Dell Endpoint Security Suite Enterprise

Advanced Threat Prevention Quick Start Guide v3.9

January 2024
Rev. A01

DELL Technologies

Anmerkungen, Vorsichtshinweise und Warnungen

ANMERKUNG: HINWEIS enthält wichtige Informationen, mit denen Sie Ihr Produkt besser nutzen können.

VORSICHT: ACHTUNG deutet auf mögliche Schäden an der Hardware oder auf den Verlust von Daten hin und zeigt, wie Sie das Problem vermeiden können.

WARNUNG: WARNUNG weist auf ein potenzielles Risiko für Sachschäden, Verletzungen oder den Tod hin.

Contents

1

Introduction

Before you perform tasks explained in this guide, the following components must be installed:

- Endpoint Security Suite Enterprise - refer to *Endpoint Security Suite Enterprise Advanced Installation Guide* or *Endpoint Security Suite Enterprise Basic Installation Guide*
- Security Management Server or Security Management Server Virtual Server - refer to *Security Management Server Installation and Migration Guide* or *Security Management Server Virtual Server Quick Start and Installation Guide*

This guide explains basic administration of Advanced Threat Prevention and should be used with *AdminHelp*, available in the Management Console.

Dell ProSupport for Software kontaktieren

Telefonischen Support 24x7 für Ihr Dell Produkt erhalten Sie unter der Rufnummer 877-459-7304, Durchwahl 4310039.

Zusätzlich steht Ihnen unser Online-Support für Dell Produkte unter dell.com/support zur Verfügung. Der Online-Support enthält Treiber, Handbücher, technische Ratgeber, FAQs und eine Beschreibung festgestellter Probleme.

Halten Sie bei Ihrem Anruf Ihre Service-Tag-Nummer oder Ihren Express-Servicecode bereit, damit wir Sie schneller mit dem richtigen Ansprechpartner für Ihr technisches Problem verbinden können.

Telefonnummern außerhalb der Vereinigten Staaten finden Sie unter Dell ProSupport for Software – Internationale Telefonnummern.

2

Erste Schritte

Dieses Kapitel erläutert die empfohlenen Schritte, um mit dem Einsatz von Advanced Threat Prevention zu beginnen.

Die empfohlenen Schritte, um mit dem Einsatz von Advanced Threat Prevention zu beginnen, umfassen die folgenden Phasen:

- Bereitstellung eines Mandanten für Advanced Threat Prevention
  - Erforderlich, um Advanced Threat Prevention bereitzustellen
  - Die Lizenzen für Advanced Threat Prevention müssen auf dem Dell Server vorhanden sein.
- Konfigurieren der automatischen Aktualisierung des Advanced Threat Prevention-Agenten
  - Registrieren für automatische Aktualisierungen von Advanced Threat Prevention (optional)
  - Aktualisierungen werden monatlich herausgegeben
- Zuweisen oder Ändern von Administratorrollen
  - Advanced Threat Prevention-Dienst bereitstellen oder wiederherstellen
  - Sichern und Herunterladen bestehender Advanced Threat Prevention-Zertifikate
  - Richtlinien anzeigen, ändern und festlegen
- Benachrichtigungen einrichten
  - Festlegen von E-Mail- und Dashboard-Benachrichtigungen für Advanced Threat Prevention-Warnungen (optional)
  - Anpassen der Benachrichtigungen auf Grundlage der Anforderungen Ihres Unternehmens

Bereitstellung eines Mandanten

Ein Tenant muss im Dell Server bereitgestellt werden, bevor die Durchsetzung von Advanced Threat Prevention-Richtlinien aktiv wird.

Voraussetzungen

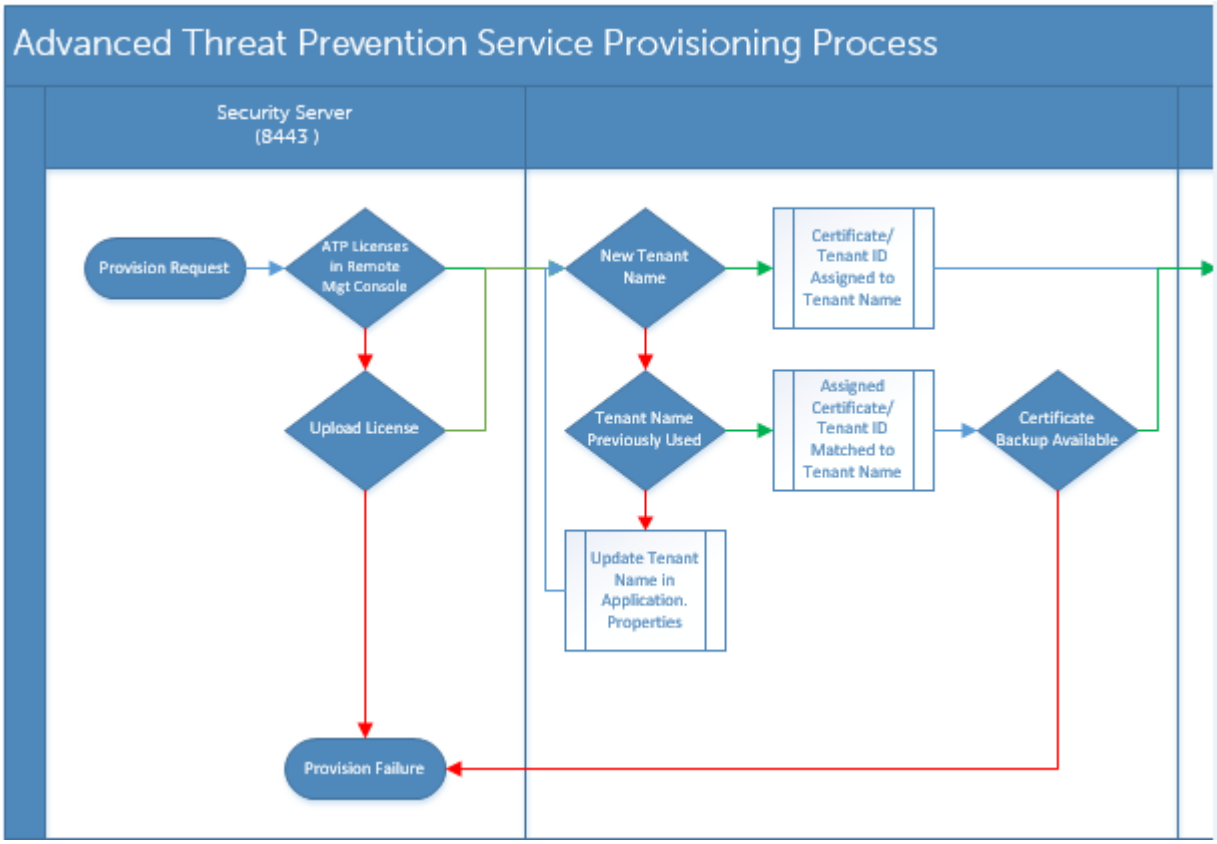
- Muss durch einen Administrator mit der Systemadministratorrolle durchgeführt werden.
- Muss über eine Verbindung mit dem Internet verfügen, um auf dem Dell Server bereitgestellt zu werden.
- Muss über eine Verbindung mit dem Internet auf dem Client verfügen, um die Online-Dienst-Integration von Advanced Threat Prevention in der Verwaltungskonsole anzuzeigen.
- Die Bereitstellung basiert auf einem Token, das im Rahmen der Bereitstellung aus einem Zertifikat generiert wird.
- Die Lizenzen für Advanced Threat Prevention müssen auf dem Dell Server vorhanden sein.

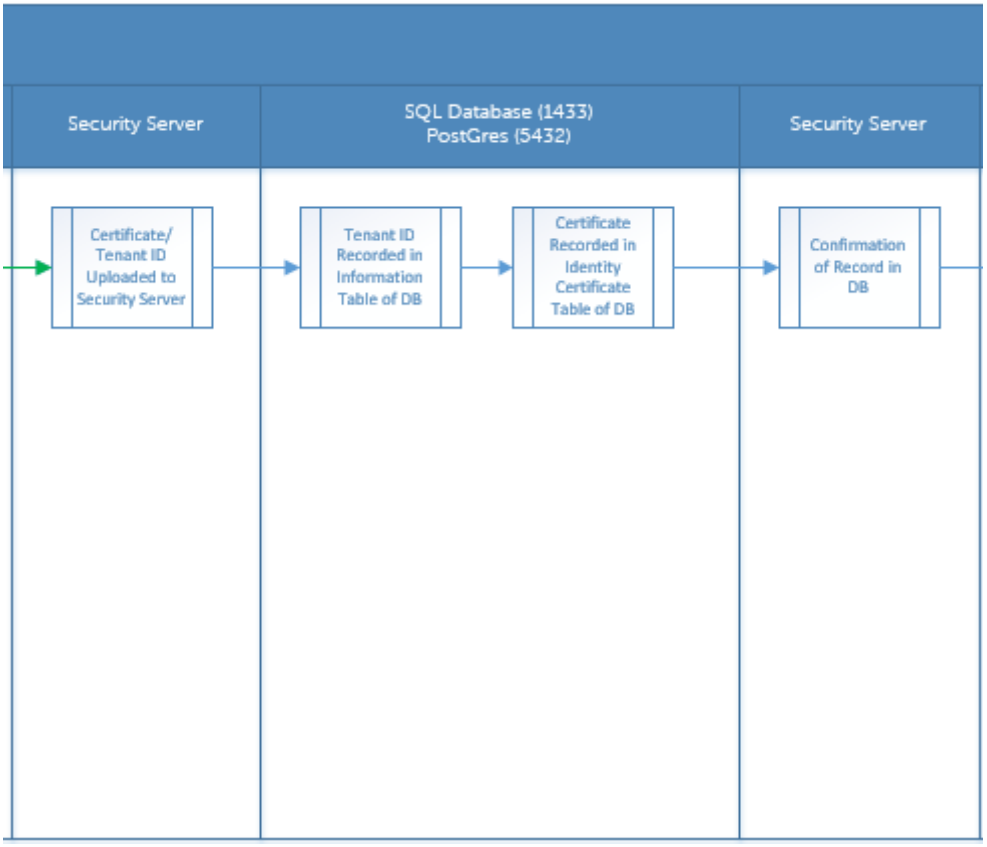
Bereitstellung eines Mandanten

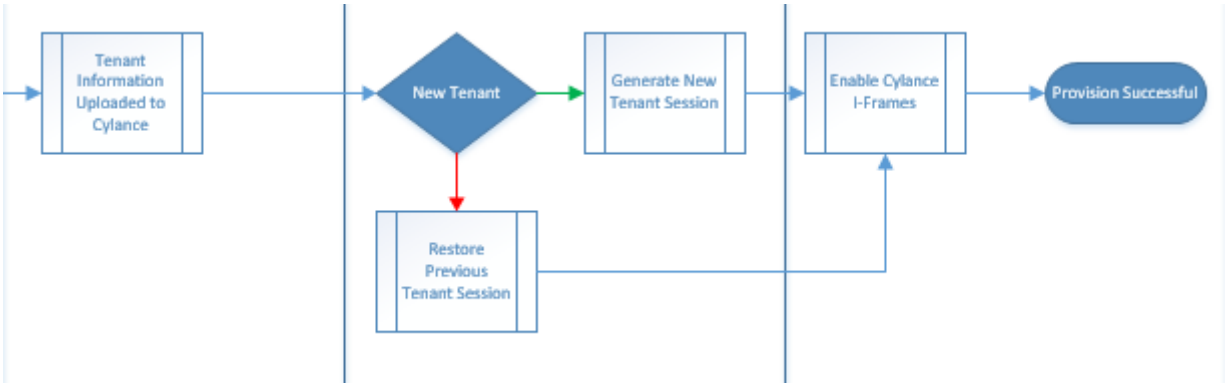
1. Melden Sie sich als Dell Administrator bei der Verwaltungskonsole an.
2. Klicken Sie im linken Bereich der Verwaltungskonsole auf Verwaltung > Servicemanagement.
3. Klicken Sie auf **Advanced Threat Protection-Dienst einrichten**. Importieren Sie Ihre Advanced Threat Prevention Lizenzen, wenn zu diesem Zeitpunkt ein Fehler auftritt.
4. Die geführte Einrichtung beginnt, sobald die Lizenzen importiert wurden. Klicken Sie zum Starten auf **Weiter**.
5. Lesen Sie die EULA, stimmen Sie ihr zu und klicken Sie dann auf **Weiter**.
6. Geben Sie die Anmeldeinformationen für den Dell Server ein, um den Mandanten bereitzustellen. Klicken Sie auf **Weiter**. *Die Bereitstellung eines vorhandenen Mandanten der Marke Cylance wird nicht unterstützt.*
7. Laden Sie das Zertifikat herunter. Dies ist erforderlich, um eine Wiederherstellung im Falle von Notfallszenarien mit dem Dell Server durchzuführen. Dieses Zertifikat wird nicht automatisch gesichert. Sichern Sie das Zertifikat auf einem sicheren Speicherplatz auf einem anderen Computer. Aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie das Zertifikat gesichert haben, und klicken dann Sie auf **Weiter**.
8. Die Einrichtung ist abgeschlossen. Klicken Sie auf **OK**.

Bereitstellung und Kommunikation mit Agenten

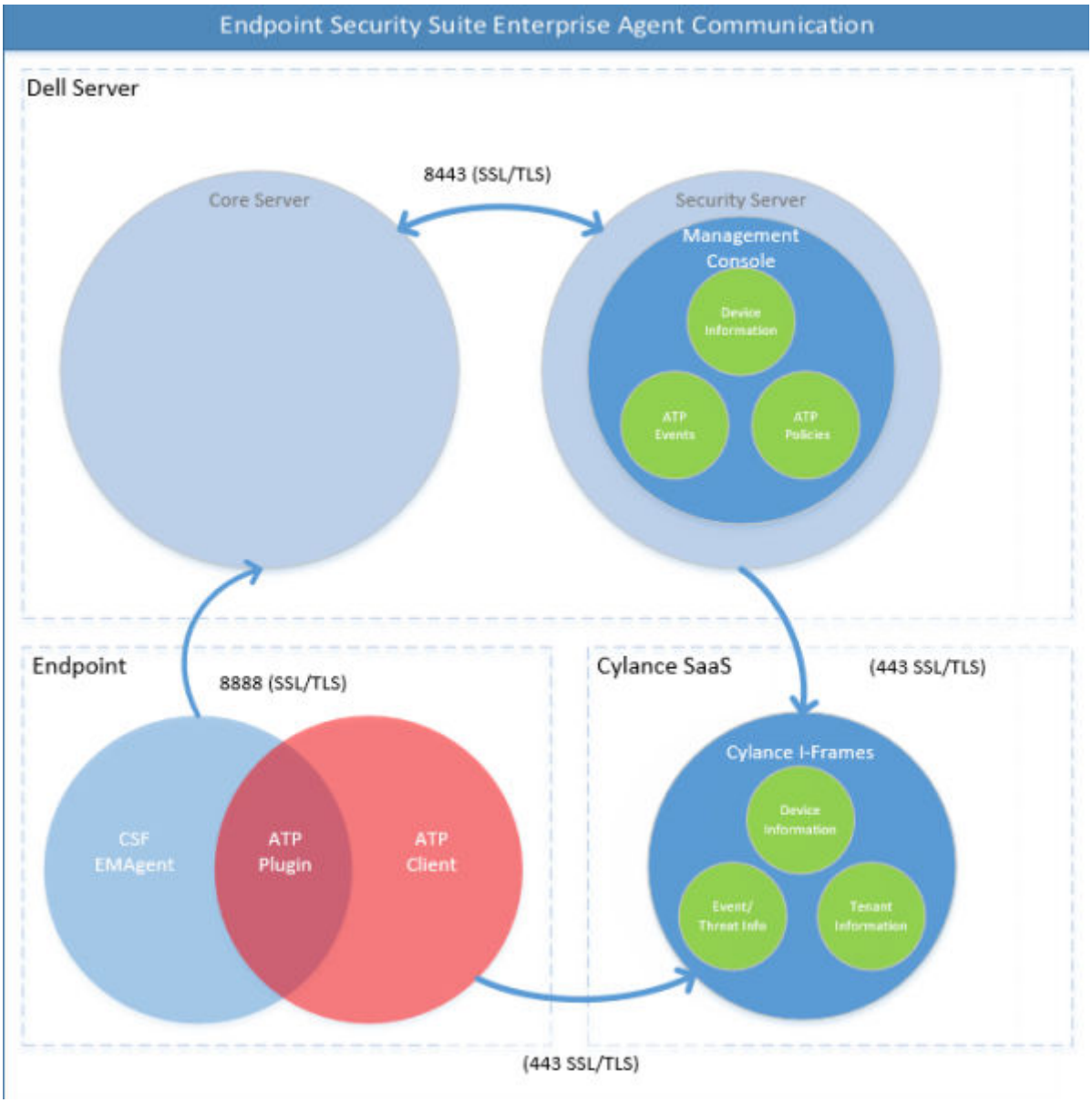
Die folgenden Diagramme veranschaulichen die Bereitstellung des Advanced Threat Prevention-Dienstes.



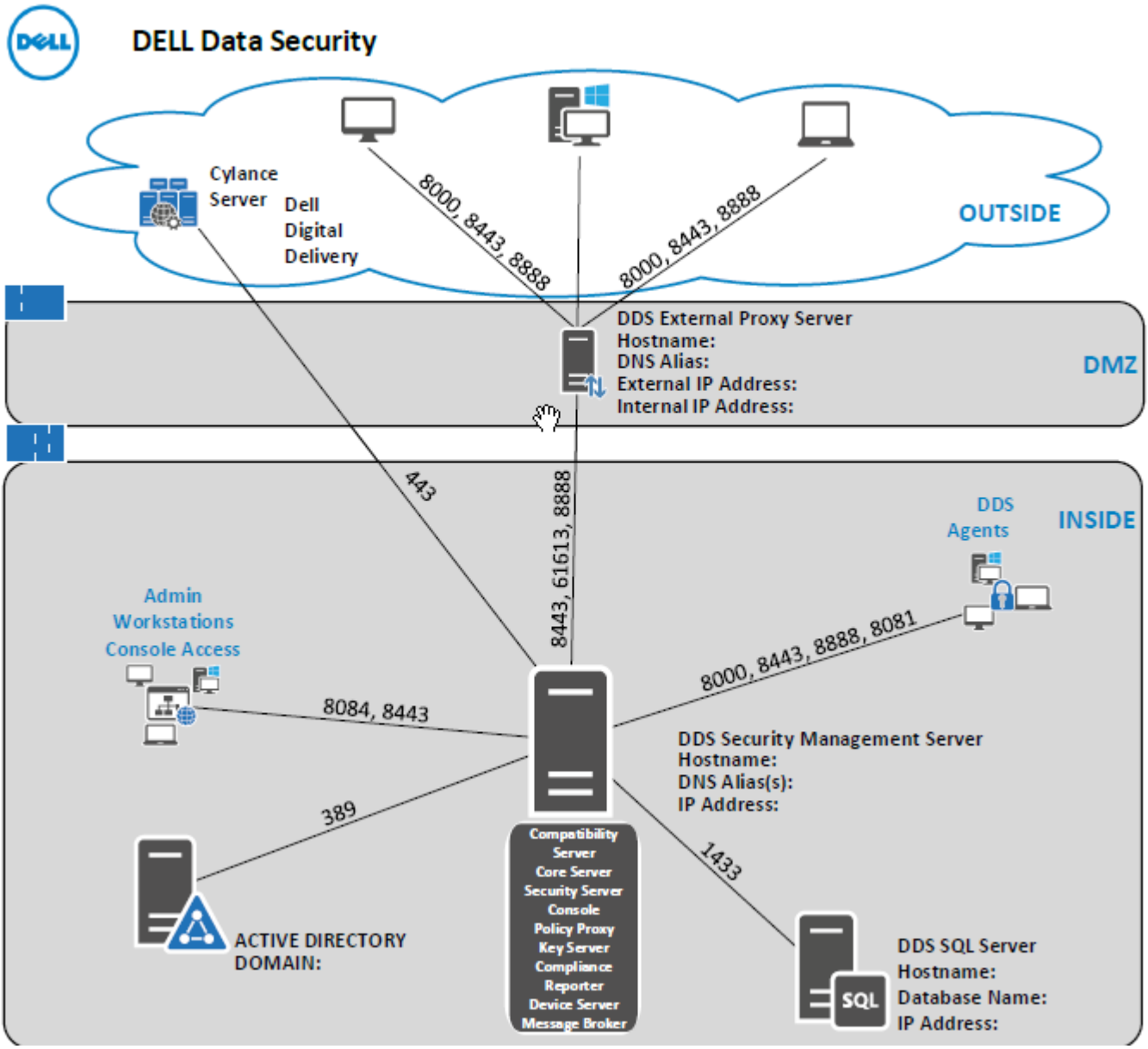




Das folgende Diagramm veranschaulicht die Agentenkommunikation für Advanced Threat Prevention.



Das folgende Diagramm zeigt die Dell Server-Architektur und -Kommunikation.



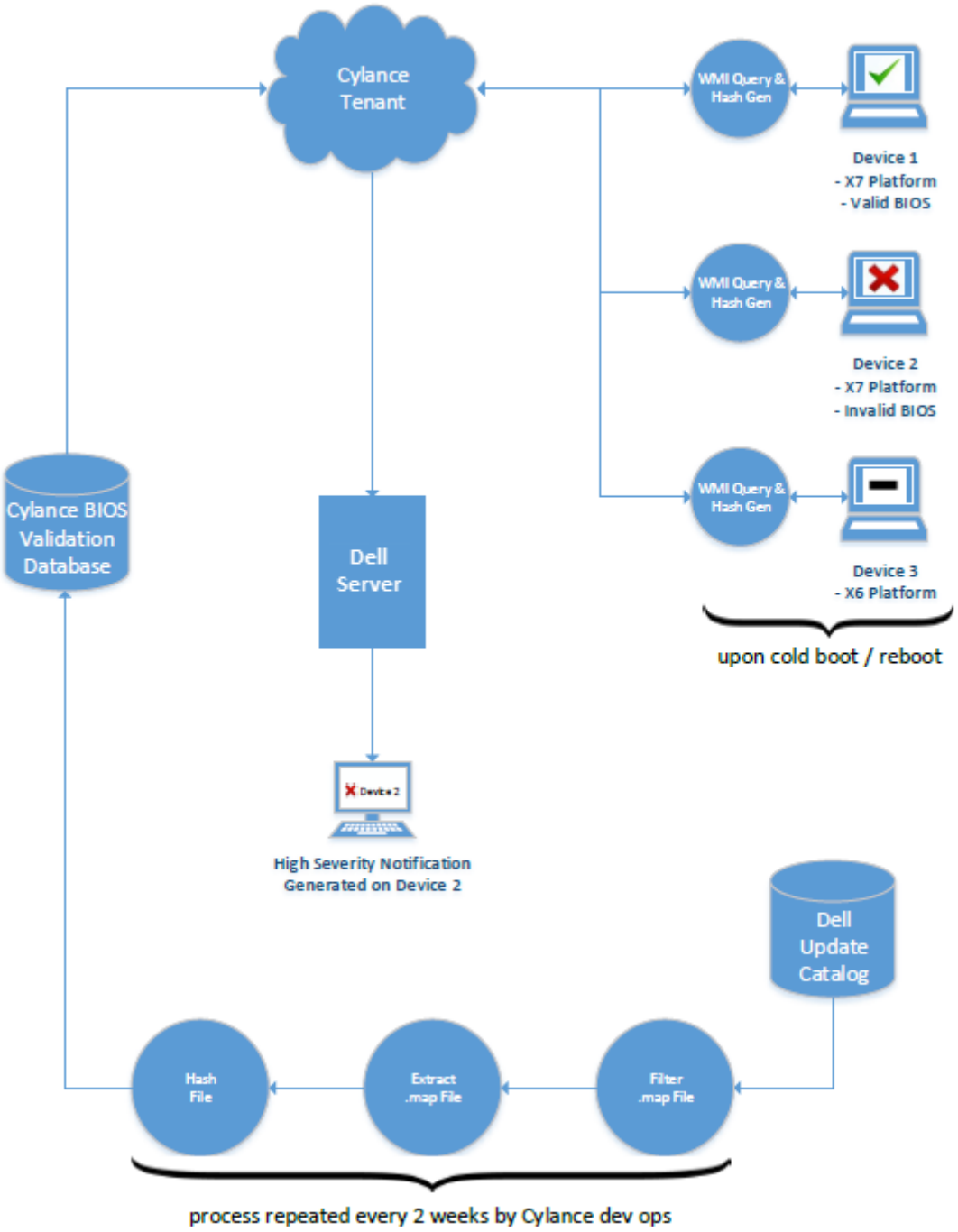
Integritätsüberprüfung des BIOS-Image aktivieren

Die Integritätsüberprüfung des BIOS-Image ist standardmäßig aktiviert, wenn der Hauptschalter für Advanced Threat Prevention aktiviert ist.

Eine Übersicht über die Integritätsüberprüfung des BIOS-Image finden Sie unter Prozess für die Integritätsüberprüfung des BIOS-Image.

Überprüfungsvorgang

Das folgende Diagramm veranschaulicht die Integritätsüberprüfung des BIOS-Abbildes.



Wenn die Richtlinie *BIOS-Gewährleistung aktivieren* in der Verwaltungskonsole ausgewählt ist, validiert der Cylance-Mandant einen BIOS-Hash auf Endpunkt-Computern, um sicherzustellen, dass das BIOS nicht von der werkseitigen Dell Version verändert wurde, was einen möglichen Angriffspunkt darstellen würde. Wenn eine Gefahr erkannt wird, wird eine Benachrichtigung an den Dell Server gesendet und der IT-Administrator wird in der Remote-Verwaltungskonsole über diesen Vorfall benachrichtigt. Eine Übersicht über den Prozess finden Sie unter Prozess für die Integritätsüberprüfung des BIOS-Abbildes.

ANMERKUNG: Ein benutzerdefiniertes Originalabbild kann mit dieser Funktion nicht verwendet werden, da das BIOS verändert wurde.

Dell Computermodelle, auf denen die Integritätsüberprüfung des BIOS-Abbildes unterstützt wird	
• Latitude 3470 • Latitude 3570 • Latitude 7275	• OptiPlex 5040 • OptiPlex 7040 • OptiPlex 7440

Dell Computermodelle, auf denen die Integritätsüberprüfung des BIOS-Abbildes unterstützt wird		
• Latitude 7370 • Latitude E5270 • Latitude E5470 • Latitude E5570 • Latitude E7270 • Latitude E7470 • Latitude Rugged 5414 • Latitude Rugged 7214 Extreme • Latitude Rugged 7414 • OptiPlex 3040 • OptiPlex 3240	• Precision Mobile Workstation 3510 • Precision Mobile Workstation 5510 • Precision Workstation 3620 • Precision Workstation 7510 • Precision Workstation 7710 • Precision Workstation T3420 • Venue 10 Pro 5056 • Venue Pro 5855 • Venue XPS 12 9250 • XPS 13 9350 • XPS 9550	

Konfigurieren der automatischen Aktualisierung des Advanced Threat Prevention Agenten

Sie können sich in der Verwaltungskonsole anmelden, um automatische Aktualisierungen für den Advanced Threat Prevention-Agenten zu erhalten. Durch die Anmeldung für den Empfang automatischer Agent-Aktualisierungen können Clients Aktualisierungen automatisch herunterladen und über den Advanced Threat Prevention Dienst anwenden. Aktualisierungen werden monatlich herausgegeben.

ANMERKUNG:

Die automatischen Aktualisierungen des Agenten werden ab Dell Server Version 9.4.1 unterstützt.

Automatische Aktualisierungen für den Agenten empfangen

So melden Sie sich an, um automatische Agent-Aktualisierungen zu erhalten:

1. Klicken Sie im linken Bereich der Verwaltungskonsole auf **Verwaltung** > **Dienstverwaltung**.
2. Auf der Registerkarte *Advanced Threats* unter *Automatische Agent-Aktualisierung* klicken Sie auf die Schaltfläche **Ein** und dann auf die Schaltfläche **Einstellungen speichern**.

   Es kann einige Minuten dauern, bis die Bestückung mit Informationen abgeschlossen ist und die automatischen Aktualisierungen angezeigt werden.

Beenden des Empfangs von automatischen Agent-Aktualisierungen

So beenden Sie den Empfang von automatischen Agent-Aktualisierungen:

1. Klicken Sie im linken Bereich der Verwaltungskonsole auf **Verwaltung** > **Dienstverwaltung**.
2. Auf der Registerkarte *Advance Threats* unter *Automatische Agent-Aktualisierung* klicken Sie auf die Schaltfläche **Aus** und dann auf die Schaltfläche **Einstellungen speichern**.

Zuweisen oder Ändern von Administratorrollen

Lassen Sie sich vorhandene Administratorrechte auf der Seite „Verwaltung“ in der Verwaltungskonsole anzeigen oder ändern Sie diese.

Administratorrollen

Die Administrator-Anmeldung ist in Active Directory integriert, so dass die Verwaltung von Administratoren vereinfacht wird und Sie Ihre vorhandene Infrastruktur zur Benutzerauthentifizierung nutzen können. Administratoren werden Rollen zugewiesen, die die zulässige Zugriffsstufe für jeden Administrator festlegen. Manche Administratoren dürfen beispielsweise eine Wiederherstellung nur mit Helpdesk-Unterstützung durchführen, während andere Administratoren vollständigen Zugriff auf die Bearbeitung von Sicherheitsrichtlinien haben. Sie können Active Directory-Gruppen Administratorrollen zuweisen. Dies ermöglicht Ihnen, die Ebene des Administratorzugriffs von Benutzern einfach durch die Änderung der AD-Gruppenmitgliedschaft zu modifizieren. Benutzern außerhalb der Domäne kann über Compliance Reporter ein Berichtszugriff gewährt werden.

Die Systemadministratorrolle ist erforderlich, um die folgenden Aufgaben durchzuführen:

- Advanced Threat Prevention-Dienst bereitstellen oder wiederherstellen
- Registrieren für automatische Aktualisierungen von Advanced Threat Prevention
- Festlegen von E-Mail- oder Dashboard-Benachrichtigungen für Advanced Threat Prevention-Warnungen
- Sichern und Herunterladen bestehender Advanced Threat Prevention-Zertifikate

ANMERKUNG: Die Sicherheitsadministratorrolle ist erforderlich für das Anzeigen, Ändern oder Festlegen von Richtlinien.

Zum Anzeigen oder Ändern der vorhandenen Administratorrechte gehen Sie wie folgt vor:
1. Klicken Sie im linken Fensterbereich auf **Bestückungen > Administratoren**.
2. Suchen oder wählen Sie die Zeile aus, die den Benutzernamen des gewünschten Administrators enthält, um die Benutzerdetails anzuzeigen.
3. Die Administratorrollen können Sie im rechten Bereich anzeigen oder ändern.
4. Klicken Sie auf **Speichern**.

ANMERKUNG: Dell empfiehlt, Administratorrollen auf Gruppenebene und nicht auf Benutzerebene zuzuweisen.

So werden Administratorrollen auf Gruppenebene angezeigt, zugewiesen oder geändert:
1. Klicken Sie im linken Fensterbereich auf **Bestückungen > Benutzergruppen**.
2. Suchen oder wählen Sie einen Gruppennamen und wählen Sie anschließend die Registerkarte **Administrator** aus. Daraufhin wird die Seite „Benutzergruppendetails“ angezeigt.
3. Wählen Sie die einer Gruppe zugewiesenen Administratorrollen aus oder heben Sie die bestehende Auswahl auf.
4. Klicken Sie auf **Speichern**.

Wenn Sie eine Gruppe entfernen, die über Administrationsrechte verfügt, und diese Gruppe dann zu einem späteren Zeitpunkt wieder hinzufügen, bleibt sie eine Administratorgruppe.

So werden Administratorrollen auf Benutzerebene angezeigt, zugewiesen oder geändert:
1. Klicken Sie im linken Fensterbereich auf **Bestückungen > Benutzer**.
2. Suchen oder wählen Sie einen Benutzernamen aus und wählen Sie anschließend die Registerkarte Administrator aus.
3. Wählen Sie die einem Benutzer zugewiesenen Administratorrollen aus oder heben Sie die bestehende Auswahl auf.
4. Klicken Sie auf **Speichern**.

Administratorrollen – Weisen Sie dem Benutzer Rollen zu, oder ändern Sie die Rollen und klicken Sie anschließend auf **Speichern**.

Übernommene Gruppenrollen – Eine schreibgeschützte Liste der Rollen, die der Benutzer von einer Gruppe übernommen hat. Klicken Sie zum Ändern der Rollen auf die Registerkarte **Benutzergruppen** für diesen Benutzer und wählen Sie den Gruppennamen aus.

Zugewiesene Rollen – Delegieren Sie Administratorrechte an einen Benutzer.

Benachrichtigungen einrichten

In der Remote-Verwaltungskonsole können Sie den Empfang von Benachrichtigungen einrichten. Die Benachrichtigungsliste stellt eine konfigurierbare Zusammenfassung von Neuigkeiten, Alarmen und Ereignissen bereit, die auf dem Dashboard anzuzeigen oder als E-Mail-Benachrichtigungen zu senden sind.

Benachrichtigungstypen

Sie können auswählen, welche Benachrichtigungstypen zur Liste gehören sollen. Die übrigen Benachrichtigungstypen werden ausgeblendet. Benachrichtigungen zu **Threat Protection** und **Advanced Threat-Ereignissen** gehören zur Advanced Threat Prevention.

Zu den Arten gehören Folgende:
- **Aktualisierung** - Aktuelles zu anstehenden Produktaktualisierungen. Um Produktaktualisierungen anzeigen und empfangen zu können, müssen Sie sich für diese Produkte registrieren. Wählen Sie **Dienstverwaltung > Produktbenachrichtigungen**, klicken Sie auf **ein** und klicken Sie dann auf **Einstellungen speichern**.
- **Config** - Aktuelles über Konfigurationsänderungen.
- **Knowledge Base** - Zusammenfassungen und Links zu Artikeln in der Knowledge Base mit tiefgreifenden technischen Informationen wie alternative Arbeitsschritte und Konfigurationsmethoden.
- **Ankündigung** - Aktuelles zu bevorstehenden Versionen und neuen Produkten.
- **Lizenz** - Warnungen, wenn Ihre Volume-Lizenzierungsverfügbarkeit gering ist oder wenn die Client-Zugriffslizenzanzahl überschritten wurde.
- **Threat Protection** - Eine Bedrohungswarnung von Advanced Threat Prevention.

- **Erweitertes Bedrohungsereignis** - Ein von Advanced Threat Prevention erkanntes Ereignis. Die Zusammenfassung enthält eine Liste mit kritischen, wichtigen, weniger wichtigen, Warn- und Informationsereignissen, die zu detaillierteren Informationen führen.
- **Bedrohungsereignis** - Ein von Threat Protection erkanntes Ereignis.
- **Zertifikat** - Benachrichtigung zum Zertifikatsablaufdatum.
- **Dell Server-Ausnahmen** – Ein Dell Server-Kommunikationsfehler wirkt sich auf die Zustellung der folgenden Benachrichtigungen aus: Threat Protection, Aktualisierung, Konfig, Wissensdatenbank und Ankündigung.

Nach Auswahl einer oder mehrerer Benachrichtigungsarten klicken Sie zur Anwendung Ihrer Auswahl irgendwo oberhalb der Liste.

Wählen Sie **Ausgewählte Elemente löschen** aus, um die Auswahl in dieser Liste zurückzusetzen.

Prioritätsebenen:

ANMERKUNG: Prioritätsebenen für Benachrichtigungen beziehen sich nicht auf die Prioritätsebenen, die in anderen Dashboard-Bereichen als dem Benachrichtigungsbereich angezeigt werden.

Zur Auswahl stehen die Prioritäten kritisch, hoch, mittel und niedrig. Diese Prioritätsebenen stehen nur innerhalb einer Benachrichtigungsart zueinander im Verhältnis.

Sie können die Prioritätsebenen für Benachrichtigungen auswählen, die zu den Listen im Benachrichtigungsbereich oder den E-Mail-Benachrichtigungen im Dashboard hinzugefügt werden sollen. Benachrichtigungen der übrigen Prioritätsebenen werden nicht in der Dashboard- oder E-Mail-Benachrichtigungsliste hinzugeführt.

Wählen Sie **Ausgewählte Elemente löschen** aus, um die Auswahl in dieser Liste zurückzusetzen. Alle Benachrichtigungen werden angezeigt (sofern nicht anderswo gefiltert).

3

Richtlinien

Dieses Kapitel erläutert die Richtlinienverwaltung für Advanced Threat Prevention.

- Aktivieren von Advanced Threat Prevention
- Empfohlene Richtlinieneinstellungen
- Richtlinienänderungen festlegen

Die vollständige Liste der Richtlinien für Advanced Threat Prevention und ihre Beschreibungen finden Sie in der *AdminHelp*, die in der Verwaltungskonsole verfügbar ist.

Aktivieren von Advanced Threat Prevention

Die Richtlinie Advanced Threat Prevention ist standardmäßig auf **Aus** eingestellt und muss auf **Ein** festgelegt werden, um die Richtlinien der Advanced Threat Prevention zu aktivieren. Die Richtlinien der Advanced Threat Prevention sind auf Unternehmens-, Endpunktgruppen- und Endpunktebene verfügbar.

Zum Aktivieren der Richtlinie der Advanced Threat Prevention auf Unternehmensebene führen Sie die folgenden Schritte aus:

1. Klicken Sie im linken Bereich auf **Bestückungen > Unternehmen**.
2. Klicken Sie auf **Advanced Threat Prevention**.
3. Schalten Sie den Hauptschalter für Advanced Threat Prevention von **Aus** auf **Ein**.

Zum Aktivieren der Richtlinie Advanced Threat Prevention auf Endpunktgruppenebene führen Sie die folgenden Schritte aus:

1. Klicken Sie im linken Fensterbereich auf **Bestückungen > Endpunktgruppe**.
2. Klicken Sie auf **Advanced Threat Prevention**.
3. Schalten Sie den Hauptschalter für Advanced Threat Prevention von **Aus** auf **Ein**.

Zum Aktivieren der Richtlinie Advanced Threat Prevention auf Endpunktebene führen Sie die folgenden Schritte aus:

1. Klicken Sie im linken Fensterbereich auf **Bestückungen > Endpunkte**.
2. Klicken Sie auf **Advanced Threat Prevention**.
3. Schalten Sie den Hauptschalter für Advanced Threat Prevention von **Aus** auf **Ein**.

Empfohlene Richtlinieneinstellungen

- Die aktuellste Liste der von Dell empfohlenen Richtlinieneinstellungen finden Sie im KB-Artikel: SLN301562.

Richtlinienänderungen festlegen

So legen Sie Richtlinien fest, die geändert und gespeichert wurden:

1. Klicken Sie im linken Bereich der Verwaltungskonsole auf **Verwaltung > Bestätigung**.
2. Geben Sie in „Anmerkung“ eine Beschreibung der Änderung ein.
3. Klicken Sie auf **Richtlinien bestätigen**.

Eine Richtlinie wird dann veröffentlicht/bestätigt, wenn ein Administrator auf **Richtlinien bestätigen** klickt. Die folgenden Informationen werden angezeigt:

- Ausstehende Richtlinienänderungen – Die Anzahl von Richtlinienänderungen, die zur Festlegung bereit steht.
- Datum der Bestätigung – Datum und Uhrzeit der Richtlinienbestätigung.
- Geändert von – Benutzername des Administrators, der die Richtlinie bestätigt hat
- Kommentar – Anmerkungen, die beim Festlegen der Richtlinien hinzugefügt wurden.
- Version – Die Anzahl der Richtlinienspeicherungen seit der letzten Richtlinienbestätigung plus letzte Version.

4

Bedrohungen, die innerhalb der letzten 24 Stunden und insgesamt

Dieses Kapitel erläutert die Identifizierung und Verwaltung von Bedrohungen, die nach der Installation von Advanced Threat Prevention in einer Unternehmensumgebung auftreten können.

Identifizieren einer Bedrohung

E-Mail- und Dashboard-Benachrichtigungen

Wenn Sie E-Mail-Benachrichtigungen für Threat Protection und Advanced Threat-Ereignisse eingerichtet haben, wird ein Administrator per E-Mail über Advanced Threat Prevention-Ereignisse und Bedrohungen benachrichtigt.

Die Dashboard-Benachrichtigungszusammenfassung in der Verwaltungskonsole zeigt Advanced Threat-Bedrohungen und Ereignisse als die Benachrichtigungstypen „Threat Protection“ und „Advanced Threat-Ereignisse“ an.

- Threat Protection-Typ – Eine Bedrohungswarnung von Advanced Threat Prevention.
- Advanced Threat-Ereignistyp – Ein von Advanced Threat Prevention erkanntes Ereignis. Ein Ereignis ist nicht unbedingt eine Bedrohung.

In der folgenden Tabelle sind Bedrohungsbezeichnung, Schweregrad und Bedrohungsinformationen aufgeführt.

Bezeichnung	Schweregrad	Details
ThreatFound	Kritisch	Zeigt an, dass eine Portable Executable (PE) auf einem Gerät identifiziert, aber auf dem Endpunkt nicht blockiert oder anderweitig isoliert wurde, was auf eine aktive Bedrohung im System hinweist.
ThreatBlocked	Warnung	Zeigt an, dass eine Portable Executable auf dem Gerät identifiziert, die Ausführung jedoch blockiert wurde. Diese Bedrohung wurde nicht ausdrücklich in Quarantäne gestellt, was wahrscheinlich darauf zurückzuführen ist, dass entweder die Richtlinie für die automatische Quarantäne nicht aktiviert wurde oder dass sich die Datei in einem Verzeichnis befindet, auf das wir mit dem lokalen Systemkonto nicht schreiben konnten (Netzwerkfreigabe, USB-Gerät, das entfernt wurde usw.).
ThreatTerminated	Warnung	Zeigt an, dass eine Portable Executable (PE) auf dem Gerät erkannt und der Prozess abgebrochen wurde, da er als aktiv ausgeführt erkannt wurde. Dies zeigt nicht an, dass die Datei auch in Quarantäne gestellt wurde, da die PE möglicherweise von einem anderen Speicherort aus ausgeführt wurde. Es wird empfohlen, nach einem anderen Ereignis zu suchen, das mit diesem Endpunkt und der ausführbaren Datei korreliert ist, um zu überprüfen, ob die Bedrohung korrekt eingedämmt ist.

Bezeichnung	Schweregrad	Details
MemoryViolationBlocked	Warnung	Zeigt an, dass die Ausführung einer ausführbaren Datei oder eines Skripts fehlgeschlagen ist, aber gegen die Speicherschutz- oder Skriptsteuerungsrichtlinie verstoßen hat. Die Ausführung der ausführbaren Datei oder des Skripts wurde anschließend blockiert. In der Regel ist dies ein Hinweis darauf, dass der korrelierende Speicherschutz oder die Skript-Steuerungsrichtlinie auf Blockieren eingestellt wurde.
MemoryViolationTerminated	Warnung	Zeigt an, dass die Ausführung einer ausführbaren Datei oder eines Skripts erkannt wurde und gegen die Speicherschutz- oder Skriptsteuerungsrichtlinie verstoßen hat. Die ausführbare Datei oder das Skript wurde anschließend beendet. In der Regel ist dies ein Hinweis darauf, dass der korrelierende Speicherschutz oder die Skript-Steuerungsrichtlinie auf „Beenden“ eingestellt wurde.
MemoryViolation	Warnung	Zeigt an, dass eine ausführbare Datei oder ein Skript erkannt wurde, die bzw. das gegen die Speicherschutz- oder Skriptsteuerungsrichtlinie verstoßen hat. Gegen die ausführbare Datei oder das Skript wurde keine Maßnahme durchgeführt, da die Richtlinie wahrscheinlich auf „Zulassen“ festgelegt wurde.
ThreatRemoved	Informationen	Zeigt an, dass eine zuvor gekennzeichnete Portable Executable (PE), die als Bedrohung betrachtet wurde, vom Endpunkt entfernt wurde. Dies kann darauf hinweisen, dass die PE aus der Quarantäne entfernt oder vom ursprünglichen Speicherort entfernt wurde. Dies ist häufig bei PEs der Fall, die anfänglich auf Wechseldatenträgern (USB, CD-ROM usw.) erkannt wurden.
ThreatQuarantined	Informationen	Zeigt an, dass eine Portable Executable (PE) als potenzielle Bedrohung erkannt und später erfolgreich in die Quarantäne verschoben wurde. Dies weist darauf hin, dass die Richtlinie zur automatischen Quarantäne von Bedrohungen basierend auf der Klassifizierung Anormal (Cylance-Bewertung von 0 bis 60) oder Unsicher (Cylance-Bewertung von 60 bis 100) aktiviert ist.
ThreatWaived	Informationen	Zeigt an, dass eine Portable Executable (PE), die als potenzielle Bedrohung erkannt wurde, basierend auf der globalen sicheren Liste oder durch eine lokale Freigabe aufgehoben wurde. Dies kann auch darauf hinweisen, dass der SHA256-Hash der Richtlinien „Freigabe“ oder „Globale sichere Liste“ im Dell Security Management Server hinzugefügt wurde.
ThreatChanged	Informationen	Gibt an, wann die Cylance-Bewertung einer PE (Portable Executable) geändert wurde. Dies geschieht in der Regel aufgrund der zweistufigen Bewertung, die von Cylance durchgeführt wird. Die Analyse der Bedrohung durch die lokale Bewertungs-Engine stimmte möglicherweise nicht mit der Analyse der Cylance-Cloud-Engine überein. In diesen Fällen wird aufgrund der zusätzlichen Daten, die die Cylance-Cloud-Engine hat, die Bewertung verwendet, die von der Cylance-Cloud-Engine abgeleitet wurde. Dies kann auch darauf hinweisen, dass eine Aktualisierung auf Cylance eine erneute Analyse der Dateien initialisiert hat, die zuvor als Bedrohungen galten, und es wurde ein neuer Wert berechnet, der dieses PE nicht mehr als Bedrohung einstuft.
ProtectionStatusChanged	Informationen	Zeigt an, wann der Schutzstatus eines Endpunkts geändert wurde. Diese Funktion wird ausgelöst, wenn der Dell Encryption Management Agent die Verbindung zu den Cylance-Services über die Cylance-Plugins erneut herstellt. Dies wird im Allgemeinen ausgelöst, wenn ein Endpunkt neu gestartet wurde, da während

Bezeichnung	Schweregrad	Details
		eines kurzen Zeitraums das CSF während des Starts möglicherweise nicht mit dem Cylance-Plug-in verbunden ist.

Klicken Sie auf „Benachrichtigung“, um weitere Details aufzurufen. Die Zusammenfassung enthält Links zu weiteren Bedrohungs- oder Ereignisdetails.

Registerkarte „Advanced Threats“

Auf der Registerkarte „Advanced Threats“ werden ausführliche Ereignisinformationen für das gesamte Unternehmen auf dynamische Weise angezeigt. Sie enthält außerdem eine Liste mit Geräten, auf denen Ereignisse stattgefunden haben, mit den jeweiligen Aktionen, die auf den Geräten hinsichtlich des Ereignisses durchgeführt wurden.

Gehen Sie folgendermaßen vor, um die Registerkarte „Enterprise Advanced Threats“ aufzurufen:

1. Klicken Sie im linken Bereich auf **Bestückungen > Unternehmen**.
2. Wählen Sie die Registerkarte **Erweiterte Bedrohungen** aus.

Informationen zu Ereignissen, Geräten und Maßnahmen werden auf den folgenden Registerkarten organisiert:

- **Schutz** – Listet potenziell gefährliche Dateien und Skripte sowie Details dazu auf, einschließlich der Geräte, auf welchen die Dateien und Skripts zu finden sind.
- **Agenten** – Stellt Informationen zu den Geräten bereit, die den Advanced Threat Prevention-Client ausführen, sowie die Option zum Export der Informationen oder Entfernen von Geräte aus der Liste.
- **Globale Liste** – Listet Dateien in der globalen Quarantäne und in der sicheren Liste auf und stellt die Option zum Verschieben von Dateien in diese Listen bereit.
- **Optionen** – stellt eine Integrationsmöglichkeit mit dem „Security Information Event Management“ (SIEM) bereit.
- **Zertifikat** - Ermöglicht das Hochladen des Zertifikats. Nach dem Hochladen werden die Zertifikate auf der Registerkarte „Globale Liste“ angezeigt und können als Sicher aufgelistet werden.

Die Tabellen auf den Registerkarten können wie folgt organisiert werden:

- Spalten zur Liste hinzufügen oder entfernen - Klicken Sie auf den Pfeil neben einer Spaltenüberschrift, wählen Sie **Spalten** aus, wählen Sie die Spalten aus, die angezeigt werden sollen. Deaktivieren Sie die Kontrollkästchen der Spalten, die verborgen werden sollen.
- Daten sortieren – Klicken Sie auf eine Spaltenüberschrift.
- Nach Spalten anordnen – Ziehen Sie die Spaltenüberschrift nach oben, bis sie grün wird.

Registerkarte „Erweiterte Bedrohungsereignisse“

Auf der Registerkarte „Advanced-Threat-Ereignisse“ werden Informationen über Ereignisse für das gesamte Unternehmen auf Grundlage von auf dem Dell Server verfügbaren Informationen angezeigt.

Auf der Registerkarte wird angezeigt, ob der Dienst Advanced Threat Prevention bereitgestellt wird und Lizenzen verfügbar sind.

Um Daten von der Registerkarte „Erweiterte Bedrohungsereignisse“ zu exportieren, klicken Sie auf **Exportieren** und wählen Sie das Dateiformat **Excel** oder **CSV** aus.

ANMERKUNG: Excel-Dateien sind auf 65.000 Zeilen begrenzt. CSV-Dateien haben keine Größenbeschränkung.

Cylance Score und Gefahrenmodell-Aktualisierungen

Jeder Datei, die als Abnormal oder Unsicher gilt, wird ein bestimmter Cylance Score (Bewertungszahl) zugewiesen. Die Bewertungszahl drückt die Vertrauensstufe aus und gibt an, inwieweit es sich bei der Datei um Malware handeln könnte. Je höher die Zahl, desto größer ist das Vertrauen.

Das vorhergesagte Bedrohungsmodell, das für den Schutz der Geräte verwendet wird, empfängt regelmäßig Aktualisierungen, um die Erkennungsraten zu verbessern.

Zwei Spalten auf der Seite „Schutz“ auf der Verwaltungskonsole zeigen, welchen Einfluss ein neues Bedrohungsmodell auf Ihr Unternehmen hat. Zeigen Sie den Produktionsstatus an und vergleichen Sie diesen mit den Spalten des neuen Status, um zu erkennen, welche Dateien auf den Geräten möglicherweise von der Modelländerung beeinflusst werden.

So zeigen Sie den Produktionsstatus und die Spalten mit dem neuen Status an:

1. Klicken Sie im linken Bereich auf **Bestückungen > Unternehmen**.
2. Wählen Sie die Registerkarte **Erweiterte Bedrohungen** aus.
3. Klicken Sie auf die Registerkarte **Schutz**.
4. Klicken Sie auf den Dropdownpfeil in der Spaltenüberschrift der Tabelle.
5. Bewegen Sie den Mauszeiger über die **Spalten**.

6. Wählen Sie den **Produktionsstatus** und die Spalten mit dem **neuen Status** aus.

Produktionsstatus – Aktueller Modellstatus für die Datei (sicher, abnormal oder unsicher).

Neuer Status – Modellstatus für die Datei in dem neuen Modell.

Beispielsweise könnte eine Datei, die im aktuellen Modell als sicher angesehen wird, im neuen Modell als unsicher gelten. Wenn Ihr Unternehmen diese Datei benötigt, können Sie sie zur sicheren Liste hinzufügen. Eine Datei, die nie angezeigt oder vom aktuellen Modell bewertet wurde, kann vom neuen Modell als unsicher eingestuft werden. Wenn Ihr Unternehmen diese Datei benötigt, können Sie sie zur sicheren Liste hinzufügen.

Nur Dateien, die auf dem Gerät in Ihrer Organisation gefunden werden und die eine Änderung in der Cylance Score erfahren haben, werden angezeigt. Einige Dateien haben möglicherweise eine Bewertungsänderung erfahren, bleiben aber dennoch innerhalb des aktuellen Status. Wenn sich der Cylance Score für eine Datei von 10 auf 20 ändert, bleibt der Dateistatus abnormal und die Datei wird in der aktualisierten Modellliste angezeigt (wenn diese Datei auf Geräten in Ihrer Organisation existiert).

Vergleich des aktuellen Modells mit dem neuen Modell

Sie können die Unterschiede zwischen dem aktuellen Modell und dem neuen Modell überprüfen.

Die beiden Szenarien sollten Sie kennen:

Produktionsstatus = Sicher, neue Status = abnormal oder unsicher

- Ihr Unternehmen geht davon aus, dass die Datei sicher ist
- Ihre Organisation hat für abnormal und/oder unsicher eine automatische Quarantäne festgelegt

In den oben aufgeführten Szenarien wird empfohlen, die Dateien, die für die Organisation zugelassen werden sollen, auf die sichere Liste zu setzen.

Klassifikationen identifizieren

Zur Identifizierung der Klassifikationen, die Einfluss auf Ihre Organisation haben können, empfiehlt Dell den folgenden Ansatz:

1. Wenden Sie einen Filter auf die Spalte des neuen Status an, um alle unsicheren, abnormalen und unter Quarantäne stehenden Dateien anzuzeigen.
2. Wenden Sie einen Filter auf die Spalte des Produktionsstatus an, um alle sicheren Dateien anzuzeigen.
3. Wenden Sie einen Filter auf die Spalte Klassifizierung an, um nur vertrauenswürdige, lokale Bedrohung anzuzeigen.

Vertrauenswürdig - Lokale Dateien wurden von Cylance analysiert und als sicher befunden. Setzen Sie diese Elemente nach der Überprüfung auf die sichere Liste. Wenn Sie viele Dateien in der gefilterten Liste haben, müssen Sie ggf. mithilfe von weiteren Attributen priorisieren. Fügen Sie beispielsweise einen Filter zur Spalte „Erkannt von“ zu, um die Bedrohungen zu überprüfen, die von der Ausführungssteuerung gefunden wurden. Diese werden bewertet, sobald ein Benutzer versucht, eine Anwendung auszuführen und eine dringendere Aufmerksamkeit benötigt als inaktive Dateien, die von der Background Threat Detection oder vom File Watcher bewertet werden.

Die Informationen für den Modellvergleich stammen aus der Datenbank, nicht von Ihren Geräten. Somit wird keine erneute Analyse für den Modellvergleich unternommen. Wenn jedoch ein neues Modell verfügbar ist und ein geeigneter Agent installiert ist, wird eine erneute Analyse für Ihre Organisation durchgeführt und alle Modelländerungen werden angewendet.

Weitere Informationen finden Sie in der *AdminHelp*.

Anzeigen von Web-Schutz- und Firewall-Ereignissen

Bedrohungen werden in die Kategorien Malware/Exploit, Web-Filter, Firewall und Ohne Kategorie unterteilt. Die Liste der Bedrohungsereignisse kann nach einer beliebigen Spaltenüberschrift sortiert werden. Sie können die Bedrohungsereignisse für das gesamte Unternehmen oder für einen bestimmten Endpunkt anzeigen. Um die Bedrohungsereignisse eines bestimmten Endpunkts anzuzeigen, wählen Sie auf der Registerkarte „Bedrohungsereignisse – Unternehmen“ in der Spalte „Geräte-ID“ das Gerät aus.

Gehen Sie folgendermaßen vor, um die Bedrohungsereignisse im Unternehmen anzuzeigen:

1. Klicken Sie im linken Bereich auf **Bestückungen > Unternehmen**.
2. Klicken Sie auf die Registerkarte **Bedrohungsereignisse**.
3. Wählen Sie den Schweregrad und den Zeitraum aus, für den Ereignisse angezeigt werden sollen.

Gehen Sie folgendermaßen vor, um die Bedrohungen auf einem bestimmten Endpunkt anzuzeigen:

1. Klicken Sie im linken Fensterbereich auf **Bestückungen > Endpunkte**.
2. Suchen oder wählen Sie einen Hostnamen aus, und klicken Sie anschließend auf die Registerkarte **Bedrohungsereignisse**.

Bedrohung verwalten

Sie können Bedrohungen unter Quarantäne stellen, auf die sichere Liste setzen, verwerfen und exportieren.

Führen Sie die folgenden Maßnahmen auf Unternehmensebene aus:

- Exportieren einer Bedrohung oder eines Skripts, die/das eine Warnung ausgelöst hat
- Verschieben einer Bedrohung in Quarantäne
- Bedrohung auf die sichere Liste setzen
- Globale Liste manuell bearbeiten

So verwalten Sie eine Bedrohung, die auf Unternehmensebene identifiziert wurde:

1. Klicken Sie im linken Bereich auf **Bestückungen > Unternehmen**.
2. Wählen Sie die Registerkarte **Erweiterte Bedrohungen** aus.
3. Wählen Sie „Protection“ aus.

Aus der Tabelle „Skriptsteuerung“ können Sie ein Skript exportieren, das in der Tabelle als potenzielle Bedrohung aufgeführt wird.

Erweiterte Unternehmensbedrohungen verwalten

Auf der Registerkarte „Schutz“ finden Sie Informationen zu potenziell schädlichen Dateien und Skripten.

Tabelle der Bedrohungen

Von der Tabelle der Bedrohungen können Sie eine Bedrohung exportieren, unter Quarantäne stellen oder der sicheren Liste hinzufügen. Sie können eine Bedrohung auch manuell der globalen Quarantäneliste hinzufügen.

In der Tabelle sind alle Ereignisse aufgeführt, die innerhalb der Organisation gefunden wurden. Ein Ereignis kann, aber muss nicht gleichzeitig eine Bedrohung sein.

Um zusätzliche Informationen zu einer bestimmten Bedrohung anzuzeigen, klicken Sie entweder auf den Link mit dem Namen der Bedrohung (Details werden auf einer neuen Seite angezeigt) oder an eine beliebige Stelle in die Zeile mit der Bedrohung (Details werden auf derselben Seite unten angezeigt).

Um zusätzliche Informationen zu einer Bedrohung in der Tabelle anzuzeigen, klicken Sie auf den Dropdown-Pfeil in der Spaltenüberschrift, um die Spalten auszuwählen und hinzuzufügen. Die Spalten zeigen Metadaten zur Datei an, wie Klassifizierungen, Cylance Score (Vertrauensebene), AV Industry-Überzeugung (verlinkt auf VirusTotal.com für den Vergleich mit anderen Anbietern), das Datum des ersten Vorkommnisses, SHA256, MD5, Dateiinformationen (Autor, Beschreibung, Version) und Signaturdetails.

Befehle

- **Export** – Exportieren Sie die Bedrohungsdaten in eine CSV-Datei. Wählen Sie die zu exportierenden Zeilen aus und klicken Sie anschließend auf **Export**.
- **Globale Quarantäne** – Eine Datei zur globalen Quarantäneliste hinzufügen. Die Bedrohung ist für alle Geräte dauerhaft unter Quarantäne gestellt.
- **Speichern** – Eine Datei zur sicheren Liste hinzufügen. Die Datei wird auf allen Geräten dauerhaft als sicher behandelt.

  ANMERKUNG: Gelegentlich kommt es vor, dass eine „gutartige“ Datei als unsicher gemeldet wird. (Dies ist der Fall, wenn die Merkmale der Datei den Merkmalen bösartiger Dateien stark ähneln.) In einer solchen Situation kann das Freigeben oder Verschieben der Datei in die sichere Liste hilfreich sein.

- **Globale Liste bearbeiten** – Dateien der globalen Quarantäneliste hinzufügen oder aus ihr entfernen.
- **Verwerfen** – Eine Datei zur Verwerfen-Liste auf einem Computer hinzufügen. Diese Datei darf auf dem Computer ausgeführt werden.

Erweiterte Endpunktbedrohungen verwalten

So verwalten Sie eine Bedrohung, die auf einem bestimmten Computer identifiziert wurde:

1. Klicken Sie im linken Bereich auf **Bestückungen > Unternehmen**.
2. Wählen Sie die Registerkarte **Erweiterte Bedrohungen** aus.
3. Wählen Sie „Agenten“.
4. Wählen Sie einen bestimmten Agentennamen und wählen Sie den entsprechenden Befehl für eine Bedrohung aus: **Export**, **Quarantäne** oder **Verwerfen**.

5

Getrennter Modus

Der getrennte Modus ermöglicht einem Dell Server die Verwaltung der Advanced Threat Prevention-Endpunkte ohne Client-Verbindung mit dem Internet oder externen Netzwerk. Der getrennte Modus ermöglicht dem Dell Server außerdem die Verwaltung von Clients ohne Internetverbindung oder einen bereitgestellten und gehosteten Advanced Threat Prevention-Dienst. Der Dell Server erfasst im getrennten Modus alle Ereignis- und Bedrohungsdaten.

Um zu ermitteln, ob ein Dell Server im getrennten Modus läuft, klicken Sie auf das Zahnradsymbol oben rechts von der Remote Management Console und wählen Sie Info aus. Der Info-Bildschirm zeigt unter Dell Server-Version an, dass sich ein Dell Server im getrennten Modus befindet.

Der getrennte Modus unterscheidet sich von einer verbundenen Standardinstallation des Dell Server auf folgende Weise:

Client-Aktivierung

Ein Installationstoken wird erzeugt, wenn der Administrator ein Advanced Threat Prevention-Lizenz lädt, wodurch der Advanced Threat Prevention-Client aktiviert werden kann.

Management Console

Folgende Elemente sind in der Verwaltungskonsole **nicht verfügbar**, wenn der Dell Server im getrennten Modus ausgeführt wird:

- Die folgenden Bereiche sind spezifisch für die Advanced Threat Prevention: erweiterte Bedrohungen nach Priorität, (erweiterte Bedrohungs-) Ereignisse nach Klassifizierung, Top Ten der erweiterte Bedrohungen und Advanced Threat Prevention-Ereignisse.
- **Unternehmen > Erweiterte Bedrohungen** Auf der Registerkarte „Erweiterte Bedrohungen“ werden ausführliche Ereignisinformationen für das gesamte Unternehmen auf dynamische Weise angezeigt. Sie enthält außerdem eine Liste mit Geräten, auf denen Ereignisse stattgefunden haben mit den jeweiligen Aktionen, die auf den Geräten hinsichtlich des Ereignisses durchgeführt wurden.
- (Linker Navigationsbereich) Dienstverwaltung, die das Aktivieren des Advanced Threat Prevention-Service und der Produktbenachrichtigungs-Registrierung ermöglicht.

Die folgenden Elemente sind in der Verwaltungskonsole **verfügbar**, um den getrennten Modus zu unterstützen:

- Registerkarte **Unternehmen > Advanced Threat-Ereignisse**, die eine Liste mit Ereignisinformationen für das gesamte Unternehmen enthält, die auf den Informationen basieren, die dem Dell Server zur Verfügung stehen, selbst wenn er im getrennten Modus läuft.

Funktionalität

Folgende Funktionen sind in der Verwaltungskonsole nicht verfügbar, wenn der Dell Server im getrennten Modus ausgeführt wird:

- Security Management Server Upgrade, Aktualisierung und Migration
- Automatische Aktualisierung von Security Management Server Virtual – Update muss manuell durchgeführt werden.
- Cloud-Profilaktualisierung
- Advanced Threat Prevention – automatische Aktualisierung
- Hochladen von unsicheren oder abnormalen ausführbaren Dateien für die Analyse von Advanced Threat Prevention
- Advanced Threat Prevention-Datei hochladen und Protokolldatei hochladen

Die folgende Funktionalität ist anders:

- Der Dell Server sendet die globale sichere Liste, die Quarantäneliste und die sichere Liste an Agenten.
- Die globale sichere Liste wird mit der Global-zulassen-Richtlinie auf den Dell Server importiert.
- Die Quarantäneliste wird mit der Quarantänelisten-Richtlinie auf den Dell Server importiert.
- Die sichere Liste wird mit der Sichere-Liste-Richtlinie auf den Dell Server importiert

Diese Richtlinien sind nur im getrennten Modus verfügbar. Weitere Informationen über diese Richtlinien finden Sie in der *AdminHelp*, die in der Dell Server Remote-Verwaltungskonsole verfügbar ist.

Weitere Informationen zum getrennten Modus finden Sie unter „Getrennter Modus“ in der *AdminHelp*, die in der Verwaltungskonsole verfügbar ist.

Identifizierung und Verwaltung von Bedrohungen im getrennten Modus

Zur Verwaltung von Bedrohungen im getrennten Modus müssen Sie zuerst die folgenden Advanced Threat Prevention-Richtlinien festlegen, je nachdem welche für Ihr Unternehmen gelten:

- Global zulassen
- Quarantäneliste
- Sichere Liste

Diese Richtlinien werden nur dann an den Advanced Threat Prevention-Client gesendet, wenn der Dell Server einen Installationstoken für den getrennten Modus mit dem Präfix „DELLAG“ erkennt.

In der *AdminHelp* finden Sie Beispiele für diese Richtlinien.

Zum Anzeigen von Dateien, die Advanced Threat Prevention als potenzielle Bedrohungen identifiziert hat, navigieren Sie zur Registerkarte **Unternehmen > Advanced Threat-Ereignisse**. Diese Registerkarte enthält eine Liste der Ereignisinformationen für das gesamte Unternehmen und die ergriffenen Maßnahmen, wie z. B. blockiert oder beendet.

6

Fehlerbehebung

Wiederherstellen von Advanced Threat Prevention

Wiederherstellen des Dienstes

Um den Advanced Threat Prevention-Dienst wiederherzustellen, benötigen Sie das gesicherte Zertifikat.

1. Klicken Sie im linken Bereich der Verwaltungskonsole auf **Verwaltung > Dienstverwaltung**.
2. Klicken Sie auf **Advanced Threat Prevention-Dienst wiederherstellen**.
3. Folgen Sie den Anweisungen des geführten Wiederherstellungsverfahrens und laden Sie das Zertifikat für Advanced Threat Prevention bei entsprechender Aufforderung hoch.

Produktcode mit Windows PowerShell ermitteln

- Sie können den Produktschlüssel über dieses Verfahren leicht identifizieren, wenn er sich in der Zukunft ändern sollte.

  ```
  Get-WmiObject  Win32_Product | Where-Object {$_.Name -like '*Cylance*'} | FT IdentifyingNumber, Name, LocalPackage
  ```

  Die Ausgabe hat den vollständigen Pfad und den MSI-Dateinamen (den konvertierten HEX-Namen der Datei) zur Folge.

Advanced Threat Prevention

- Damit das Advanced Threat Prevention-Plugin „HKLM\SOFTWARE\Dell\Dell Data Protection“ Änderungen des Werts „LogVerbosity“ überwacht und die Client-Protokollierungsebene entsprechend aktualisiert, legen Sie den folgenden Wert fest.

  [HKLM\SOFTWARE\Dell\Dell Data Protection]

  "LogVerbosity"=DWORD:<see below>

  Dump: 0

  Schwerwiegender Fehler: 1

  Fehler 3

  Warnung 5

  Info 10

  Ausführlich 12

  Verfolgen 14

  Debuggen 15

  Der Registrierungswert ist aktiviert, wenn der Advanced Threat Prevention-Dienst startet oder immer dann, wenn der Wert sich ändert. Wenn der Registrierungswert nicht vorhanden ist, gibt es keine Änderung auf der Protokollierungsebene.

  Verwenden Sie diese Registrierungseinstellung nur für Prüfungs-/Debugging-Aktivitäten, da sie die Ausführlichkeitsstufe für andere Komponenten steuert, einschließlich Encryption und Encryption Management Agent.

- Mit dem Kompatibilitätsmodus können Anwendungen auf dem Client-Computer ausgeführt werden, während die Richtlinien Speicherschutz oder Speicherschutz und Skriptsteuerung aktiviert sind. Das Aktivieren des Kompatibilitätsmodus macht das Hinzufügen eines Registrierungswerts auf dem Clientcomputer notwendig.

  Führen Sie zur Aktivierung des Kompatiblitätsmodus die folgenden Schritte aus:

  1. Deaktivieren Sie in der Verwaltungskonsole die Richtlinie *Speicherschutz aktiviert*. Wenn die *Skriptsteuerung*srichtlinie aktiviert ist, deaktivieren Sie sie.

2. Fügen Sie die Registrierungswert CompatibilityMode hinzu.
   a. Gehen Sie mithilfe des Registrierungs-Editors auf dem Client-Computer zu `HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop`.
   b. Klicken Sie mit der rechten Maustaste auf **Desktop**, klicken Sie auf **Berechtigungen**, übernehmen Sie dann den Besitz und gewähren Sie sich selbst Vollzugriff.
   c. Klicken Sie mit der rechten Maustaste auf **Desktop**, wählen Sie dann **Neu Binarwert** aus.
   d. Geben Sie für den Namen `CompatibilityMode` ein.
   e. Öffnen Sie die Einstellung der Registrierungsdatei und ändern Sie den Wert in `01`.
   f. Klicken Sie auf **OK**, und schließen Sie dann den Registrierungs-Editor.

   Zum Hinzufügen des Registrierungswerts durch einen Befehl können Sie eine der folgenden Befehlszeilenoptionen zur Ausführung auf dem Clientcomputer verwenden:

   - (Für einen einzigen Computer) Psexec:

     ```
     psexec -s reg add HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop /v
     CompatibilityMode /t REG_BINARY /d 01
     ```

   - (Für mehrere Computer) Invoke-Command cmdlet:

     ```
     $servers = "testComp1","testComp2","textComp3"

     $credential = Get-Credential -Credential {UserName}\administrator

     Invoke-Command -ComputerName $servers -Credential $credential -ScriptBlock {New-Item
     -Path HKCU:\Software\Cylance\Desktop -Name CompatibilityMode -Type REG_BINARY -Value
     01}
     ```

3. Aktivieren Sie in der Verwaltungskonsole die Richtlinie *Speicherschutz aktiviert* erneut. Wenn die *Skriptsteuerung*srichtlinie zuvor aktiviert war, aktivieren Sie sie erneut.