihnen das Erstellen von AirPlay- und AirPrint-Richtlinien für Ihre Organisation und deren Verteilung auf iOS-Mobilgeräte.

Klicken Sie zum Konfigurieren von AirPlay- und/oder AirPrint-Richtlinieneinstellungen auf **Richtlinien**. Klicken Sie dann auf den Namen der Richtlinie und anschließend auf **AirPlay/AirPrint-Richtlinie**.

Design-Richtlinie

Mit Hilfe der Einstellungen für Design-Richtlinien können Sie Schriftarten verwenden und ein Hintergrundbild für den Start- und Sperrbildschirm von iOS-Mobilgeräten festlegen. Diese Richtlinie gilt für iOS-Mobilgeräte, die ausschließlich im überwachten Modus ausgeführt werden.

Zum Konfigurieren von Einstellungen für Design-Richtlinien klicken Sie auf **Richtlinien**, dann auf den Namen der Richtlinie und anschließend auf **Design-Richtlinie**.

Richtlinie für verwaltete Domänen

Mit der Richtlinie für verwaltete Domänen können Sie die E-Mail- und/oder Webdomänen konfigurieren, die Ihre Organisation verwaltet.

- Nicht gekennzeichnete E-Mail-Domänen: Wenn ein Benutzer eine E-Mail mit dem E-Mail-Client des Systems verfasst, wird jede eingegebene E-Mail-Adresse, die nicht den konfigurierten Domänen entspricht, in Rot hervorgehoben (markiert). Administratoren sollten die Verwendung dieser Funktion erwägen, um Benutzer zu warnen, die versehentlich versuchen, vertrauliche Informationen an nicht vertrauenswürdige E-Mail-Adressen zu senden.
- Verwaltete Safari Web-Domänen: Sie können festlegen, dass Dateien, die über Safari von bestimmten Domänen heruntergeladen werden, nur mit verwalteten Apps geöffnet werden können. Beispielsweise kann eine von 'internal.example.com' heruntergeladene PDF-Datei mit Adobe Reader (einer verwalteten App), aber nicht mit Dropbox (einer nicht verwalteten App) geöffnet werden. Dadurch wird die Containerisierung von Safari verbessert und die Nutzung als Enterprise-Browser ausgedehnt.

Wichtig

Sie müssen die folgenden iOS-Funktionen in der Richtlinie zur Funktionssperre deaktivieren. Andernfalls sind die Einstellungen der verwalteten Safari Web-Domänen nicht wirksam, da die heruntergeladenen Dateien mit anderen (nicht verwalteten) Apps geöffnet werden können:

- Dokumente über verwaltete Apps in anderen Apps (7.0 oder höher) öffnen
- Dokumente über andere Apps in verwalteten Apps (7.0 oder höher) öffnen

Um Richtlinieneinstellungen für verwaltete Domänen zu konfigurieren, klicken Sie auf **Richtlinien**, dann auf den Namen der Richtlinie und anschließend auf **Richtlinie für verwaltete Domänen**.

Sicherheitsrichtlinie im Bereitstellungsmodus der Vollversion

Sie können das **Sicherheitseinstellungen** vom **Sicherheitsrichtlinie**-Bildschirm aus konfigurieren.

Zum Konfigurieren von Einstellungen für die Sicherheitsrichtlinie klicken Sie auf **Richtlinien**, dann auf den Namen der Richtlinie und anschließend auf **Sicherheitsrichtlinie**.

In der folgenden Tabelle sind die verfügbaren Einstellungen für diese Richtlinie beschrieben.

TABELLE 38-2. Einstellungen der Sicherheitsrichtlinie

ABSCHNITT	VORGANG	BESCHREIBUNG	UNTERSTÜTZTES BETRIEBSSYSTEM FÜR MOBILGERÄTE
Sicherheitseinstellungen	**Nur installierte Anwendungen durchsuchen**	Wählen Sie diese Option, wenn Sie nur installierte Anwendungen durchsuchen möchten	
	Installierte Anwendungen und Dateien durchsuchen	Wählen Sie diese Option, wenn Sie installierte Anwendungen und andere auf dem Mobilgerät gespeicherte Dateien durchsuchen möchten. Wenn Sie diese Option wählen, geben Sie an, ob Sie nur APK-Dateien oder alle Dateien durchsuchen möchten.	
	Nach erfolgtem Pattern-Update durchsuchen	Aktivieren Sie diese Option, wenn Sie die Malware-Suche nach jedem Pattern-Update durchführen möchten.	

Abschnitt	Vorgang	Beschreibung	Unterstütztes Betriebssystem für Mobilgeräte
		Mobile Security führt nach jedem erfolgreichen Pattern-Update auf Android-Mobilgeräten automatisch eine Suche durch.	
	Facebook-Durchsuchung aktivieren	Aktivieren Sie diese Option, um die Facebook-Datenschutzeinstellungen zu durchsuchen. **Hinweis** Durch das Aktivieren der **Facebook-Suche** können Benutzer ihre Daten schützen und sicherstellen, dass sie nur Daten mit Personen teilen, denen sie vertrauen.	

Abschnitt	Vorgang	Beschreibung	Unterstütztes Betriebssystem für Mobilgeräte
Zeitplan durchsuchen	**Täglich**	Die Suche wird einmal pro Tag am angegebenen Tag zur **Startzeit** durchgeführt.	
	Wöchentlich	Die Suche wird einmal wöchentlich am angegebenen Tag zur **Startzeit** durchgeführt.	
	Monatlich	Die Suche wird einmal pro Monat am angegebenen Tag zur **Startzeit** durchgeführt.	

Sicherheitsrichtlinie im Bereitstellungsmodus der Sicherheitssuche

Sie können das **Sicherheitseinstellungen** vom **Sicherheitsrichtlinie**-Bildschirm aus konfigurieren.

Zum Konfigurieren von Einstellungen für die Sicherheitsrichtlinie klicken Sie auf **Richtlinien**, dann auf den Namen der Richtlinie und anschließend auf **Sicherheitsrichtlinie**.

In der folgenden Tabelle sind die verfügbaren Einstellungen für diese Richtlinie beschrieben.

TABELLE 38-3. Einstellungen der Sicherheitsrichtlinie

ABSCHNITT	VORGANG	BESCHREIBUNG	UNTERSTÜTZTES BETRIEBSSYSTEM FÜR MOBILGERÄTE
Sicherheitseinstellungen	**Nur installierte Anwendungen durchsuchen**	Wählen Sie diese Option, wenn Sie nur installierte Anwendungen durchsuchen möchten	
	Installierte Anwendungen und Dateien durchsuchen	Wählen Sie diese Option, wenn Sie installierte Anwendungen und andere auf dem Mobilgerät gespeicherte Dateien durchsuchen möchten. Wenn Sie diese Option wählen, geben Sie an, ob Sie nur APK-Dateien oder alle Dateien durchsuchen möchten.	
	Nach erfolgtem Pattern-Update durchsuchen	Aktivieren Sie diese Option, wenn Sie die Malware-Suche nach jedem Pattern-Update durchführen möchten. Mobile Security führt nach jedem erfolgreichen Pattern-Update auf Android-Mobilgeräten	

Abschnitt	Vorgang	Beschreibung	Unterstütztes Betriebssystem für Mobilgeräte
		automatisch eine Suche durch.	
Zeitplan durchsuchen	**Täglich**	Die Suche wird einmal pro Tag am angegebenen Tag zur **Startzeit** durchgeführt.	
	Wöchentlich	Die Suche wird einmal wöchentlich am angegebenen Tag zur **Startzeit** durchgeführt.	
	Monatlich	Die Suche wird einmal pro Monat am angegebenen Tag zur **Startzeit** durchgeführt.	

Spamschutzrichtlinie

Die Spamschutzrichtlinie in Mobile Security bietet Schutz vor WAP-Push-Spam und SMS-Textnachrichten.

Zum Konfigurieren von Einstellungen für Spamschutzrichtlinien klicken Sie auf **Richtlinien**, dann auf den Namen der Richtlinie und anschließend auf **Spamschutzrichtlinie**.

Richtlinien für SMS-Spamschutz

Diese Funktion bietet serverseitige Steuerung von SMS-Spamschutzrichtlinien. Die folgenden Funktionen sind für die Konfiguration von SMS-Spamschutzrichtlinien verfügbar:

- Aktivieren oder Deaktivieren von SMS-Spamschutz für Mobilgeräte

- Konfigurieren der Mobilgeräte zur Verwendung der Listen „Gesperrt“ und „Zulässig“ oder Deaktivieren der SMS-Anti-Spam-Funktion für Mobilgeräte.
- Eine Liste 'Zulässig' über die Verwaltungskonsole konfigurieren
- Eine Liste 'Gesperrt' über die Verwaltungskonsole konfigurieren

Weitere Informationen zur Konfiguration der Listen für gesperrte oder zulässige Filter finden Sie in der folgenden Tabelle.

Tabelle 38-4. Filtern der Listenkonfiguration für SMS-Spamschutzrichtlinie

Zentrale Steuerung	Benutzersteuerung	Beschreibung
Deaktiviert	Aktiviert	Der Benutzer kann die Liste 'Gesperrt'/'Zulässig' im Agent für Mobilgeräte bearbeiten. Mobile Security genehmigt die Nachrichten oder sperrt sie basierend auf folgender Priorität: 1. Liste 'Zulässig' im Agent für Mobilgeräte 2. Liste 'Gesperrt' im Agent für Mobilgeräte
Aktiviert	Deaktiviert	Der Benutzer darf die Liste „Gesperrt“/„Zulässig“ nur auf dem Mobilgerät-Agent bearbeiten. Mobile Security genehmigt die Nachrichten oder sperrt sie basierend auf folgender Priorität: 1. Liste „Zulässig“ oder „Gesperrt“ auf dem Server 2. Liste 'Zulässig' im Agent für Mobilgeräte 3. Liste 'Gesperrt' im Agent für Mobilgeräte

Zentrale Steuerung	Benutzersteuerung	Beschreibung
Aktiviert	Aktiviert	Der Benutzer kann die vom Administrator definierte Liste 'Gesperrt'/'Zulässig' anzeigen oder bearbeiten und auch die Liste 'Gesperrt'/'Zulässig' im Agent für Mobilgeräte verwenden. Wenn die Sicherheitsrichtlinien mit dem Agent für Mobilgeräte synchronisiert werden, werden die Filterlisten nicht synchronisiert. Alle übrigen Einstellungen werden gemäß den Richtlinien aktualisiert. Mobile Security genehmigt die Nachrichten oder sperrt sie basierend auf folgender Priorität: 1. Liste 'Zulässig' im Agent für Mobilgeräte 2. Liste 'Gesperrt' im Agent für Mobilgeräte 3. Liste „Zulässig“ oder „Gesperrt“ auf dem Server

Hinweis

Die Listen „Zulässig“ und „Gesperrt“ für SMS müssen folgendes Format verwenden: "[name1:]number1;[name2:]number2;...".

'name' darf nicht mehr als 30 Zeichen umfassen, während die Telefonnummer zwischen 4 und 20 Zeichen lang sein muss und die folgenden Zeichen enthalten darf: 0-9, +, -, #, (,) und Leerzeichen. Die Anzahl der Einträge darf maximal 200 betragen.

Spamschutzrichtlinie für WAP-Push

Diese Funktion bietet serverseitige Steuerung des WAP-Push-Schutzes. Wenn aktiviert, können Sie eine für WAP genehmigte Liste verwenden.

Hinweis

Die für WAP genehmigte Liste muss folgendes Format verwenden: "[name1:]number1;[name2:]number2;...".

'name' darf nicht mehr als 30 Zeichen umfassen, während die Telefonnummer zwischen 4 und 20 Zeichen lang sein muss und die folgenden Zeichen enthalten darf: 0-9, +, -, #, (,) und Leerzeichen. Die Anzahl der Einträge darf maximal 200 betragen.

Im Folgenden werden die Funktionen aufgeführt, die beim Konfigurieren von WAP-Push-Schutzrichtlinien zur Verfügung stehen:

- Aktivieren oder Deaktivieren von WAP-Push-Schutz für Mobilgeräte
- Konfigurieren der Mobilgeräte zur Verwendung einer genehmigten Liste oder Deaktivieren von WAP-Push-Schutz auf dem Mobilgerät
- Eine Liste 'Zulässig' über die Verwaltungskonsole konfigurieren
- Wenn der Administrator serverseitige Steuerung aktiviert hat, kann der Benutzer den vom Administrator festgelegten Typ des WAP-Push-Schutzes nicht ändern
- Wenn der Administrator serverseitige Steuerung deaktiviert und Benutzern erlaubt hat, Mobile Security-Einstellungen auf Mobilgeräten zu konfigurieren, kann der Benutzer die vom Administrator konfigurierte WAP-Push-Schutzliste weder anzeigen noch bearbeiten. Der Benutzer kann unter Umständen die private WAP-Push-Schutzliste auf dem Mobilgerät bearbeiten

Hinweis

Die persönlichen Einstellungen des Benutzers für Spam-Nachrichten werden gelöscht, nachdem die Spam-Schutzrichtlinie auf die Mobilgeräte-Agents angewendet wurde.

Anruffilterrichtlinie

Diese Funktion ermöglicht Ihnen die serverseitige Steuerung der Anruffilterrichtlinien. Um Richtlinieneinstellungen für Anruffilter zu konfigurieren, klicken Sie auf **Richtlinien**, dann auf den Namen der Richtlinie und anschließend auf **Filterrichtlinie**.

Die folgenden Funktionen sind verfügbar, wenn Sie die Anruffilterrichtlinien konfigurieren:

- Anruffilter für Mobilgeräte aktivieren oder deaktivieren
- Das Mobilgerät für die Verwendung einer Liste 'Gesperrt' oder einer Liste 'Zulässig' konfigurieren
- Eine Liste 'Zulässig' über die Verwaltungskonsole konfigurieren
- Eine Liste 'Gesperrt' über die Verwaltungskonsole konfigurieren

Weitere Informationen zur Konfiguration der Listen für gesperrte oder zulässige Filter finden Sie in der folgenden Tabelle.

Tabelle 38-5. Konfiguration der Filterliste für die Anruffilterrichtlinie

Zentrale Steuerung	Benutzersteuerung	Beschreibung
Deaktiviert	Aktiviert	Der Benutzer kann die Liste 'Gesperrt'/'Zulässig' im Agent für Mobilgeräte bearbeiten. Mobile Security sperrt URLs basierend auf den folgenden Prioritäten bzw. lässt diese entsprechend zu: 1. Liste 'Zulässig' im Agent für Mobilgeräte 2. Liste 'Gesperrt' im Agent für Mobilgeräte

Zentrale Steuerung	Benutzersteuerung	Beschreibung
Aktiviert	Deaktiviert	Der Benutzer darf die Liste 'Gesperrt'/'Zulässig' nur im Agent für Mobilgeräte bearbeiten. Mobile Security sperrt eingehende Anrufe basierend auf den folgenden Prioritäten bzw. lässt diese entsprechend zu: 1. Liste 'Gesperrt' auf Server 2. Liste 'Zulässig' im Agent für Mobilgeräte 3. Liste 'Gesperrt' im Agent für Mobilgeräte Sie können auch die serverseitige Kontrolle für ausgehende Anrufe auf Android-Mobilgeräten konfigurieren.
Aktiviert	Aktiviert	Der Benutzer kann die vom Administrator definierte Liste 'Gesperrt'/'Zulässig' anzeigen oder bearbeiten und auch die Liste 'Gesperrt'/'Zulässig' im Agent für Mobilgeräte verwenden. Wenn die Sicherheitsrichtlinien mit dem Agent für Mobilgeräte synchronisiert werden, werden die Filterlisten nicht synchronisiert. Alle übrigen Einstellungen werden gemäß den Richtlinien aktualisiert. Mobile Security sperrt eingehende Anrufe basierend auf den folgenden Prioritäten bzw. lässt diese entsprechend zu: 1. Liste 'Zulässig' im Agent für Mobilgeräte 2. Liste 'Gesperrt' im Agent für Mobilgeräte 3. Liste 'Gesperrt' auf Server Sie können auch die serverseitige Kontrolle für ausgehende Anrufe auf Android-Mobilgeräten konfigurieren.

Hinweis

Die Liste der zulässigen und gesperrten Anruffilter muss das folgende Format aufweisen: "[name1:]number1;[name2:]number2;...".

'name' darf nicht mehr als 30 Zeichen umfassen, während die Telefonnummer zwischen 4 und 20 Zeichen lang sein muss und die folgenden Zeichen enthalten darf: 0-9, +, -, #, (,) und Leerzeichen. Die Anzahl der Einträge darf maximal 200 betragen.

Richtlinie zum Schutz vor Internet-Bedrohungen

Ermöglicht die Verwaltung der Richtlinie zum Schutz vor Internet-Bedrohungen über den Mobile Security-Management Server sowie die Bereitstellung der Richtlinie auf Android-Mobilgeräten. Darüber hinaus können Android-Mobilgeräte das Protokoll zum Schutz vor Internet-Bedrohungen zurück an den Server senden.

Hinweis

Die Mobile Security-Funktion „Schutz vor Internet-Bedrohungen“ unterstützt nur den Standard-Browser von Android und Google Chrome.

Zum Konfigurieren von Einstellungen zum Schutz vor Internet-Bedrohungen klicken Sie auf **Richtlinien**, dann auf den Namen der Richtlinie und anschließend auf **Richtlinie zum Schutz vor Internet-Bedrohungen**.

Schutz vor Internet-Bedrohungen für Android-Mobilgeräte

Die Funktion „Schutz vor Internet-Bedrohungen“ bietet Ihnen die serverseitige Steuerung der entsprechenden Richtlinien auf Android-Mobilgeräten sowie drei vordefinierte Sicherheitsebenen: **Niedrig**, **Normal** und **Hoch**. Darüber hinaus werden gesperrte und zulässige Listen zum Sperren oder Zulassen bestimmter URLs bereitgestellt. Mobile Security blockiert alle URLs, die Sie zur Liste 'Gesperrt' hinzufügen, und erlaubt alle URLs aus der zulässigen Liste.

Hinweis

Die Richtlinie zum Schutz vor Internet-Bedrohungen unterstützt nur Google Chrome und den Standard-Browser von Android auf Mobilgeräten.

Weitere Informationen zur Konfiguration der Listen für gesperrte oder zulässige Filter finden Sie in der folgenden Tabelle.

TABELLE 38-6. Filterlistenkonfiguration für die Richtlinie zum Schutz vor Internet-Bedrohungen

SERVERSTEUERUNG	BENUTZERSTEUERUNG	BESCHREIBUNG
Deaktiviert	Aktiviert	Der Benutzer kann die Liste 'Gesperrt'/'Zulässig' im Agent für Mobilgeräte bearbeiten. Mobile Security sperrt URLs basierend auf den folgenden Prioritäten bzw. lässt diese entsprechend zu: 1. Liste 'Zulässig' im Agent für Mobilgeräte 2. Liste 'Gesperrt' im Agent für Mobilgeräte
Aktiviert	Deaktiviert	Der Benutzer darf die Liste 'Gesperrt'/'Zulässig' nur im Agent für Mobilgeräte bearbeiten. Mobile Security sperrt URLs basierend auf den folgenden Prioritäten bzw. lässt diese entsprechend zu: 1. Zulässige Liste auf dem Server 2. Liste 'Gesperrt' auf Server 3. Liste 'Zulässig' im Agent für Mobilgeräte 4. Liste 'Gesperrt' im Agent für Mobilgeräte

Serversteuerung	Benutzersteuerung	Beschreibung
Aktiviert	Aktiviert	Der Benutzer kann die vom Administrator definierte Liste 'Gesperrt'/'Zulässig' anzeigen oder bearbeiten und auch die Liste 'Gesperrt'/'Zulässig' im Agent für Mobilgeräte verwenden. Wenn die Sicherheitsrichtlinien mit dem Agent für Mobilgeräte synchronisiert werden, werden die Filterlisten nicht synchronisiert. Alle übrigen Einstellungen werden gemäß den Richtlinien aktualisiert. Mobile Security sperrt URLs basierend auf den folgenden Prioritäten bzw. lässt diese entsprechend zu: 1. Liste 'Zulässig' im Agent für Mobilgeräte 2. Liste 'Gesperrt' im Agent für Mobilgeräte 3. Zulässige Liste auf dem Server 4. Liste 'Gesperrt' auf Server

Hinweis

Die Liste 'Zulässig' und 'Gesperrt' zur Internet-Bedrohungsfilterung müssen folgendes Format verwenden: [URL1] [URL2] [URL3] mit einem Leerzeichen oder Zeilenumbruch zwischen zwei URLs.

Schutz vor Internet-Bedrohungen für iOS-Mobilgeräte

Die Funktion „Schutz vor Internet-Bedrohungen“ bietet die serverseitige Steuerung auf überwachten iOS-Mobilgeräten, indem Zugriff auf Folgendes bereitgestellt wird:

- Nur bestimmte Websites
- Beschränkte jugendgefährdende Inhalte

In der folgenden Tabelle finden Sie Informationen zu den Funktionen:

TABELLE 38-7. Filterlistenkonfiguration für die Richtlinie zum Schutz vor Internet-Bedrohungen

FUNKTION	BESCHREIBUNG
Nur bestimmte Websites	Mit dieser Option wird der Zugriff auf die Websites beschränkt, die Sie auf dem Server konfiguriert haben. Sie können die zulässigen URLs auf der iOS-Registerkarte der Richtlinie zum Schutz vor Internet-Bedrohungen hinzufügen. Diese URLs werden dem Safari-Browser auf den iOS-Mobilgeräten der Benutzer hinzugefügt.
Beschränkte jugendgefährdende Inhalte	Diese Option verwendet Filterlisten, um die Serversteuerung der Websites bereitzustellen, die auf iOS-Mobilgeräten gesperrt oder zugelassen werden sollen. Unabhängig von den Standardfiltereinstellungen auf iOS-Mobilgeräten sperren oder gewähren diese Filter Zugriff auf die Websites.

Hinweis

Die Liste 'Zulässig' und 'Gesperrt' zur Internet-Bedrohungsfilterung müssen folgendes Format verwenden: [URL1] [URL2] [URL3] mit einem Leerzeichen oder Zeilenumbruch zwischen zwei URLs.

Kennwortrichtlinie

Die Kennwortrichtlinie verhindert unbefugten Zugriff auf Daten auf Mobilgeräten.

Zum Konfigurieren von Einstellungen für Kennwortrichtlinien klicken Sie auf **Richtlinien**, dann auf den Namen der Richtlinie und anschließend im linken Menü auf **Kennwortrichtlinie**.

Richtlinie zur Funktionssperre

Mit dieser Funktion können Sie die Nutzung bestimmter Funktionen/Komponenten für Mobilgeräte einschränken (deaktivieren) oder zulassen (aktivieren). Beispielsweise können Sie für alle Mobilgeräte in einer bestimmten Gruppe die Kamera deaktivieren.

Um Einstellungen für die Richtlinie zur Funktionssperre zu konfigurieren, klicken Sie auf **Richtlinien**, dann auf den Namen der Richtlinie und anschließend im Menü auf der linken Seite auf **Richtlinie zur Funktionssperre**.

See *Unterstützte Betriebssystemfunktionen für Mobilgeräte auf Seite 38-25* for the list of supported features/components.

Warnung!

Seien Sie vorsichtig, wenn Sie WLAN/WIFI und/oder Microsoft ActiveSync deaktivieren. Das Mobilgerät kann möglicherweise nicht mit dem Server kommunizieren, wenn beide Optionen nicht verfügbar sind.

Bei Android-Mobilgeräten können Sie auch Access Points hinzufügen, um die Verfügbarkeit der Gerätekomponenten im Gültigkeitsbereich dieser Access Points zu steuern.

Unterstützte Betriebssystemfunktionen für Mobilgeräte

Die folgende Tabelle enthält die Liste der Funktionen, die Mobile Security auf jeder Plattform unterstützt.

TABELLE 38-8. Trend Micro Mobile Security 9.7 – Funktionstabelle

RICHTLINIE	FUNKTIONEN	EINSTELLUNGEN			
Bereitstellung	Wi-Fi	Standardmäßige WLAN-Konfiguration	●	●	
		Legacy-Hotspot-Konfiguration	●		
		Hotspot 2.0-	●		

Richtlinie	Funktionen	Einstellungen			
		Konfiguration			
	Exchange ActiveSync	Exchange ActiveSync-Konfiguration	●		
	VPN	VPN-Konfiguration	●		
	Allgemeiner HTTP-Proxy	Allgemeine HTTP-Proxy-Konfiguration	●		
	Single Sign-On	Single Sign-On-Konfiguration	●		
	Zertifikat	Zertifikatkonfiguration	●		
	Mobilfunknetz	Konfiguration des Mobilfunknetzes	●		
	AirPlay/AirPrint	AirPlay/AirPrint-Konfiguration	●		

Richtlinie	Funktionen	Einstellungen			
	Designs (nur überwacht)	Hintergrundkonfiguration	●		
		Schriftartkonfiguration	●		
	Verwaltete Domänen	Nicht gekennzeichnete E-Mail-Domänen	●		
		Verwaltete Safari-Webdomänen	●		
Gerätesicherheit	Sicherheitseinstellungen	Echtzeitsuche		●	
		Nach erfolgtem Pattern-Update durchsuchen		●	
		Manuelle Suche	●	●	
		Facebook-Suche	●	●	
Datenschutz	SMS-Spamschutz	Serverseitige		●	

Richtlinie	Funktionen	Einstellungen			
		Kontrolle			
		Liste 'Gesperrt' verwenden		●	
		Liste 'Zulässig' verwenden		●	
	WAP-Push-Spamschutz	Serverseitige Kontrolle		●	
		Liste 'Zulässig' verwenden		●	
	Anruffilter	Serverseitige Kontrolle		●	
		Liste 'Gesperrt' verwenden		●	
		Liste 'Zulässig' verwenden		●	

Richtlinie	Funktionen	Einstellungen			
	Schutz vor Internet-Bedrohungen	Serverseitige Kontrolle		●	
		Liste 'Gesperrt' verwenden		●	
		Liste 'Zulässig' verwenden		●	
		Nur bestimmte Websites zulassen	●		
		Eingeschränkte jugendgefährdende Inhalte zulassen	●		
Datenschutz	Kennworteinstellungen	Kennwort für die Anmeldung verwenden	●	●	●
		Einfaches Kennwo	●	●	●

Richtlinie	Funktionen	Einstellungen			
		rt zulassen			
		Alphanumerisches Kennwort anfordern	●	●	●
		Minimale Kennwortlänge	●	●	●
		Ablauf des Kennworts	●	●	●
		Kennwortverlauf	●	●	●
		Automatische Sperre	●	●	●
		Aktion bei Kennwortfehler	●	●	●
	Funktionssperre	Kamera	●	●	
		FaceTime	●		
		Bildschirmfoto	●		

Richtlinie	Funktionen	Einstellungen			
		Installation von Apps	●		
		Bei Roaming synchronisieren	●		
		Sprachwahl	●		
		App-interner Kauf	●		
		Spiel für mehrere Spieler	●		
		Game Center-Freunde hinzufügen	●		
		Game Center (nur überwacht)	●		
		Verschlüsselte Backups erzwingen	●		
		Anstößige Musik,	●		

Richtlinie	Funktionen	Einstellungen			
		Podcast und iTunes U			
		Passbook bei gesperrtem Gerät aktivieren	●		
		Bluetooth und Bluetooth-Erkennung		●	
		WLAN/Wi-Fi		●	
		3G-Datennetzwerk		●	
		Tethering		●	
		Entwicklermodus		●	
		Lautsprecher/ Lautsprechertelefon/ Mikrofon			

Richtlinie	Funktionen	Einstellungen			
		Speicherkarten einschränken		●	
		Siri	●		
		Siri bei gesperrtem Gerät aktivieren	●		
		Filter für anstößige Ausdrücke aktivieren	●		
		Zugriff auf iCloud-Dienste aktivieren	●		
		Cloud-Backup	●		
		Cloud-Dokumentsynchronisierung	●		
		Fotostream	●		

Richtlinie	Funktionen	Einstellungen			
		Geteilte Fotostreams	●		
		Diagnosedaten	●		
		Nicht vertrauenswürdiges TLS-Protokoll (Transport Layer Security) akzeptieren	●		
		iTunes Store-Kennwort erzwingen	●		
		YouTube	●		
		Dokumente über verwaltete Apps in anderen Apps öffnen	●		
		Dokumente über	●		

Richtlinie	Funktionen	Einstellungen			
		andere Apps in verwalteten Apps öffnen			
		iTunes	●		
		Safari-Webbrowser	●		
		AutomAusfüllen	●		
		JavaScript	●		
		Popup-Fenster	●		
		Betrugswarnung erzwingen	●		
		Cookies zulassen	●		
		Apps entfernen (nur überwacht)	●		
		Bookstore (nur überwacht)	●		

Richtlinie	Funktionen	Einstellungen			
		Erotik (nur überwacht)	●		
		Konfigurationsprofilinstallation (nur überwacht)	●		
		iMessage (nur überwacht)	●		
		Bewertungsregion	●		
		Filme	●		
		TV-Serien	●		
		Apps	●		
		Kontoänderung (nur überwacht)	●		
		AirDrop (nur überwacht)	●		
		Änderung der	●		

Richtlinie	Funktionen	Einstellungen			
		Anwendungen für mobile Daten (nur überwacht)			
		Assistent (Siri) für benutzergenerierte Inhalte (nur überwacht)	●		
		Cloud Keychain-Synchronisierung	●		
		Änderung bei 'Meine Freunde suchen' (nur überwacht)	●		
		Fingerabdruck zum Entsperr	●		

Richtlinie	Funktionen	Einstellungen			
		en eines Geräts			
		Host-Kopplung (nur überwacht)	●		
		Sperrbildschirm / Kontrollzentrum	●		
		Sperrbildschirm / Benachrichtigungsansicht	●		
		Sperrbildschirm Tagesansicht	●		
		OTAPKI-Updates (Over the Air Public Key Infrastructure)	●		
		Begrenzung von Werbe-Tracking	●		

Richtlinie	Funktionen	Einstellungen			
		erzwingen			
		Anfordern von Kopplungskennwort durch AirPlay erzwingen	●		
		Zulassen, dass verwaltete Apps Daten in iCloud speichern können	●		
		Sicherung von Unternehmensbüchern zulassen	●		
		Konfigurationseinschränkungen zulassen	●		
		Löschen sämtlicher Inhalte und Einstellu	●		

Richtlinie	Funktionen	Einstellungen			
		ngen zulassen			
		Handoff zulassen	●		
		Internetergebnisse in Spotlight zulassen	●		
		Synchronisierung von Notizen und Markierungen für Unternehmensbücher zulassen	●		
		Freigabe von verwalteten Dokumenten mit AirDrop zulassen	●		
		iCloud-Fotomediathek zulassen	●		
		Installation von	●		

Richtlinie	Funktionen	Einstellungen			
		Apps über Gerät zulassen			
		Tastenkombinationen zulassen	●		
		Gekoppelte Apple Watch zulassen	●		
		Kennwortänderung zulassen	●		
		Geräten amensänderung zulassen	●		
		Hintergrundänderung zulassen	●		
		Automatisches Herunterladen von Apps zulassen	●		
		Einstufen von Enterpri	●		

Richtlinie	Funktionen	Einstellungen			
		se-Apps als vertrauenswürdig zulassen			
	Konformitätseinstellungen	Mit Root-Zugriff/ Mit Jailbreak	●	●	
		Unverschlüsselt	●	●	
		Überprüfung der Betriebssystemversion	●	●	
Anwendungsverwaltung	Anwendungsüberwachung und -kontrolle	Erforderliche Anwendungen	●	●	
		Zulässige Anwendungen	●	●	
		App-Sperre (nur überwacht)	●		
	Volumenkaufprogramm	Volumenkaufprogramm	●		

Richtlinie	Funktionen	Einstellungen			
Remote-Steuerung	Registrieren		●	●	
	Aktualisieren		●	●	
	Diebstahlschutz	Remote-Ortung		●	
		Remote-Sperre	●	●	
		Remote-Löschung	●	●	●
		Kennwort zurücksetzen	●	●	
	Samsung KNOX Workspace	Container erstellen		●	
		Container entfernen		●	
		Container sperren		●	
		Container entsperren		●	
		Container-Kennwort		●	

Richtlinie	Funktionen	Einstellungen			
		zurücksetzen			
Richtlinie von Samsung KNOX Workspace	Container-Kontoeinstellung	Liste 'Gesperrt'		●	
		Zulässige Liste		●	
	Einstellungen zur Zugriffsbeschränkung	Benutzern die Verwendung der Kamera erlauben		●	
		Anzeigen der Liste der Anwendungen 'Teilen über' zulassen		●	
	Browsereinstellungen	Einstellung 'Automatisches Ausfüllen aktivieren'		●	
		Einstellung 'Cookies aktivieren'		●	

Richtlinie	Funktionen	Einstellungen			
		Einstellung 'Popup-Fenster aktivieren'		●	
		Einstellung 'Erzwingen von Betrugswarnung aktivieren'		●	
		Einstellung 'JavaScript aktivieren'		●	
		Internet-Proxy aktivieren		●	
Richtlinie von Samsung KNOX Workspace	Container-Kennwort – Einstellungen	Kennwortsichtbarkeit aktivieren		●	
		Mindestzeitraum für Kennwortänderung		●	

Richtlinie	Funktionen	Einstellungen			
		Minimale Kennwortlänge		●	
		Maximale Inaktivitätszeitüberschreitung		●	
		Maximale Anzahl an Fehlversuchen		●	
		Kennwortverlauf		●	
		Maximales Alter des Kennworts		●	
		Mindestanzahl der in einem Kennwort erforderlichen Sonderzeichen		●	
		Kennwortkomplexität		●	

Richtlinie	Funktionen	Einstellungen			
	Anwendungseinstellungen	Liste 'Zulässig' der Installation		●	
		Liste 'Gesperrt' der Installation		●	
		Erforderliche Anwendungen		●	
		Deaktivierte Anwendungen		●	
Programm zur Geräteregistrierung			●		

Konformitätsrichtlinie

Mit Hilfe der Komformitätsrichtlinie können Sie die Konformitätskriterien für die Mobilgeräte festlegen. Wenn ein Mobilgerät diese Kriterien nicht erfüllt, zeigt Mobile Security den nicht konformen Status auf der Server-Benutzeroberfläche an. Mobile Security sendet außerdem eine E-Mail an das nicht konforme iOS-Gerät, während auf nicht konformen Android-Mobilgeräten eine Benachrichtigung angezeigt wird. Die Prüfung zur Einhaltung von Richtlinien umfasst Folgendes:

- **Mit Root-Zugriff/Mit Jailbreak**: Überprüft, ob auf dem Mobilgerät ein Root-Zugriff/Jailbreak erfolgt ist oder nicht.
- **Unverschlüsselt**: Überprüft, ob die Verschlüsselung auf dem Mobilgerät aktiviert ist oder nicht.

- **Überprüfung der Betriebssystemversion**: Überprüft, ob die Betriebssystemversion die definierten Kriterien erfüllt oder nicht.

Um Einstellungen zur Einhaltung von Richtlinien zu konfigurieren, klicken Sie auf **Richtlinien**, dann auf den Namen der Richtlinie und anschließend auf **Konformitätsrichtlinie**.

Richtlinie zur Anwendungsüberwachung und -kontrolle

Richtlinien zur Anwendungsüberwachung und -kontrolle bieten Ihnen die serverseitige Kontrolle über die auf Mobilgeräten installierten Anwendungen und ermöglichen die Übertragung der erforderlichen Anwendungen auf die Mobilgeräte.

Zum Konfigurieren der Einstellungen der Richtlinie zur Anwendungsüberwachung und -kontrolle klicken Sie auf **Richtlinien**, dann auf den Namen der Richtlinie und dann auf **Richtlinie zur Anwendungsüberwachung und -kontrolle**.

- **Erforderliche Anwendungen**: Mit dieser Option werden alle Anwendungen, die Sie in der Liste hinzufügen, an die Mobilgeräte übertragen. Sie können auch ein VPN mit Anwendungen verknüpfen, sodass die Anwendungen immer dieses VPN nutzen, um eine Verbindung mit dem Netzwerk herzustellen.
- **Zulässige Anwendungen**: Sie können die auf Mobilgeräten installierten Anwendungen mit Hilfe der Listen 'Zulässig' und 'Gesperrt' steuern.

  Bei iOS-Mobilgeräten sendet Mobile Security eine Benachrichtigung an den Administrator und den Benutzer für jede Anwendung, die nicht der Richtlinie entspricht.

  Bei Android-Mobilgeräten sperrt Mobile Security die Anwendung, die nicht der Richtlinie entspricht und lässt alle anderen Anwendungen zu.

  - **Sperren von System-Apps aktivieren** (nur Android):

    Wenn diese Option ausgewählt ist, sperrt Mobile Security alle System-Apps auf Android-Mobilgeräten.

  - **Anwendungskategorie aktivieren**: Wählen Sie die Anwendungskategorie aus, die Sie auf Mobilgeräten aktivieren oder

deaktivieren möchten. Sie können auch eine Ausnahme festlegen, indem Sie die Anwendungen, die zu dieser Kategorie gehören, zu der Liste 'Zulässig' oder 'Gesperrt' hinzufügen. Wenn Sie zum Beispiel den Kategorietyp Spiele deaktiviert haben, sperrt Mobile Security alle Anwendungen, die dieser Kategorie angehören, es sei denn, solche Anwendungen sind in der Liste 'Zulässig' eingetragen.

Mobile Security lässt Anwendungen entsprechend den folgenden Prioritäten zu bzw. sperrt diese:

1. **Liste 'Zulässig'**: Mobile Security lässt Anwendungen zu, die sich in der Liste 'Zulässig‟ befinden, auch wenn sie zu der von Ihnen deaktivierten Kategorie gehören.
2. **Liste 'Gesperrt'**: Mobile Security sperrt Anwendungen, die sich in der Liste 'Gesperrt' befinden, auch wenn sie zu der von Ihnen aktivierten Kategorie gehören.
3. **Anwendungsberechtigungen**: Mobile Security lässt Anwendungen zu bzw. sperrt Anwendungen gemäß des von Ihnen ausgewählten Berechtigungsstatus für die Kategorie, zu der diese gehören.

- **Anwendungsberechtigungen aktivieren** (nur für Android): Wählen Sie die Anwendungsdienste, die Sie auf Android-Mobilgeräten aktivieren oder deaktivieren möchten. Sie können auch eine Ausnahme festlegen, indem Sie die Anwendungen, die diese Dienste nutzen, zu der Liste 'Zulässig' oder 'Gesperrt' hinzufügen. Wenn Sie beispielsweise den Diensttyp **Daten lesen** deaktiviert haben, sperrt Mobile Security alle Anwendungen, die den Datentyp 'Daten lesen' nutzen, es sei denn, solche Anwendungen sind in der Liste 'Zulässig' enthalten.

  Mobile Security lässt Anwendungen entsprechend den folgenden Prioritäten zu bzw. sperrt diese:

  1. **Liste 'Zulässig'**: Mobile Security lässt Anwendungen zu, die sich in der Liste 'Zulässig' befinden, auch wenn sie die von Ihnen deaktivierten Dienste nutzen.

2. **Liste 'Gesperrt'**: Mobile Security sperrt Anwendungen, die sich in der Liste 'Gesperrt' befinden, auch wenn sie die von Ihnen aktivierten Dienste nutzen.

3. **Anwendungsberechtigungen**: Mobile Security lässt Anwendungen zu bzw. sperrt Anwendungen gemäß des von Ihnen ausgewählten Berechtigungsstatus für die Dienste, die sie nutzen.

- **Nur die folgenden Anwendungen zulassen**: Fügen Sie die Anwendungen der Liste 'Zulässig' hinzu, die Benutzer auf ihren Mobilgeräten nutzen dürfen sollen. Wenn aktiviert:
  - Mobile Security zeigt auf Android-Mobilgeräten eine Popup-Warnung an, wenn Anwendungen erkannt werden, die sich nicht in der Liste 'Zulässig' befinden.
  - Wenn Mobile Security auf iOS-Mobilgeräten eine Anwendung erkennt, die nicht in der Liste 'Zulässig' enthalten ist, sendet Mobile Security eine E-Mail-Benachrichtigung an den Benutzer.
- **Nur die folgenden Anwendungen sperren**: Fügen Sie die Anwendungen zur Liste 'Gesperrt' hinzu, die Benutzer nicht auf ihren Mobilgeräten verwenden sollen. Wenn aktiviert:
  - Mobile Security zeigt auf Android-Mobilgeräten eine Popup-Warnung an, wenn Anwendungen erkannt werden, die sich in der Liste 'Gesperrt' befinden.
  - Wenn Mobile Security auf iOS-Mobilgeräten eine Anwendung erkennt, die nicht in der Liste 'Gesperrt' enthalten ist, sendet Mobile Security eine E-Mail-Benachrichtigung an den Benutzer.
- **App-Sperre (nur für überwachten Modus)**: Beschränkt das iOS-Mobilgerät auf die angegebene Anwendung.

Mobile Security prüft auf unzulässige Anwendungen und sendet eine E-Mail-Benachrichtigung an die Benutzer:

- automatisch gemäß den Einstellungen für die **Häufigkeit des Sammelns von Informationen** unter **Administration** > **Communication Server-Einstellungen** > **Allgemeine Einstellungen (Registerkarte)** oder

- beim Aktualisieren der Einstellungen für die **Häufigkeit des Sammelns von Informationen** unter **Administration** > **Communication Server-Einstellungen** > **Allgemeine Einstellungen (Registerkarte)**.

Richtlinie zum Volumenkaufprogramm

Mit Hilfe dieser Richtlinie kann der Administrator die iOS-Anwendungen, die über das Volumenkaufprogramm von Apple erworben wurden, in die Verwaltungs-Webkonsole von Mobile Security importieren. Mit Mobile Security werden alle Anwendungen in der Liste des Volumenkaufprogramms auf Mobilgeräte in einer Gruppe übertragen.

So konfigurieren Sie die Richtlinie zum Volumenkaufprogramm:

1. Fügen Sie Anwendungen zum Enterprise App Store hinzu. Informationen über das Verfahren finden Sie unter *Anwendung hinzufügen auf Seite 38-51*.
2. Klicken Sie auf **Richtlinien**, dann auf den Namen der Richtlinie und anschließend auf **Richtlinie zum Volumenkaufprogramm**.
3. Klicken Sie auf **Importieren** und wählen Sie dann Anwendungen für den Import aus dem Enterprise App Store aus.
4. Klicken Sie auf **Speichern**, um alle Anwendungen auf die iOS-Mobilgeräte zu übertragen.

Anwendung hinzufügen

Prozedur

1. Navigieren Sie in der Mobile Security Administration-Webkonsole zu **Anwendungen** > **Enterprise App Store**.

   Das Fenster **Enterprise App Store** wird angezeigt.

2. Klicken Sie auf die Registerkarte **Android** oder **iOS**.
3. Klicken Sie auf **Hinzufügen**.

   Das Fenster **Anwendung hinzufügen** wird angezeigt.

4. Sie können jetzt mit einer der folgenden Optionen eine Anwendung in der Liste hinzufügen:

   - **Vom lokalen Computer hinzufügen**: Wählen Sie eine Installationsdatei für Android- oder iOS-Mobilgeräte aus.
   - **Webclip hinzufügen**: Geben Sie die URL der Anwendung ein. Daraufhin wird das Anwendungssymbol auf dem Startbildschirm des Mobilgeräts des Benutzers angezeigt, und der Link wird im Standard-Webbrowser auf dem mobilen Gerät geöffnet.
   - (Android) **Aus externem App Store hinzufügen**: Geben Sie den Link zu der Anwendung in einem externen App Store ein. Das Anwendungssymbol wird auf dem Startbildschirm des Mobilgeräts des Benutzers angezeigt, und der Link wird im Standard-Webbrowser auf dem mobilen Gerät geöffnet.
   - (iOS) **Bitte Suchbegriff eingeben**: Geben Sie den Namen der VPP-Anwendung ein, die Sie durchsuchen möchten, und wählen Sie ein Land aus, in dessen Apple App Store nach der Anwendung, die Sie aus den Suchergebnissen hinzufügen möchten, gesucht werden soll. Nachdem die VPP-Anwendung hinzugefügt wurde, ist sie nur im **App Store** der Mobile Security Administration-Webkonsole verfügbar. Um die Anwendung auf Mobilgeräte zu verschieben, müssen Sie die Anwendung der **Richtlinie zum Volumenkaufprogramm** hinzufügen. Informationen über das Verfahren finden Sie unter *Richtlinie zum Volumenkaufprogramm auf Seite 38-51*.

5. Klicken Sie auf **Weiter**.

   Das Fenster **Anwendung bearbeiten** wird geöffnet.

6. Konfigurieren Sie das Folgende:

   - **Anwendungsname**: Geben Sie einen Namen für die Anwendung ein.
   - **Anwendungssymbol**: Wenn das Symbol der Anwendung nicht angezeigt wird, klicken Sie auf das Symbol 'App hochladen', um das Anwendungssymbol auszuwählen und hochzuladen.

- **Anwendungs-ID**: Wenn die Anwendungs-ID nicht angezeigt wird, geben Sie die Anwendungs-ID ein.
- **Datei mit VPP-Codes**: Laden Sie für die iOS VPP-Anwendung die Datei mit VPP-Codes (Volume Purchase Codes) hoch, die Sie von Apple erhalten haben.
- **Kategorie**: Wählen Sie eine Kategorie für die Anwendung aus.

Hinweis

Sie müssen eine Kategorie aus der Dropdown-Liste auswählen. Zum Hinzufügen oder Löschen einer Kategorie klicken Sie auf die Schaltfläche **Kategorie**.

- **Beschreibung**: Geben Sie eine Beschreibung für die Anwendung ein.
- **Veröffentlichen**: Wählen Sie eine der folgenden Optionen aus:
  - **Nicht veröffentlichen**: Zum Hochladen der Anwendung auf den Server, aber verborgen für Mobilgeräte.
  - **Als Produktversion veröffentlichen**: Zum Hochladen der Anwendung auf den Server und Veröffentlichen zum Download auf Mobilgeräte.
  - **Als Betaversion veröffentlichen**: Zum Hochladen der Anwendung auf den Server und Veröffentlichen als Betaversion für den Download auf Mobilgeräte.
- **Screenshots**: Hiermit können Sie Anwendungs-Screenshots auswählen und hochladen.

7. Klicken Sie auf **Weiter**.

   Die Anwendung wird in der Liste der Anwendungen angezeigt.

Container-Richtlinie

Mit dieser Richtlinie können Sie Einstellungen für die Sicherheit von Samsung KNOX-Containern verwalten. Sie können die Liste 'Zulässig'

oder 'Gesperrt' für Konten konfigurieren, Einschränkungen festlegen und Browser-, Kennwort- und Anwendungseinstellungen konfigurieren.

Hinweis

Sie müssen die KNOX-Lizenz in Mobile Security konfigurieren, bevor Sie diese Richtlinie aktivieren. Navigieren Sie zum Konfigurieren der KNOX-Lizenz in der Webkonsole für die Verwaltung zu **Administration** > **Produktlizenz**.

- **Kontoeinstellungen**: Geben Sie mit Hilfe der Listen für zulässige und/oder gesperrte Konten die Konten an, die in Samsung KNOX-Containern hinzugefügt oder eingeschränkt werden können.
- **Einstellungen zur Zugriffsbeschränkung**: Deaktivieren Sie die Kamera oder die Dateifreigabe für Samsung KNOX-Container.
- **Browsereinstellungen**: Konfigurieren Sie die Sicherheitseinstellungen für den systemeigenen Android-Webbrowser für Samsung KNOX-Container.
- **Kennworteinstellungen**: Konfigurieren Sie Kennwortsicherheitseinstellungen für Samsung KNOX-Container.
- **Anwendungseinstellungen**: Konfigurieren Sie die folgenden Listen:
  - **Listen mit Anwendungsfiltern**: Konfigurieren Sie die Liste 'Zulässig' oder 'Gesperrt', um die Installation von Anwendungen für Samsung KNOX-Container zu beschränken.
  - **Erforderliche Anwendungen**: Konfigurieren Sie die Liste der erforderlichen Anwendungen, um Anwendungen anzugeben, die für Samsung KNOX installiert werden müssen.
  - **Anwendungen deaktivieren**: Konfigurieren Sie die Liste der deaktivierten Anwendungen, um bestimmte Anwendungen auf dem Mobilgerät zu deaktivieren. Wenn die Anwendungen in der Liste auf dem Mobilgerät installiert sind, werden sie nicht entfernt, aber der Benutzer kann die Anwendungen nicht verwenden.

Um Einstellungen für Container-Richtlinien zu konfigurieren, klicken Sie auf **Richtlinien**, dann auf den Namen der Richtlinie und anschließend auf **Container-Richtlinie**.

Teil XVII

Widgets für Virtual Mobile Infrastructure

Kapitel 39

Dashboard-Widgets für Virtual Mobile Infrastructure

Dieser Abschnitt enthält Hilfethemen für die in Trend Micro Apex Central unterstützten Virtual Mobile Infrastructure-Widgets.

Es werden folgende Themen behandelt:

Die 5 am häufigsten gestarteten Trend Micro Virtual Mobile Infrastructure-Anwendungen – Widget

Dieses Widget zeigt die fünf am häufigsten gestarteten Anwendungen an, die von Trend Micro Virtual Mobile Infrastructure-Servern gemeldet wurden.

Die Daten werden in einem Balkendiagramm angezeigt. Auf der Y-Achse wird der Anwendungsname und auf der X-Achse die Häufigkeit angezeigt, mit der eine Anwendung gestartet wurde.

Ändern Sie den verwalteten Server, den das Widget als Quelle verwendet, indem Sie auf das Dropdown-Menü klicken. Wählen Sie in den Optionen des Dropdown-Menüs die IP-Adresse des verwalteten Servers aus, der als Quelle verwendet werden soll.

Die 5 am häufigsten gestarteten Trend Micro Virtual Mobile Infrastructure-Webanwendungen – Widget

Dieses Widget zeigt die fünf am häufigsten gestarteten Webanwendungen an, die von Trend Micro Virtual Mobile Infrastructure Servern gemeldet wurden.

Die Daten werden in einem Balkendiagramm angezeigt. Auf der Y-Achse wird der Anwendungsname und auf der X-Achse die Häufigkeit angezeigt, mit der eine Anwendung gestartet wurde.

Ändern Sie den verwalteten Server, den das Widget als Quelle verwendet, indem Sie auf das Dropdown-Menü klicken. Wählen Sie in den Optionen des Dropdown-Menüs die IP-Adresse des verwalteten Servers aus, der als Quelle verwendet werden soll.

Die 5 häufigsten Online-Benutzer von Trend Micro Virtual Mobile Infrastructure – Widget

Dieses Widget zeigt die fünf aktivsten von den Trend Micro Virtual Mobile Infrastructure-Servern gemeldeten Benutzer an, die am längsten auf ihren Arbeitsbereich zugegriffen haben.

Die Daten werden in einem Balkendiagramm angezeigt. Auf der Y-Achse wird der Benutzername und auf der X-Achse der Zeitraum in Minuten angezeigt, während dem der Benutzer auf seinen Arbeitsbereich zugegriffen hat.

Ändern Sie den verwalteten Server, den das Widget als Quelle verwendet, indem Sie auf das Dropdown-Menü klicken. Wählen Sie in den Optionen des Dropdown-Menüs die IP-Adresse des verwalteten Servers aus, der als Quelle verwendet werden soll.

CPU-Auslastungsstatus des Trend Micro Virtual Mobile Infrastructure-Servers – Widget

Dieses Widget zeigt die CPU-Auslastung von Trend Micro Virtual Mobile Infrastructure-Servern an.

Die Daten werden in einem Diagramm dargestellt. Auf der Y-Achse wird die CPU-Auslastung als Prozentsatz dargestellt. Auf der X-Achse wird der Zeitraum dargestellt, während dem die CPU-Auslastung aufgezeichnet wurde.

Ändern Sie den verwalteten Server, den das Widget als Quelle verwendet, indem Sie auf das Dropdown-Menü klicken. Wählen Sie in den Optionen des Dropdown-Menüs die IP-Adresse des verwalteten Servers aus, der als Quelle verwendet werden soll.

Festplattennutzungsstatus von Trend Micro Virtual Mobile Infrastructure-Servern – Widget

Dieses Widget zeigt die Festplattennutzung von Trend Micro Virtual Mobile Infrastructure-Servern an.

Die folgenden Daten werden in einem Tortendiagramm dargestellt:

- **Frei**: Die Menge des verfügbaren Festplattenspeichers auf dem verwalteten Server.
- **Verwendet**: Die Menge des verwendeten Festplattenspeichers auf dem verwalteten Server.

- **Gesamt**: Die Menge des gesamten Festplattenspeichers auf dem verwalteten Server.

Ändern Sie den verwalteten Server, den das Widget als Quelle verwendet, indem Sie auf das Dropdown-Menü klicken. Wählen Sie in den Optionen des Dropdown-Menüs die IP-Adresse des verwalteten Servers aus, der als Quelle verwendet werden soll.

Speicherauslastungsstatus des Trend Micro Virtual Mobile Infrastructure Servers

Diese Widget zeigt die Speicherauslastung von Trend Micro Virtual Mobile Infrastructure-Servern an.

Die folgenden Daten werden in einem Tortendiagramm dargestellt:

- **Frei**: Die Menge des verfügbaren Arbeitsspeichers auf dem verwalteten Server.
- **Verwendet**: Die Menge des verwendeten Arbeitsspeichers auf dem verwalteten Server.
- **Gesamt**: Die Menge des gesamten Arbeitsspeichers auf dem verwalteten Server.

Ändern Sie den verwalteten Server, den das Widget als Quelle verwendet, indem Sie auf das Dropdown-Menü klicken. Wählen Sie in den Optionen des Dropdown-Menüs die IP-Adresse des verwalteten Servers aus, der als Quelle verwendet werden soll.

Trend Micro Virtual Mobile Infrastructure-Benutzerstatus – Widget

Dieses Widget zeigt die Statusangaben der aktuellen Benutzer an, die von Trend Micro Virtual Mobile Infrastructure-Servern gemeldet wurden.

Die folgenden Statusangaben werden in einem Tortendiagramm dargestellt:

- **Aktiv**: Der Benutzer ist aktuell mit dem Server verbunden und greift auf den Arbeitsbereich zu.

- **Im Leerlauf**: Der Benutzer ist mit dem Server verbunden, greift aktuell aber nicht auf den Arbeitsbereich zu.
- **Offline**: Der Benutzer ist nicht mit dem Server verbunden.
- **Deaktiviert**: Das Benutzerkonto wurde deaktiviert, und der Benutzer kann nicht auf den Server zugreifen.

Ändern Sie den verwalteten Server, den das Widget als Quelle verwendet, indem Sie auf das Dropdown-Menü klicken. Wählen Sie in den Optionen des Dropdown-Menüs die IP-Adresse des verwalteten Servers aus, der als Quelle verwendet werden soll.

Teil XVIII

Vulnerability Protection – Widgets

Kapitel 40

Widgets für Vulnerability Protection Dashboard

Dieser Abschnitt enthält Hilfethemen für die im Trend Micro Apex Central unterstützten Vulnerability Protection-Dashboard-Widgets.

Es werden folgende Themen behandelt:

Vulnerability Protection nach (erkanntem) Anwendungstyp – Widget

Dieses Widget verfolgt die Anwendungstypen, die mit IPS-Ereignissen (Erkannt) auf dem Endpunkt verknüpft sind.

Sie können auswählen, welche Vulnerability Protection-Installation als Datenquelle für dieses Widget verwendet werden soll. Um die Datenquelle auszuwählen, klicken Sie auf das Einstellungssymbol (>) und wählen Sie die Quelle aus der bereitgestellten Liste aus.

Tipp

Dieses Widget kann nur Daten von einem einzigen Vulnerability Protection-Server anzeigen. Erstellen Sie ein neues Widget für jeden Server, um mehrere Vulnerability Protection-Server zu überwachen.

Um eine Vulnerability Protection-Installation für die Vulnerability Protection-Widgets verfügbar zu machen, navigieren Sie zu **Administration** > **Verwaltete Server** > **Serverregistrierung** und fügen einen neuen Vulnerability Protection-Server hinzu.

Hinweis

Die in den Widgets angezeigten Daten sind auf die Daten beschränkt, die aufgrund der Benutzerkontoberechtigungen zulässig sind.

Klicken Sie zum Öffnen der Seite **Ereignisse** des Vulnerability Protection Managers, auf der die gefilterten mit dem spezifischen Anwendungstyp verknüpften IPS-Ereignisse (Erkannt) angezeigt werden, auf einen Wert in der Spalte **Summen**.

Daten	Beschreibung
Name des Anwendungstyps	Der Name des Anwendungstyps

Daten	Beschreibung
Gesamt	Anzahl der Ereignisse im Zeitraum und Prozentsatz der darin dargestellten gesamten Ereignisse dieses Typs
Vorherige Gesamtanzahl	Anzahl der Ereignisse im Zeitraum, der dem aktuellen Zeitraum vorangeht
Trend	Änderung in Prozent vom vorherigen zum aktuellen Zeitraum

Vulnerability Protection nach (verhindertem) Anwendungstyp – Widget

Dieses Widget verfolgt die Anwendungstypen, die mit IPS-Ereignissen (Verhindert) auf dem Endpunkt verknüpft sind.

Sie können auswählen, welche Vulnerability Protection-Installation als Datenquelle für dieses Widget verwendet werden soll. Um die Datenquelle auszuwählen, klicken Sie auf das Einstellungssymbol (>) und wählen Sie die Quelle aus der bereitgestellten Liste aus.

Tipp

Dieses Widget kann nur Daten von einem einzigen Vulnerability Protection-Server anzeigen. Erstellen Sie ein neues Widget für jeden Server, um mehrere Vulnerability Protection-Server zu überwachen.

Um eine Vulnerability Protection-Installation für die Vulnerability Protection-Widgets verfügbar zu machen, navigieren Sie zu **Administration** > **Verwaltete Server** > **Serverregistrierung** und fügen einen neuen Vulnerability Protection-Server hinzu.

Hinweis

Die in den Widgets angezeigten Daten sind auf die Daten beschränkt, die aufgrund der Benutzerkontoberechtigungen zulässig sind.

Klicken Sie zum Öffnen der Seite **Ereignisse** des Vulnerability Protection Managers, auf der die gefilterten mit dem spezifischen Anwendungstyp verknüpften IPS-Ereignisse (Verhindert) angezeigt werden, auf einen Wert in der Spalte **Summen**.

Daten	Beschreibung
Name des Anwendungstyps	Der Name des Anwendungstyps
Gesamt	Anzahl der Ereignisse im Zeitraum und Prozentsatz der darin dargestellten gesamten Ereignisse dieses Typs
Vorherige Gesamtanzahl	Anzahl der Ereignisse im Zeitraum, der dem aktuellen Zeitraum vorangeht
Trend	Änderung in Prozent vom vorherigen zum aktuellen Zeitraum

Überblick über die Funktionen von Vulnerability Protection – Widget

Dieses Widget zeigt die letzte Aktivität aller Vulnerability Protection-Module an.

Sie können auswählen, welche Vulnerability Protection-Installation als Datenquelle für dieses Widget verwendet werden soll. Um die Datenquelle auszuwählen, klicken Sie auf das Einstellungssymbol (>) und wählen Sie die Quelle aus der bereitgestellten Liste aus.

Tipp

Dieses Widget kann aggregierte Daten aus mehreren Vulnerability Protection-Installationen anzeigen. Die in diesem Widget dargestellten Vulnerability Protection-Installationen werden im Fenster **Serverregistrierung** definiert. Erstellen Sie ein neues Widget für jede Installation, um mehrere Vulnerability Protection-Installationen einzeln zu überwachen.

Um eine Vulnerability Protection-Installation für die Vulnerability Protection-Widgets verfügbar zu machen, navigieren Sie zu **Administration**

> **Verwaltete Server** > **Serverregistrierung** und fügen einen neuen Vulnerability Protection-Server hinzu.

Hinweis

Die in den Widgets angezeigten Daten sind auf die Daten beschränkt, die aufgrund der Benutzerkontoberechtigungen zulässig sind.

Verwenden Sie die Dropdown-Liste **Bereich**, um den Zeitraum für die angezeigten Daten auszuwählen.

Daten	Beschreibung
Modul	Der Name des Vulnerability Protection-Moduls
Geschützte Computer	Die aktuelle Anzahl der verwalteten Computer, die vom Modul geschützt werden, und der Prozentsatz aller verwalteten Computer, den diese Anzahl repräsentiert
Anzahl der Ereignisse	Die Anzahl der Ereignisse, die während des festgelegten Zeitraums vom Modul generiert wurden
Trend	Änderung in Prozent vom vorherigen zum aktuellen Zeitraum

Vulnerability Protection Firewall – Ereignisverlauf – Widget

Dieses Widget zeigt die Anzahl der Firewall-Ereignisse während eines bestimmten Zeitraums an. Das Diagramm zeigt von Firewall-Regeln ausgelöste Ereignisse im Erkennungs- und Verhinderungsmodus an.

Sie können auswählen, welche Vulnerability Protection-Installation als Datenquelle für dieses Widget verwendet werden soll. Um die Datenquelle auszuwählen, klicken Sie auf das Einstellungssymbol (>) und wählen Sie die Quelle aus der bereitgestellten Liste aus.

Um eine Vulnerability Protection-Installation für die Vulnerability Protection-Widgets verfügbar zu machen, navigieren Sie zu **Administration** > **Verwaltete Server** > **Serverregistrierung** und fügen einen neuen Vulnerability Protection-Server hinzu.

Hinweis

Die in den Widgets angezeigten Daten sind auf die Daten beschränkt, die aufgrund der Benutzerkontoberechtigungen zulässig sind.

Klicken Sie zum Öffnen der Seite **Ereignisse** des Vulnerability Protection Managers, auf der die gefilterten Firewall-Ereignisse (Erkannt oder Verhindert) im ausgewählten Zeitraum angezeigt werden, auf einen Bereich im Balkendiagramm.

Vulnerability Protection zur Erkennung von Eindringlingen – Ereignisverlauf – Widget

Dieses Widget zeigt die Anzahl der IPS-Ereignisse während eines bestimmten Zeitraums an. Das Diagramm zeigt die von IPS-Regeln ausgelösten Ereignisse im Erkennungs- und im Verhinderungsmodus an.

Sie können auswählen, welche Vulnerability Protection-Installation als Datenquelle für dieses Widget verwendet werden soll. Um die Datenquelle auszuwählen, klicken Sie auf das Einstellungssymbol (>) und wählen Sie die Quelle aus der bereitgestellten Liste aus.

Um eine Vulnerability Protection-Installation für die Vulnerability Protection-Widgets verfügbar zu machen, navigieren Sie zu **Administration** > **Verwaltete Server** > **Serverregistrierung** und fügen einen neuen Vulnerability Protection-Server hinzu.

Hinweis

Die in den Widgets angezeigten Daten sind auf die Daten beschränkt, die aufgrund der Benutzerkontoberechtigungen zulässig sind.

Klicken Sie zum Öffnen der Seite **Ereignisse** des Vulnerability Protection Managers, auf der die gefilterten IPS-Ereignisse (Erkannt oder Verhindert) während eines bestimmten Zeitraums angezeigt werden, auf einen Bereich im Balkendiagramm.

Vulnerability Protection – (erkannte) IPS-Aktivität – Widget

Dieses Widget zeigt die fünf IPS-Regeln im Erkennungsmodus an, die die größte Anzahl an Ereignissen ausgelöst haben.

Sie können auswählen, welche Vulnerability Protection-Installation als Datenquelle für dieses Widget verwendet werden soll. Um die Datenquelle auszuwählen, klicken Sie auf das Einstellungssymbol (>) und wählen Sie die Quelle aus der bereitgestellten Liste aus.

Um eine Vulnerability Protection-Installation für die Vulnerability Protection-Widgets verfügbar zu machen, navigieren Sie zu **Administration** > **Verwaltete Server** > **Serverregistrierung** und fügen einen neuen Vulnerability Protection-Server hinzu.

Hinweis

Die in den Widgets angezeigten Daten sind auf die Daten beschränkt, die aufgrund der Benutzerkontoberechtigungen zulässig sind.

Klicken Sie zum Öffnen der Seite **Ereignisse** des Vulnerability Protection Managers, auf der die gefilterten von einer bestimmten Regel ausgelösten IPS-Ereignisse (Erkannt) angezeigt werden, auf einen Wert in der Spalte **Summen**.

Daten	Beschreibung
Grund	Name der Regel
Gesamt	Anzahl der Ereignisse im Zeitraum und Prozentsatz der darin dargestellten gesamten Ereignisse dieses Typs
Vorherige Gesamtanzahl	Anzahl der Ereignisse im Zeitraum, der dem aktuellen Zeitraum vorangeht
Trend	Änderung in Prozent vom vorherigen zum aktuellen Zeitraum

Vulnerability Protection – (verhinderte) IPS-Aktivität – Widget

Dieses Widget zeigt die fünf IPS-Regeln im Verhinderungsmodus an, die die meisten Ereignisse ausgelöst haben.

Sie können auswählen, welche Vulnerability Protection-Installation als Datenquelle für dieses Widget verwendet werden soll. Um die Datenquelle auszuwählen, klicken Sie auf das Einstellungssymbol (>) und wählen Sie die Quelle aus der bereitgestellten Liste aus.

Um eine Vulnerability Protection-Installation für die Vulnerability Protection-Widgets verfügbar zu machen, navigieren Sie zu **Administration** > **Verwaltete Server** > **Serverregistrierung** und fügen einen neuen Vulnerability Protection-Server hinzu.

Hinweis

Die in den Widgets angezeigten Daten sind auf die Daten beschränkt, die aufgrund der Benutzerkontoberechtigungen zulässig sind.

Klicken Sie zum Öffnen der Seite **Ereignisse** des Vulnerability Protection Managers, auf der die gefilterten von einer bestimmten Regel ausgelösten IPS-Ereignisse (Verhindert) angezeigt werden, auf einen Wert in der Spalte **Summen**.

Daten	Beschreibung
Grund	Name der Regel
Gesamt	Anzahl der Ereignisse im Zeitraum und Prozentsatz der darin dargestellten gesamten Ereignisse dieses Typs
Vorherige Gesamtanzahl	Anzahl der Ereignisse im Zeitraum, der dem aktuellen Zeitraum vorangeht
Trend	Änderung in Prozent vom vorherigen zum aktuellen Zeitraum

Wichtigster Leistungsindikator für Vulnerability Protection – Widget

Dieses Widget zeigt die Anzahl der von den Erkennungseinstellungen der Aufklärungssuche angezeigten Ereignisse an, die im angegebenen Zeitraum stattgefunden haben.

Sie können auswählen, welche Vulnerability Protection-Installation als Datenquelle für dieses Widget verwendet werden soll. Um die Datenquelle auszuwählen, klicken Sie auf das Einstellungssymbol (>) und wählen Sie die Quelle aus der bereitgestellten Liste aus.

Um eine Vulnerability Protection-Installation für die Vulnerability Protection-Widgets verfügbar zu machen, navigieren Sie zu **Administration** > **Verwaltete Server** > **Serverregistrierung** und fügen einen neuen Vulnerability Protection-Server hinzu.

Hinweis

Die in den Widgets angezeigten Daten sind auf die Daten beschränkt, die aufgrund der Benutzerkontoberechtigungen zulässig sind.

Klicken Sie zum Öffnen der Seite **Ereignisse** des Vulnerability Protection Managers, auf der die gefilterten in der Aufklärungssuche gefundenen Ereignisse während eines bestimmten Zeitraums angezeigt werden, auf einen Bereich im Balkendiagramm.

Vulnerability Protection Aufklärungssuche – Ereignisverlauf – Widget

Dieses Widget zeigt die Anzahl der von den Erkennungseinstellungen der Aufklärungssuche angezeigten Ereignisse an, die im angegebenen Zeitraum stattgefunden haben.

Sie können auswählen, welche Vulnerability Protection-Installation als Datenquelle für dieses Widget verwendet werden soll. Um die Datenquelle auszuwählen, klicken Sie auf das Einstellungssymbol (>) und wählen Sie die Quelle aus der bereitgestellten Liste aus.

Um eine Vulnerability Protection-Installation für die Vulnerability Protection-Widgets verfügbar zu machen, navigieren Sie zu **Administration** > **Verwaltete Server** > **Serverregistrierung** und fügen einen neuen Vulnerability Protection-Server hinzu.

Hinweis

Die in den Widgets angezeigten Daten sind auf die Daten beschränkt, die aufgrund der Benutzerkontoberechtigungen zulässig sind.

Klicken Sie zum Öffnen der Seite **Ereignisse** des Vulnerability Protection Managers, auf der die gefilterten in der Aufklärungssuche gefundenen Ereignisse während eines bestimmten Zeitraums angezeigt werden, auf einen Bereich im Balkendiagramm.

Vulnerability Protection – Statusüberblick – Widget

In diesem Widget werden die Anzahl der kritischen Warnungen und Warnungsbenachrichtigungen sowie ein Tortendiagramm mit dem Prozentsatz der Endpunkte angegeben, die sich in einem bestimmten Zustand befinden.

Sie können auswählen, welche Vulnerability Protection-Installation als Datenquelle für dieses Widget verwendet werden soll. Um die Datenquelle auszuwählen, klicken Sie auf das Einstellungssymbol (>) und wählen Sie die Quelle aus der bereitgestellten Liste aus.

Tipp

Dieses Widget kann aggregierte Daten aus mehreren Vulnerability Protection-Installationen anzeigen. Die in diesem Widget dargestellten Vulnerability Protection-Installationen werden im Fenster **Serverregistrierung** definiert. Erstellen Sie ein neues Widget für jede Installation, um mehrere Vulnerability Protection-Installationen einzeln zu überwachen.

Um eine Vulnerability Protection-Installation für die Vulnerability Protection-Widgets verfügbar zu machen, navigieren Sie zu **Administration** > **Verwaltete Server** > **Serverregistrierung** und fügen einen neuen Vulnerability Protection-Server hinzu.

Hinweis

Die in den Widgets angezeigten Daten sind auf die Daten beschränkt, die aufgrund der Benutzerkontoberechtigungen zulässig sind.

COMPUTERSTATUS	BESCHREIBUNG
Verwaltet (grün)	Geschützt und ohne Fehler oder Warnungen
Nicht verwaltet (blau)	Nicht geschützt
Gesperrt (grau)	Gesperrt. Befindet sich ein Computer im gesperrten Zustand, kommuniziert der Vulnerability Protection Manager weder mit dem Agent/der Appliance noch erzeugt er beliebige computerbezogene Warnungen.
Kritisch (rot)	In einem Fehlerzustand
Warnung (gelb)	In einem Warnungszustand

Vulnerability Protection für gefährdete Endpunkte – Widget

Verwenden Sie dieses Widget, um gefährdete Endpunkte zu ermitteln.

Sie können auswählen, welche Vulnerability Protection-Installation als Datenquelle für dieses Widget verwendet werden soll. Um die Datenquelle auszuwählen, klicken Sie auf das Einstellungssymbol (>) und wählen Sie die Quelle aus der bereitgestellten Liste aus.

Tipp

Dieses Widget kann nur Daten von einem einzigen Vulnerability Protection-Server anzeigen. Erstellen Sie ein neues Widget für jeden Server, um mehrere Vulnerability Protection-Server zu überwachen.

Um eine Vulnerability Protection-Installation für die Vulnerability Protection-Widgets verfügbar zu machen, navigieren Sie zu **Administration** > **Verwaltete Server** > **Serverregistrierung** und fügen einen neuen Vulnerability Protection-Server hinzu.

Hinweis

Die in den Widgets angezeigten Daten sind auf die Daten beschränkt, die aufgrund der Benutzerkontoberechtigungen zulässig sind.

Zum Öffnen der Regeleigenschaftenseite des Vulnerability Protection Managers, auf der virtuelle gepatchte/ungeschützte Endpunkte angezeigt werden, klicken Sie auf einen Wert in der Spalte **Virtuell gepatcht/ ungeschützt**.

Daten	Beschreibung
Name	Der Name der Eindringschutzregel
Schweregrad	Der Schweregrad der Eindringschutzregel
CVE	CVE-Anzahl (Common Vulnerabilities and Exposure)
CVSS-Bewertung	Eine Bewertung des Schweregrads der Schwachstelle gemäß der nationalen Schwachstellendatenbank
MS-ID	ID des Microsoft-Sicherheitspatchs
Virtuell gepatcht	Anzahl der Endpunkte, denen die Regel im Anschluss einer Suche nach Empfehlungen zugewiesen wird
Ungeschützt	Anzahl der Endpunkte, denen die Regel im Anschluss einer Suche nach Empfehlungen nicht zugewiesen wird

Stichwortverzeichnis

A

actions
    Prävention vor Datenverlust, 19-11
ActiveAction, 10-54
Active Directory
    Benutzer importieren, 27-6
Agent-Eigenschutz, 7-12
Aktion bei überwachten Systemereignissen, 9-9
Aktionen
    Prävention vor Datenverlust, 35-4
Allgemeine Richtlinie
    Aktualisierungseinstellungen, 38-5
    Deinstallationsschutzfunktionen, 38-5
    Protokolleinstellungen, 38-5
Angegebene Richtlinien
    Priorität, 2-12
Anruffilter
    Format der Filterliste, 38-21
    Konfiguration der Filterliste, 38-19
Apex Central
    Vernetzung mit Trend Micro Endpoint Sensor, 30-2
Ausdrücke, 3-17, 3-18
    benutzerdefiniert
        Kriterien, 3-20, 3-21
    customized, 3-19, 3-23
    vordefiniert, 3-18, 3-19
Ausnahmeliste, 9-11
    Verhaltensüberwachung, 9-11
Ausstehende Ziele, 2-29
Authentifizierung
    Über, 28-2

B

Bedrohungsstatistik-Registerkarte, 1-38
Begriffe, 4
Benutzer, 28-3
    Aus AD importieren, 27-6
    Sperre, 28-18
Benutzerdefinierte Ausdrücke, 3-20, 3-21
    Kriterien, 3-20, 3-21
Benutzerdefinierte Schlüsselwörter
    Kriterien, 3-28–3-30
Berechtigungen
    Beenden, Berechtigung, 7-7
    Programmpfad und -name, 13-9
Bereitgestellte Ziele, 2-29
Browsing-Ziele, 2-12

C

Cache-Einstellungen für die Suche, 7-15
Cache für die On-Demand-Suche, 7-16
components
    on the Update Agent, 7-2
condition statements, 3-34
customized expressions, 3-19, 3-23
    importing, 3-23
customized keywords, 3-28
    importing, 3-32
customized templates, 3-34
    creating, 3-35
    importing, 3-37

D

dashboard
- registerkarten
  - Bildschirmpräsentation, 1-2
  - hinzufügen, 1-2
  - löschen, 1-3
  - umbenennen, 1-2
  - zusammenfassung, 1-15
- Widgets
  - hinzufügen, 1-4
  - Produktbereich ändern, 1-5
  - verschieben, 1-4

Dashboard
- Registerkarten, 1-2
- Widgets, 1-2

Data Discovery, 18-2
- Richtlinien erstellen, 18-2

data identifiers, 3-17
- Ausdrücke, 3-17
- Dateiattribute, 3-17
- Schlüsselwörter, 3-18

Dateiattribute, 3-17, 3-23–3-25
- creating, 3-24
- importing, 3-25
- wildcards, 3-24

Datenschutz, 19-2
Deinstallation
- Verwenden des Deinstallationsprogramms, 7-8

Dekomprimierungsregeln, 19-19
device control, 13-6, 21-35
- permissions, 13-6, 21-35
- storage devices, 13-6, 21-35

Device List, 19-10
digitaler Signatur-Cache, 7-15
DLP, 3-16
Dokumentation, 2
DSP, 13-10

E

Echtzeitsuche, 10-5
email domains, 19-9
E-Mail-Warnung senden, 38-50
Entwurfsrichtlinien, 2-5
Ereignisüberwachung, 9-7

G

Gefilterte Richtlinien
- Neu anordnen, 2-30

Geräte
- Endpoint Encryption Geräte-Widget, 27-9
- sperren, 28-18

Gerätesteuerung, 13-2, 13-9, 13-10, 21-33
- Berechtigungen, 13-9
  - Programmpfad und -name, 13-9
- Platzhalter, 13-10
- Provider der digitalen Signatur, 13-10
- Voraussetzungen, 13-2

Gesperrte Programmliste, 9-11

H

Herkömmliche Suche, 21-4
- Wechsel zur intelligenten Suche, 21-4

I

Intelligente Suche, 21-4
- Wechsel von der herkömmlichen Suche, 21-4

Internet-Bedrohungen
Beschränkte jugendgefährdende Inhalte, 38-23
Format der Filterliste, 38-23, 38-24
Konfiguration der Filterliste, 38-22
Nur bestimmte Websites, 38-23

J

Jetzt durchsuchen, 10-43

K

Komprimierte Dateien
Dekomprimierungsregeln, 19-19
Konformität (Registerkarte), 1-32
Konformitätsrichtlinie
Prüfliste, 38-47
Kriterien
Benutzerdefinierte Ausdrücke, 3-20, 3-21
Schlüsselwörter, 3-28–3-30

L

Liste 'Zulässig', 14-5
Liste der zulässigen Programme, 9-11
logical operators, 3-34

M

mail scan, 7-18
Manuelle Suche, 10-32
monitored email subdomains, 19-9
monitored targets, 19-17, 19-19

N

nach Kriterien filtern, 2-5
network channels, 19-8, 19-15, 19-16, 19-18
email clients, 19-8
monitored targets, 19-15
non-monitored targets, 19-15
transmission scope
all transmissions, 19-16
external transmissions, 19-18
Netzwerkkanäle, 19-7
übertragungsumfang und Ziele, 19-7
non-monitored email domains, 19-9
non-monitored targets, 19-17, 19-19

O

Offline-Ziele, 2-29

P

Pattern für digitale Signaturen, 7-15
PCRE, 3-19
Perle Compatible Regular Expressions, 3-19
permissions
storage devices, 13-6, 21-35
Platzhalter
Gerätesteuerung, 13-10
Prävention vor Datenverlust, 3-17, 19-2
actions, 19-11
Aktionen, 35-4
Ausdrücke, 3-18–3-21, 3-23
data identifiers, 3-17
Dateiattribute, 3-23–3-25
Dekomprimierungsregeln, 19-19
network channels, 19-8, 19-15, 19-16, 19-18
Netzwerkkanäle, 19-7
Richtlinien, 35-2–35-6
Aktionen, 35-4
Aktivieren, 35-6

Benachrichtigungen, 35-5
Erstellen, 35-2
Konten auswählen, 35-2
Name und Priorität, 35-6
Ziele, 35-3
Schlüsselwörter, 3-26–3-30, 3-32
System- und Anwendungskanäle, 19-10
Vorlagen, 3-33–3-35, 3-37
Prävention vor Datenverlust (Data Loss Prevention, DLP), 3-16
privileges
mail scan privileges, 7-18
Produktbereich
Widgets, 1-5
Provider der digitalen Signatur, 13-10
Angeben, 13-10

Q

Quarantäne-Verzeichnis, 10-57

R

registerkarten
Konformität, 1-32
zusammenfassung, 1-15
Registerkarten, 1-2
Bedrohungsstatistik, 1-38
Widgets, 1-2
Registerkarte „Zusammenfassung“, 1-15
Richtlinien
allgemein, 28-15
Bearbeiten, 2-20
Benutzer, 28-6
Data Discovery, 18-2
erstellen, 2-23
Erstellen, 2-3
Full Disk Encryption, 28-9
löschen, 2-24
Neu anordnen, 2-30
Richtlinien bearbeiten, 2-20
Richtlinieneinstellungen
Kopieren, 2-17
Richtlinieneinstellungen kopieren, 2-17
Richtlinien erstellen, 2-3, 2-23
Einstellungen, 2-5
Einstellungen kopieren, 2-17
Richtlinienliste, 2-9, 2-26
Richtlinien löschen, 2-24
Richtlinien neu anordnen, 2-30
Richtlinienpriorität, 2-27
Richtlinientypen
angegeben, 2-4
Entwurf, 2-5
Richtlinien neu anordnen, 2-30
Richtlinienpriorität, 2-27
Richtlinienverwaltung, 2-3
Ausstehende Ziele, 2-29
Bereitgestellte Ziele, 2-29
Besitzer, 2-28
Besitzer ändern, 2-25
DLP, 3-16
Einstellungen, 2-5
Entwurfsrichtlinien, 2-5
Grundlegendes, 2-3
Offline-Ziele, 2-29
Richtlinien bearbeiten, 2-20
Richtlinieneinstellungen kopieren, 2-17
Richtlinien erstellen, 2-3, 2-23
Richtlinienliste, 2-9, 2-26

Richtlinien löschen, 2-24
Richtlinien neu anordnen, 2-30
Richtlinienpriorität, 2-12, 2-27
spezifizierte Richtlinien, 2-4
Ziele, 2-29
Ziele mit Problemen, 2-29
Richtlinienziele, 2-29

S

scan methods
conventional scan, 10-3
smart scan, 10-3
switching scan methods, 10-3
Schlüsselwörter, 3-18, 3-26
benutzerdefiniert, 3-28–3-30
customized, 3-28, 3-32
vordefiniert, 3-26, 3-27
Security Agent
Dateien, 7-13
Prozesse, 7-14
Registrierungsschlüssel, 7-14
Spam
SMS, 38-15
Format der Filterliste, 38-17
Konfiguration der Filterliste, 38-16
WAP-Push, 38-17
Zulässiges Listenformat, 38-18
Sperren des Malware-Verhaltens, 9-3
spezifizierte Richtlinien, 2-4
storage devices
permissions, 13-6, 21-35
Suchausschlüsse, 10-64
Suche nach Spyware/Grayware
Liste 'Zulässig', 14-5
Suchtypen, 21-2
Such-Zwischenspeicher, 7-15
System- und Anwendungskanäle, 19-10

U

Über
Authentifizierung, 28-2
Überwachte Systemereignisse, 9-7
Unterstützung für IPv6
Einschränkungen, 21-45
Update-Agent, 7-2
updates
Update-Agent, 7-2

V

Verhaltensüberwachung
Aktion bei Systemereignissen, 9-9
Ausnahmeliste, 9-11
vordefinierte Ausdrücke, 3-18
anzeigen, 3-19
Vordefinierte Schlüsselwörter
Abstand, 3-27
Anzahl der Schlüsselwörter, 3-27
Vordefinierte Vorlagen, 3-33
Vorlagen, 3-33–3-35, 3-37
condition statements, 3-34
customized, 3-34, 3-35, 3-37
logical operators, 3-34
vordefiniert, 3-33

W

web reputation, 21-29
Web Reputation, 11-2
Widgets, 1-2
Die häufigsten E-Mail-Empfänger komplexer Bedrohungen, 22-3

E-Mail-Nachrichten mit komplexen Bedrohungen, 22-3
Endpoint Encryption - Bericht zu Sicherheitsverstößen, 27-24
Endpoint Encryption Geräte-Sperre, 27-22
Endpoint Encryption-Status, 27-15
Erfolglose Anmeldeversuche an Endpoint Encryption-Geräten, 27-18
Erfolglose Anmeldeversuche von Endpoint Encryption-Benutzern, 27-20
wildcards, 3-24
Dateiattribute, 3-24

Z

Zeitgesteuerte Suche, 10-18
Ziele, 2-29
Ausstehend, 2-29
Bereitgestellt, 2-29
Durchsuchen, 2-12
Mit Problemen, 2-29
nach Kriterien filtern, 2-5
Offline, 2-29
Ziele auswählen
nach Kriterien filtern, 2-5
Ziele festlegen
Durchsuchen, 2-12
Ziele mit Problemen, 2-29