Dell Threat Defense –
Installations- und Administrator-Handbuch

Powered by Cylance
v17.06.16

16.06.2017

Inhaltsverzeichnis

ÜBERSICHT

Dell Threat Defense auf Basis von Cylance erkennt und blockiert Malware, bevor sie dem Gerät schadet. Cylance verfolgt einen mathematischen Ansatz zur Identifizierung von Malware, der auf maschinellen Lernverfahren beruht, statt auf reaktiven Signaturen, vertrauensbasierten Systemen oder Sandkästen. Durch diesen Ansatz werden neue Malware, Viren, Bots und künftige Varianten nutzlos. Threat Defense analysiert potenzielle Dateiausführungen von Malware im Betriebssystem.

In diesem Handbuch werden die Verwendung der Threat Defense Console, die Installation des Threat Defense Agent und die Konfiguration dieser beiden Komponenten erläutert.

So wird's gemacht

Threat Defense besteht aus einem kleinen Agenten, der auf jedem Host installiert ist, der mit der cloudbasierten Konsole kommuniziert. Der Agent erkennt und verhindert Malware auf dem Host anhand von erprobten mathematischen Modellen. Er erfordert weder eine kontinuierliche Cloudkonnektivität, noch regelmäßige Signaturaktualisierungen, und funktioniert sowohl in offenen als auch isolierten Netzwerken. Threat Defense passt sich kontinuierlich der immer wieder neuen Bedrohungslandschaft an. Durch konstantes Training an enormen, realen Datensets ist Threat Defense Angreifern immer einen Schritt voraus.

- **Bedrohung:** Wenn eine Bedrohung auf das Gerät heruntergeladen oder ein Exploit-Versuch unternommen wird.
- **Erkennung von Bedrohungen**: Wie Threat Defense Agent Bedrohungen identifiziert.
    - **Prozess-Scan**: Überprüft Prozesse, die auf dem Gerät ausgeführt werden.
    - **Ausführungssteuerung:** Analysiert Prozesse nur bei Ausführung. Dies umfasst alle Dateien, die beim Start ausgeführt werden, die für die automatische Ausführung konfiguriert sind, und die manuell durch den Benutzer ausgeführt werden.
- **Analyse**: Wie Dateien als bösartig oder sicher identifiziert werden.
    - **Cloud Lookup für Bedrohungsbewertungen:** Das mathematische Modell in der Cloud, das zur Bewertung von Dateien herangezogen wird.
    - **Lokal:** Das im Agenten enthaltene mathematische Modell. Dieses ermöglicht die Analyse, wenn das Gerät nicht mit dem Internet verbunden ist.
- **Maßnahme:** Was der Agent unternimmt, wenn eine Datei als Bedrohung identifiziert wird.
    - **Global:** Überprüft Richtlinieneinstellungen, einschließlich der *globalen Quarantäne* und *sicheren Listen*.
    - **Lokal:** Sucht nach Dateien, die manuell *in Quarantäne verschoben* oder *freigegeben* wurden.

Wissenswertes zu diesem Handbuch

Dell empfiehlt Benutzern, sich vor der Installation des Agenten auf Endpunkten mit der cloudbasierten Konsole vertraut zu machen. Schutz und Wartung von Endpunkten sind einfacher, wenn der Benutzer versteht, wie sie verwaltet werden. Dieser Workflow ist eine Empfehlung. Benutzern steht es frei, die Bereitstellung in ihrer Umgebung so durchzuführen, wie es für sie am besten geeignet ist.

Beispiel: Zonen sind hilfreich, um Geräte innerhalb einer Organisation zu gruppieren. Sie können beispielsweise eine Zone mit einer Zonenregel konfigurieren, die neue Geräte automatisch basierend auf bestimmten Kriterien (z. B. Betriebssystem, Gerätename oder Domänenname) einer Zone zuordnet.

Hinweis: Die Anleitungen zum Installieren des Agenten folgen im Anschluss an die Abschnitte über Richtlinien und Zonen. Benutzer können bei Bedarf direkt mit der Installation des Agenten beginnen.

KONSOLE

Die Threat Defense Console ist eine Website, an der sich der Benutzer anmelden kann, um Bedrohungsinformationen für seine Organisation anzuzeigen. Die Konsole vereinfacht die Anordnung von Geräten in Gruppen (Zonen), die Konfiguration von Maßnahmen bei Erkennung einer Bedrohung auf einem Gerät (Richtlinie) und das Herunterladen der Installationsdateien (Agent).

Die Threat Defense Console unterstützt die folgenden Sprachen.

Französisch	Deutsch	Italienisch	Japanisch
Portugiesisch (iberisch)	Koreanisch	Spanisch	Portugiesisch (brasilianisch)

Tabelle 1: Unterstützte Threat Defense Console Sprachen

Anmelden

Bei Aktivierung Ihres Kontos erhalten Sie eine E-Mail, in der Ihre Anmeldeinformationen für die Threat Defense Console enthalten sind. Klicken Sie auf den in der E-Mail enthaltenen Link, um die Anmeldeseite aufzurufen, oder rufen Sie die folgende Website auf:

- Nordamerika: http://dellthreatdefense.com
- Europa: http://dellthreatdefense-eu.cylance.com

Geräterichtlinie

Anhand von Richtlinien wird festgelegt, wie der Agent mit erkannter Malware umgehen soll. Zum Beispiel, die Malware in *Quarantäne* zu verschieben oder sie zu ignorieren, wenn sie sich in einem bestimmten Ordner befindet. Jedes Gerät muss einer Richtlinie zugeordnet sein, wobei immer nur eine Richtlinie für ein Gerät angewendet werden kann. Durch die Begrenzung auf eine Richtlinie werden Konflikte verhindert (z. B. Blockieren einer Datei, obwohl sie eigentlich erlaubt sein sollte). Wenn keine Richtlinie zugewiesen ist, wird das Gerät der Standardrichtlinie zugeteilt.

Die Standardrichtlinie sieht lediglich die Ausführungssteuerung vor, d. h. Prozesse werden nur bei Ausführung analysiert. Dadurch wird für einen grundlegenden Schutz des Geräts gesorgt, die Abläufe auf dem Gerät werden nicht unterbrochen und es bleibt Zeit, die Richtlinienfunktionen zu testen, bevor die Richtlinie in der Produktionsumgebung bereitgestellt wird.

So fügen Sie eine Richtlinie hinzu:

1. Melden Sie sich als Administrator bei der Konsole (http://dellthreatdefense.com) an. Nur Administratoren können Richtlinien erstellen.
2. Wählen Sie **Einstellungen** > **Geräterichtlinie** aus.
3. Klicken Sie auf **Neue Richtlinie hinzufügen**.
4. Geben Sie einen Richtliniennamen ein, und wählen Sie die Optionen für die Richtlinie aus.
5. Klicken Sie auf **Erstellen**.

Dateimaßnahmen

EINSTELLUNGEN > Geräterichtlinie > [Richtlinie auswählen] > Dateimaßnahmen

In den Dateimaßnahmen werden verschiedene Optionen für den Umgang mit Dateien angeboten, die von Threat Defense als *Unsicher* oder *Abnormal* erkannt wurden.

Tipp: Weitere Informationen zur Klassifizierung von *unsicheren* oder *abnormalen* Dateien finden Sie im Abschnitt Schutz – Bedrohungen.

Automatische Quarantäne mit Ausführungssteuerung

Diese Funktion stellt die *unsichere* oder *abnormale* Datei unter *Quarantäne*, um zu verhindern, dass sie ausgeführt wird. Das Verschieben in *Quarantäne* bedeutet, dass die Datei vom ursprünglichen Speicherort in das *Quarantäneverzeichnis* verschoben wird: **`C:\ProgramData\Cylance\Desktop\q`**.

Bestimmte Malware ist darauf ausgelegt, andere Dateien in bestimmte Verzeichnisse abzulegen. Die Malware versucht diesen Vorgang so lange, bis er erfolgreich ist. Threat Defense modifiziert die abgelegte Datei so, dass sie nicht ausgeführt wird, und verhindert dadurch, dass die Malware kontinuierlich versucht, die Datei abzulegen.

Tipp: Dell empfiehlt, die *Automatische Quarantäne* auf einer geringen Anzahl von Geräten zu testen, bevor Sie sie in der Produktionsumgebung anwenden. Die Testergebnisse sollten sorgfältig überprüft werden, um sicherzustellen, dass keine geschäftskritischen Anwendungen an der Ausführung gehindert werden.

Automatisch hochladen

Dell empfiehlt, dass Benutzer den automatischen Upload für *unsichere* und *abnormale* Dateien aktivieren. Threat Defense lädt automatisch alle erkannten *unsicheren* oder *abnormalen* Dateien zur ihrer genaueren Analyse in die Cylance Infinity Cloud hoch und gibt zusätzliche Details an.

Threat Defense lädt und analysiert nur unbekannte PE-Dateien (Portable Executable). Falls dieselbe unbekannte Datei auf mehreren Geräten der Organisation erkannt wird, lädt Threat Defense nur eine davon zur Analyse hoch, und nicht jede Datei auf den einzelnen Geräten.

Richtlinie „Sichere Liste“

Sie können Dateien, die als sicher gelten, auf Richtlinienebene hinzufügen. Der Agent führt keine Bedrohungsmaßnahmen an Dateien durch, die in dieser Liste enthalten sind.

Weitere Informationen zur Handhabung von Dateiausnahmen (*Quarantäne* oder *Sicher*) auf den verschiedenen Ebenen (*Lokal*, *Richtlinie* oder *Global*) finden Sie in Anhang B: Handhaben von Ausnahmen.

1. Melden Sie sich als Administrator bei der Konsole (http://dellthreatdefense.com) an. Nur Administratoren können Richtlinien erstellen.
2. Wählen Sie **Einstellungen** > **Geräterichtlinie** aus.

3. Fügen Sie eine neue Richtlinie hinzu, oder bearbeiten Sie eine bereits vorhandene Richtlinie.
4. Klicken Sie auf **Datei hinzufügen** unter *Richtlinie „Sichere Liste“*.
5. Geben Sie die **SHA256**-Informationen ein. Falls bekannt, geben Sie die MD5-Informationen und den Dateinamen an.
6. Wählen Sie eine **Kategorie** aus, um zu identifizieren, was diese Datei tut.
7. Geben Sie einen Grund ein, weshalb die Datei zur Richtlinie *Sichere Liste* hinzugefügt wird.
8. Klicken Sie auf **Senden**.

Schutzeinstellungen

EINSTELLUNGEN > Geräterichtlinie > [Richtlinie auswählen] > Schutzeinstellungen

Ausführungssteuerung

Threat Defense überwacht konstant die Ausführung bösartiger Prozesse und sendet eine Warnung, wenn versucht wird, ein Objekt der Kategorie *Unsicher* oder *Abnormal* auszuführen.

Herunterfahren des Dienstes vom Gerät verhindern

Falls diese Option markiert ist, wird verhindert, dass der Dienst „Threat Protection“ manuell oder durch einen anderen Prozess heruntergefahren werden kann.

Malware-Muster kopieren

Ermöglicht die Angabe einer Netzwerkfreigabe, in der Malware-Muster kopiert werden. Auf diese Weise können Benutzer ihre eigene Analyse von Dateien durchführen, die von Threat Defense als *unsicher* oder *abnormal* eingestuft werden.

- Es werden CIFS- und SMB-Netzwerkfreigaben unterstützt.
- Geben Sie den Speicherort einer Netzwerkfreigabe an. Beispiel: **`c:\test`**.
- Alle Dateien, die den festgelegten Kriterien entsprechen, werden in die Netzwerkfreigabe kopiert, auch Duplikate. Es wird kein Test auf Einzigartigkeit durchgeführt.
- Dateien werden nicht komprimiert.
- Die Dateien sind nicht durch ein Passwort geschützt.

WARNUNG: DIE DATEIEN SIND NICHT DURCH EIN PASSWORT GESCHÜTZT. ES MUSS DARAUF GEACHTET WERDEN, DASS DIE BÖSARTIGE DATEI NICHT VERSEHENTLICH AUSGEFÜHRT WIRD.

Skriptsteuerung

Die Skriptsteuerung schützt Geräte, indem die Ausführung bösartiger Skripte vom Typ Active Script und PowerShell gesperrt wird.

1. Melden Sie sich an der Konsole an (http://dellthreatdefense.com).
2. Wählen Sie **Einstellungen** > **Geräterichtlinie** aus.
3. Wählen Sie eine Richtlinie aus, und klicken Sie auf **Schutzeinstellungen**.
4. Markieren Sie das Kontrollkästchen, um die **Skriptsteuerung** zu aktivieren.

a. **Warnung:** Überwacht Skripte, die in der Umgebung ausgeführt werden. Wird für die Erstbereitstellung empfohlen.

b. **Blockieren:** Sorgt dafür, dass Skripte nur von bestimmten Ordnern aus ausgeführt werden können. Verwenden Sie diese Option nach dem Testen im Warnmodus.

c. **Skripte in diesen Ordnern (und Unterordnern) genehmigen**: Für Skriptordnerausnahmen muss der relative Pfad zum Ordner angegeben werden.

d. **PowerShell-Konsolennutzung blockieren**: Blockiert den Start der PowerShell-Konsole. Diese bietet zusätzliche Sicherheit durch den Schutz vor Verwendung durch PowerShell-Online-Benutzer.

   Hinweis: Wenn das Skript die PowerShell-Konsole startet und die Skriptsteuerung so eingestellt ist, dass die PowerShell-Konsole blockiert wird, schlägt das Skript fehl. Es wird empfohlen, dass die Benutzer Ihre Skripte ändern, um anstelle der PowerShell-Konsole die PowerShell-Skripte aufzurufen.

5. Klicken Sie auf **Speichern**.

Agentenprotokolle

EINSTELLUNGEN > Geräterichtlinie > [Richtlinie auswählen] > Agentenprotokolle

Aktivieren Sie die Agentenprotokolle in der Konsole, um Protokolldateien hochzuladen und deren Anzeige in der Konsole zu ermöglichen.

1. Melden Sie sich an der Konsole an (http://dellthreatdefense.com).
2. Wählen Sie **Einstellungen** > **Geräterichtlinie** aus.
3. Wählen Sie eine Richtlinie aus, und klicken Sie auf **Agentenprotokolle**. Stellen Sie sicher, dass das für die Protokolldateien ausgewählte Gerät dieser Richtlinie zugewiesen ist.
4. Wählen Sie **Automatisches Hochladen von Protokolldateien aktivieren** aus, und klicken Sie auf **Speichern**.
5. Klicken Sie auf die Registerkarte **Geräte**, und wählen Sie ein Gerät aus.
6. Klicken Sie auf **Agentenprotokolle**. Die Protokolldateien werden angezeigt.
7. Klicken Sie auf eine Protokolldatei. Der Name der Protokolldatei entspricht dem Protokolldatum.

Bewährte Verfahren für Richtlinien

Wenn Richtlinien erstmalig erstellt werden, empfiehlt Dell, die Richtlinienfunktionen phasenweise zu implementieren, um sicherzustellen, dass Leistung und Betrieb nicht beeinträchtigt werden. Wenn Sie etwas besser mit der Funktionsweise von Threat Defense in Ihrer Umgebung vertraut sind, können Sie weitere Richtlinien mit mehr aktivierten Funktionen erstellen.

1. Aktivieren Sie bei der Erstellung der ersten Richtlinien nur **Automatisches Hochladen**.
    a. Der Agent verwendet Ausführungssteuerung und Prozessüberwachung, um nur die ausgeführten Prozesse zu analysieren.

       Dies umfasst alle Dateien, die beim Start ausgeführt werden, die für die automatische Ausführung konfiguriert sind, und die manuell durch den Benutzer ausgeführt werden.

       Der Agent sendet lediglich Warnungen an die Konsole. Es werden keine Dateien blockiert oder *unter Quarantäne gestellt*.

    b. Überprüfen Sie, ob in der Konsole Warnungen zu Bedrohungen vorhanden sind.

       Ziel ist die Identifizierung von Anwendungen oder Prozessen, die am Endpunkt ausgeführt werden müssen, aber als Bedrohung eingestuft wurden (*Abnormal* oder *Unsicher*).

       Falls dies geschieht, konfigurieren Sie eine Richtlinie oder Konsoleneinstellung so, dass sie die Ausführung dieser Prozesse *Zulassen* (z. B. *Ausschließen* von Ordnern in einer Richtlinie, *Freigeben* der Dateien für das Gerät oder Hinzufügen der Dateien zur Richtlinie *Sichere Liste*).

    c. Verwenden Sie dieses erste Richtlinie einen Tag lang, um Anwendungen und Prozesse auszuführen und zu analysieren, die in der Regel auf dem Gerät verwendet werden.

WICHTIGER HINWEIS: Bestimmte Anwendungen und Prozesse, die regelmäßig auf einem Gerät ausgeführt werden (z. B. einmal pro Monat), werden möglicherweise als Bedrohung eingestuft. Sie können selbst entscheiden, ob Sie diese während der anfänglichen Richtlinie ausführen oder das Gerät bei der nächsten planmäßigen Ausführung überwachen möchten.

2. Aktivieren Sie nach Abschluss von Ausführungssteuerung und Prozessüberwachung unter Schutzeinstellungen die Option **Unsichere laufende Prozesse eliminieren**.

   Durch die Funktion „Unsichere laufende Prozesse (und Unterprozesse) eliminieren“ werden Prozesse (und deren Unterprozesse) bei Erkennung einer Bedrohung zustandsunabhängig eliminiert (EXE oder MSI).

3. Schalten Sie unter Dateimaßnahmen **Automatische Quarantäne** ein.

   Automatische Quarantäne verschiebt schädliche Dateien in den *Quarantäne*-Ordner.

4. Schalten Sie unter Schutzeinstellungen **Skriptsteuerung** ein.

   Die Skriptsteuerung sorgt dafür, dass keine bösartigen Skripte auf den Benutzergeräten ausgeführt werden.

   Benutzer haben die Möglichkeit, die Ausführung von Skripten für bestimmte Ordner zuzulassen.

   Für Skriptsteuerungs-Ordnerausnahmen muss der relative Pfad zum Ordner angegeben werden (z. B. **`\Cases\ScriptsAllowed`**).

Zonen

Zonen ermöglichen die Anordnung und Verwaltung von Geräten. So können Geräte beispielsweise nach geografischem Standort oder Funktion unterteilt werden. Bestimmte geschäftskritische Geräte können in einer Gruppe zusammengefasst, und der Zone anschließend eine hohe Priorität zugewiesen werden. Zusätzlich können Richtlinien auf Zonenebene angewendet werden. So können beispielsweise Geräte basierend auf der auf ihnen angewendeten Richtlinie in einer Zone zusammengefasst werden.

Jede Organisation verfügt über eine Standardzone (Zonenlos), auf die nur Administratoren Zugriff haben. Neue Geräte werden immer dann der Zone „Zonenlos“ zugewiesen, wenn keine Zonenregeln vorhanden sind, die eine automatische Zuweisung der Geräte in eine andere Zone vorsehen.

Zonenmanager und Benutzer können einer Zone zugewiesen werden. Sie haben dann die Möglichkeit, die Konfiguration der Zone anzuzeigen. So können Zonenmanager und Benutzer auf die von ihnen betreuten Geräte zugreifen. Es muss mindestens eine Zone vorhanden sein, damit die Anzeige durch einen Zonenmanager oder Benutzer eingerichtet werden kann.

Ein Gerät kann mehreren Zonen angehören, allerdings kann immer nur eine Richtlinie für ein Gerät angewendet werden. Die Unterstützung mehrerer Zonen bietet eine gewisse Flexibilität bei der Gruppierung von Geräten. Durch die Begrenzung auf eine Richtlinie werden Konflikte verhindert (z. B. Blockieren einer Datei, obwohl sie eigentlich *erlaubt* sein sollte).

Ein Gerät kann aus folgenden Gründen in mehreren Zonen vorhanden sein:

- Das Gerät wurde manuell mehreren Zonen hinzugefügt.
- Das Gerät entspricht den Regeln mehrerer Zonen.
- Das Gerät ist bereits in einer Zone vorhanden und entspricht auch den Regeln einer später angelegten Zone.

Empfohlene Vorgehensweisen zum Verwalten von Zonen finden Sie unter Bewährte Verfahren zum Verwalten von Zonen.

So fügen Sie eine Zone hinzu:

1. Melden Sie sich als Administrator bei der Konsole (http://dellthreatdefense.com) an. Nur Administratoren können Zonen erstellen.
2. Klicken Sie auf **Zonen**.
3. Klicken Sie auf **Neue Zone hinzufügen**.
4. Geben Sie einen Zonennamen ein, wählen Sie eine Richtlinie und anschließend einen Wert aus. Eine Zone muss mit einer Richtlinie verknüpft sein. Der Wert entspricht der Priorität der Zone.
5. Klicken Sie auf **Speichern**.

So fügen Sie Geräte zu einer Zone hinzu:

1. Melden Sie sich bei der Konsole (http://dellthreatdefense.com) mit einem Administrator- oder Zonenmanager-Konto an.
2. Klicken Sie auf **Zonen**.
3. Klicken Sie in der *Zonenliste* auf eine Zone. Die aktuellen Geräte in dieser Zone werden in der *Liste der Zonengeräte* am unteren Seitenrand angezeigt.
4. Klicken Sie auf **Geräte zur Zone hinzufügen**. Eine Liste mit Geräten wird angezeigt.
5. Wählen Sie die Geräte aus, die Sie der Zone hinzufügen möchten, und klicken Sie auf **Speichern**. Wählen Sie ggf. **Zonenrichtlinie auf die ausgewählten Geräte anwenden** aus. Durch das Hinzufügen eines Geräts zu einer Zone wird dem Gerät nicht automatisch die Zonenrichtlinie übertragen. Der Grund dafür ist, dass eine Zone auch zum Anordnen von Geräten verwendet werden kann, und nicht nur zum Verwalten der Richtlinie.

So entfernen Sie eine Zone:

1. Melden Sie sich bei der Konsole (http://dellthreatdefense.com) als Administrator an. Nur Administratoren können Zonen entfernen.
2. Klicken Sie auf **Zonen**.
3. Markieren Sie die Kontrollkästchen der zu entfernenden Zonen.
4. Klicken Sie auf **Entfernen**.
5. Klicken Sie bei der Meldung, die zur Bestätigung des Entfernens aus der ausgewählten Zone auffordert, auf **Ja**.

Zoneneigenschaften

Die Zoneneigenschaften können beliebig bearbeitet werden.

Wissenswertes über die Zonenpriorität

Zonen kann eine bestimmte Priorität zugewiesen werden (Niedrig, Normal oder Hoch). Diese gibt Aufschluss darüber, wie wichtig oder kritisch die Geräte in der betreffenden Zone sind. In verschiedenen Bereichen des Dashboards werden Geräte nach Priorität angezeigt. So ist schneller ersichtlich, welche Geräte einer sofortigen Intervention bedürfen.

Die Priorität kann bei der Erstellung der Zone festgelegt und später durch Ändern des Prioritätswerts geändert werden.

So bearbeiten Sie Zoneneigenschaften:

1. Melden Sie sich bei der Konsole (http://dellthreatdefense.com) als Administrator oder Zonenmanager an.
2. Klicken Sie auf **Zonen**.
3. Klicken Sie in der *Zonenliste* auf eine Zone.
4. Geben Sie zur Änderung des Zonennamens einen neuen Namen in das Feld **Name** ein.
5. Wählen Sie eine andere Richtlinie aus dem Dropdown-Menü **Richtlinie** aus, um die Richtlinie zu ändern.
6. Wählen Sie einen Wert (**Niedrig**, **Normal** oder **Hoch**) aus.
7. Klicken Sie auf **Speichern**.

Zonenregel

Geräte können einer Zone automatisch basierend auf bestimmten Kriterien zugewiesen werden. Dieser Automatismus ist besonders hilfreich, wenn sehr viele Geräte zu Zonen hinzugefügt werden sollen. Sobald neue Geräte hinzugefügt werden, die einer Zonenregel entsprechen, werden sie automatisch der betreffenden Zone zugewiesen. Wenn **Jetzt auf alle vorhandenen Geräte anwenden** ausgewählt ist, werden alle bereits vorhandenen Geräte, die mit der Regel übereinstimmen, zur entsprechenden Zone hinzugefügt.

Hinweis: Durch Zonenregeln können Geräte einer Zone hinzugefügt werden. Es können jedoch keine Geräte entfernt werden. Durch Ändern der IP-Adresse oder des Hostnamens des Geräts wird das Gerät nicht aus der Zone entfernt. Geräte müssen manuell aus der Zone entfernt werden.

Es gibt eine Option, die bewirkt, dass die Zonenrichtlinie auf Geräte angewendet wird, die aufgrund ihrer Übereinstimmung mit der Zonenregel zur Zone hinzugefügt wurden. Die vorhandene Richtlinie des Geräts wird in dem Fall durch die jeweilige Zonenrichtlinie ersetzt. Die Option zum automatischen Anwenden einer Richtlinie basierend auf der Zonenregel sollte mit Vorsicht verwendet werden. Bei ungenauer Handhabung könnte ein Gerät einer falschen Richtlinie zugewiesen werden, weil es mit einer bestimmten Zonenregel übereinstimmt.

Die Seite „Gerätedetails“ in der Konsole gibt Aufschluss darüber, welche Richtlinie mit einem Gerät verbunden ist.

So fügen Sie eine Zonenregel hinzu:

1. Melden Sie sich bei der Konsole (http://dellthreatdefense.com) als Administrator oder Zonenmanager an.
2. Klicken Sie auf **Zonen**, und wählen Sie eine Zone aus der *Zonenliste* aus.
3. Klicken Sie unter Zonenregel auf **Regel erstellen**.
4. Geben Sie die Kriterien für die ausgewählte Zone an. Klicken Sie auf das Pluszeichen, um weitere Bedingungen hinzuzufügen. Klicken Sie auf das Minuszeichen, um eine Bedingung zu entfernen.
5. Klicken Sie auf **Speichern**.

Kriterien für die Zonenregel

- **Wenn ein neues Gerät zur Organisation hinzugefügt wird:** Jedes neue Gerät, das zur Organisation hinzugefügt wird und der Zonenregel entspricht, wird in die Zone aufgenommen.
- **Wenn sich ein beliebiges Attribut eines Geräts geändert hat**: Wenn sich die Attribute eines bereits vorhandenen Geräts ändern, sodass das Gerät der Zonenregel entspricht, wird es ebenfalls in die Zone aufgenommen.
- **IPv4-Adresse im Bereich**: Geben Sie einen IPv4-Adressbereich ein.
- **Gerätename:**
    - Beginnt mit: Der Gerätename muss mit dieser Zeichenkette beginnen.
    - Enthält: Der Gerätename muss diese Zeichenkette enthalten, wobei die Stelle innerhalb des Namens beliebig ist.
    - Endet mit: Der Gerätename muss mit dieser Zeichenkette enden.
- **Betriebssystem:**
    - Ist: Das Betriebssystem muss dem ausgewählten System entsprechen.
    - Ist nicht: Das Betriebssystem darf nicht dem ausgewählten System entsprechen. Beispiel: Wenn die einzige Zonenregel besagt, dass das Betriebssystem nicht Windows 8 sein darf, werden alle anderen Betriebssysteme, auch solche, die keine Windows-Systeme sind, zu dieser Zone hinzugefügt.
- **Domänenname:**
    - Beginnt mit: Der Domänenname muss mit dieser Zeichenkette beginnen.
    - Enthält: Der Domänenname muss diese Zeichenkette enthalten, wobei die Stelle innerhalb des Namens beliebig ist.
    - Endet mit: Der Domänenname muss mit dieser Zeichenkette enden.
- **Vollqualifizierter Name:**
    - Beginnt mit: Der vollqualifizierte Name muss mit dieser Zeichenkette beginnen.
    - Enthält: Der vollqualifizierte Name muss diese Zeichenkette enthalten, wobei die Stelle innerhalb des Namens beliebig ist.
    - Endet mit: Der vollqualifizierte Name muss mit dieser Zeichenkette enden.
- **Mitglied von (LDAP)**:
    - Ist: Das Mitglied von (Gruppe) muss diesem Wert entsprechen.
    - Enthält: Das Mitglied von (Gruppe) muss diesen Wert enthalten.
- **Folgende Bedingungen erfüllt**:
    - Alle: Es müssen alle Bedingungen der Zonenregel erfüllt werden, damit das Gerät hinzugefügt wird.
    - Beliebige: Es muss mindestens eine Bedingung der Zonenregel erfüllt werden, damit das Gerät hinzugefügt wird.

- **Zonenrichtlinie anwenden**:
    - Nicht anwenden: Beim Hinzufügen von Geräten zur Zone, die Zonenrichtlinie nicht anwenden.
    - Anwenden: Beim Hinzufügen von Geräten zur Zone, die Zonenrichtlinie anwenden.

      Warnung: Das automatische Anwenden einer Zonenrichtlinie kann sich negativ auf bestimmte Geräte im Netzwerk auswirken. Wenden Sie die Zonenrichtlinie *nur* automatisch an, wenn sicher ist, dass die Zonenregel *nur* Geräte finden wird, auf die diese bestimmte Zonenrichtlinie angewendet werden *muss*.
- **Jetzt auf alle vorhandenen Geräte anwenden**: Wendet die Zonenregel auf alle Geräte der Organisation an. Durch diesen Vorgang wird die Zonenrichtlinie nicht angewendet.

Wissenswertes über vollqualifizierte Namen

Bestimmte Dinge müssen beachtet werden, wenn vollqualifizierte Namen in Zonenregeln verwendet werden sollen.

- Es sind keine Platzhalter erlaubt, allerdings führt die Bedingung „Enthält“ zu vergleichbaren Ergebnissen.
- Fehler in Verbindung mit vollqualifizierten Namen und Ausnahmen bezüglich des Agenten werden in den Protokolldateien erfasst.
- Falls der Agent Informationen zu vollqualifizierten Namen auf dem Gerät findet, sendet er diese automatisch an die Konsole.
- Informationen zu vollqualifizierten Namen müssen ordnungsgemäß formatiert sein.
    - Beispiel: CN=JDoe,OU=Sales,DC=dell,DC=COM
    - Beispiel: OU=Demo,OU=SEngineering,OU=Sales

Liste der Zonengeräte

Die *Liste der Zonengeräte* zeigt alle Geräte an, die dieser Zone zugewiesen sind. Geräte können mehreren Zonen angehören. Verwenden Sie **Exportieren**, um eine CSV-Datei mit Informationen zu allen Geräten auf der *Liste der Zonengeräte* herunterzuladen.

Hinweis: Wenn der Zonenlink in der Spalte „Zonen“ angeklickt wird, obwohl keine Berechtigung zum Anzeigen der Zone vorhanden ist, wird die Meldung „Ressource nicht gefunden“ angezeigt.

Bewährte Verfahren zum Verwalten von Zonen

Zonen kann man sich am besten als Markierungen vorstellen. Geräte können mehreren Zonen angehören (bzw. mehrere Markierungen aufweisen). Es gibt keine Begrenzung in Bezug auf die Anzahl der Zonen, die erstellt werden können. Es hat sich jedoch bewährt, innerhalb einer Organisation zwischen drei unterschiedlichen Zonenzugehörigkeiten zu unterscheiden, um die Granularität zwischen Test, Richtlinie und Benutzerrolle besser abzubilden.

Diese Zonen sind:

- Aktualisierungsverwaltung
- Richtlinienverwaltung
- Rollenbasierte Zugriffsverwaltung

Zonenorganisation für die Aktualisierungsverwaltung

Eine geläufige Nutzung von Zonen ist die Vereinfachung von Agentenaktualisierungen. Threat Defense unterstützt die neueste und die vorherige Agentenversion. Dies ermöglicht Unternehmen, Fenster für das Einfrieren von Änderungen zu unterstützen und die neue Agentenversion umfassend zu testen.

Es gibt drei Zonentypen, deren Verwendung für die Durchführung und Festlegung der Test- und Produktivphasen des Agenten vorgeschlagen werden:

- **Zone aktualisieren - Testgruppe**: In diesen Zonen sollten Testgeräte enthalten sein, die die Geräte (sowie die darauf verwendete Software) innerhalb der Organisation repräsentativ darstellen. Auf diese Weise kann der neueste Agent getestet werden und es wird sichergestellt, dass die Bereitstellung des Agenten auf den Produktivgeräten die Geschäftsprozesse nicht beeinträchtigt.
- **Zone aktualisieren - Pilotgruppe**: Diese Zone kann als sekundäre Testzone oder als sekundäre Produktivzone verwendet werden. Bei Verwendung als sekundäre Testzone können neue Agenten auf einer größeren Gerätegruppe getestet werden, bevor der Rollout für die Produktion erfolgt. Bei Verwendung als sekundäre Produktivzone sind zwei unterschiedliche Agentenversionen möglich, allerdings müssen Sie dann auch zwei unterschiedliche Produktivzonen verwalten.
- **Zone aktualisieren - Produktion**: Die meisten Geräte sollten sich in Zonen befinden, die der Produktion zugewiesen sind.

Hinweis: Informationen zum Aktualisieren des Agenten auf die Produktionszone finden Sie unter Agentenaktualisierung.

Hinzufügen einer Test- oder Pilotzone

1. Melden Sie sich bei der Konsole (http://dellthreatdefense.com) mit einem Administrator- oder Zonenmanager-Konto an.
2. Wählen Sie **Einstellungen** > **Agentenaktualisierung** aus.
3. Vorgehensweise für Test- oder Pilotzone:
    a. Klicken Sie auf **Testzonen auswählen** oder **Pilotzonen auswählen**.
    b. Klicken Sie auf eine Zone.

    Wenn die Produktionszone auf **Automatisch aktualisieren** eingestellt ist, sind die Test- und Pilotzonen nicht verfügbar. Ändern Sie die Option zum automatischen Aktualisieren in der Produktivzone in eine andere Einstellung, um die Test- und Pilotzonen zu aktivieren.
4. Klicken Sie auf **Bitte Version auswählen**.
5. Wählen Sie eine Agentenversion aus, die auf die Test- oder Produktivzone angewendet werden soll.
6. Klicken Sie auf **Anwenden**.

Zonenorganisation für die Richtlinienverwaltung

Die Erstellung einer weiteren Zonengruppe vereinfacht die Anwendung unterschiedlicher Richtlinien auf unterschiedliche Arten von Endpunkten. Berücksichtigen Sie folgende Beispiele:

- Richtlinienzone – Workstations
- Richtlinienzone – Workstations – Ausschlüsse
- Richtlinienzone – Server
- Richtlinienzone – Server – Ausschlüsse

- Richtlinienzone – Führungskräfte – Starker Schutz

Dell empfiehlt, standardmäßig auf alle Geräte dieser Richtlinienzone eine Richtlinie für jede dieser Zonen anzuwenden. Achten Sie darauf, dass Sie ein Gerät nicht mehreren Richtlinienzonen zuordnen, da dies zu Konflikten hinsichtlich der letztlich anzuwendenden Richtlinie führen kann. Denken Sie daran, dass das Modul für Zonenregeln Sie bei der automatischen Anordnung der Hosts nach IP-Adresse, Hostname, Betriebssystem und Domäne unterstützen kann.

Zonenorganisation für die rollenbasierte Zugriffsverwaltung

Der rollenbasierte Zugriff dient der Begrenzung des Zugriffs eines Konsolenbenutzers auf die Geräte, für deren Verwaltung er zuständig ist. Hierfür kann eine Unterscheidung nach IP-Bereich, Hostname, Betriebssystem oder Domäne vorgenommen werden. Sie können auch Gruppierungen nach geografischem Standort und/oder Typ vornehmen.

Beispiel:

- RBAC-Zone – Desktops – Europa
- RBAC-Zone – Server – Asien
- RBAC-Zone – Roter Teppich (Führungskräfte)

Mithilfe der oben beschriebenen Zonenbeispiele könnte ein Zonenmanager *RBAC-Zone – Desktops – Europa* zugewiesen werden und hätte nur Zugriff auf Geräte innerhalb dieser Zone. Wenn der Zonenmanager versucht, die anderen Zonen aufzurufen, wird eine Meldung angezeigt, die ihn darauf hinweist, dass er nicht über die erforderliche Berechtigung verfügt. Ein Gerät kann mehreren Zonen angehören, und der Zonenmanager kann dieses Gerät auch anzeigen. Wenn er allerdings versucht, die anderen Zonen anzuzeigen, denen das Gerät auch angehört, würde er diese Meldung ebenfalls erhalten und der Zugriff wird verweigert.

In anderen Teilen der Konsole, wie z. B. im Dashboard, wäre der Zugriff des Zonenmanagers für *RBAC-Zone – Desktops – Europa* auch auf Bedrohungen und andere Informationen in Bezug auf die Zone oder dieser Zone zugewiesene Geräte beschränkt.

Die gleichen Einschränkungen gelten auch für Benutzer, die einer bestimmten Zone zugewiesen sind.

Benutzerverwaltung

Administratoren verfügen über globale Berechtigungen und können Benutzer hinzufügen oder entfernen, Benutzer bestimmten Zonen zuweisen (als Benutzer oder Zonenmanager), Geräte hinzufügen und entfernen sowie Richtlinien und Zonen erstellen. Administratoren können außerdem Benutzer, Geräte, Richtlinien und Zonen dauerhaft aus der Konsole löschen.

Benutzer und Zonenmanager verfügen nur für die ihnen zugewiesene Zone über Zugriff und Berechtigungen. Dies gilt für die der Zone zugewiesenen Geräte, Bedrohungen, die auf den Geräten erkannt werden, und für Informationen im Dashboard.

Eine umfassende Liste der einzelnen Benutzerberechtigungen finden Sie in Anhang C: Benutzerberechtigungen.

So fügen Sie Benutzer hinzu:

1. Melden Sie sich als Administrator bei der Konsole (http://dellthreatdefense.com) an. Nur Administratoren können Benutzer anlegen.
2. Wählen Sie **Einstellungen > Benutzerverwaltung** aus.
3. Geben Sie die E-Mail-Adresse des Benutzers ein.
4. Wählen Sie im Dropdown-Menü „Rolle“ eine Rolle aus.
5. Wählen Sie beim Hinzufügen eines Zonenmanagers oder Benutzers eine Zone aus, um ihn zuzuweisen.
6. Klicken Sie auf **Hinzufügen**. Dem Benutzer wird eine E-Mail mit einem Link zugestellt, über den er ein Passwort erstellen kann.

So ändern Sie Benutzerrollen:

1. Melden Sie sich als Administrator bei der Konsole (http://dellthreatdefense.com) an. Nur Administratoren können Benutzer anlegen.
2. Wählen Sie **Einstellungen > Benutzerverwaltung** aus.
3. Klicken Sie auf einen Benutzer. Daraufhin wird die Seite „Benutzerdetails“ angezeigt.
4. Wählen Sie eine Rolle aus, und klicken Sie auf **Speichern**.

So entfernen Sie Benutzer:

1. Melden Sie sich als Administrator bei der Konsole (http://dellthreatdefense.com) an. Nur Administratoren können Benutzer anlegen.
2. Wählen Sie **Einstellungen > Benutzerverwaltung** aus.
3. Markieren Sie die Kontrollkästchen der zu entfernenden Benutzer.
4. Klicken Sie auf **Entfernen**.
5. Klicken Sie bei der Meldung, die zur Bestätigung des Entfernens auffordert, auf **Ja**.

Netzwerkbezogen

Konfigurieren Sie das Netzwerk so, dass der Threat Defense Agent über das Internet mit der Konsole kommunizieren kann. In diesem Abschnitt werden Firewall-Einstellungen und Proxy-Konfigurationen beschrieben.

Firewall

Zur Verwaltung von Geräten ist keine lokale Software erforderlich. Threat Defense Agenten werden von der Konsole verwaltet und berichten an die Konsole (cloudbasierte Benutzeroberfläche). Port 443 (HTTPS) wird für die Kommunikation verwendet und muss auf der Firewall geöffnet sein, damit die Agenten mit der Konsole kommunizieren können. Die Konsole wird von Amazon Web Services (AWS) gehostet und verfügt über keine festen IP-Adressen. Stellen Sie sicher, dass die Agenten mit den folgenden Sites kommunizieren können:

- login.cylance.com
- data.cylance.com
- my.cylance.com
- update.cylance.com

- api2.cylance.com
- download.cylance.com

Lassen Sie alternativ den HTTPS-Datenverkehr an *.cylance.com zu.

Proxy

Die Proxy-Unterstützung für Threat Defense wird über einen Registrierungseintrag konfiguriert. Wenn ein Proxy-Server konfiguriert ist, verwendet der Agent die IP-Adresse und den Port im Registrierungseintrag für die gesamte ausgehende Kommunikation zu den Konsolenservern.

1. Rufen Sie die Registrierung auf.

   Hinweis: Möglicherweise sind erhöhte Berechtigungen oder die Übernahme des Besitzes an der Registrierung erforderlich. Dies hängt davon ab, wie der Agent installiert wurde (geschützter Modus aktiviert oder nicht).

2. Wechseln Sie im Registrierungs-Editor zu **`HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop`**.
3. Erstellen Sie einen neuen Zeichenkettenwert (REG_SZ):
   - Value Name = ProxyServer
   - Value Data = Proxy-Einstellungen (z. B. http://123.45.67.89:8080)

Der Agent versucht unter Verwendung der Anmeldeinformationen des derzeit angemeldeten Benutzers, in authentifizierten Umgebungen mit dem Internet zu kommunizieren. Falls ein authentifizierter Proxy-Server konfiguriert, aber kein Benutzer am Gerät angemeldet ist, kann sich der Agent nicht am Proxy-Server authentifizieren und nicht mit der Konsole kommunizieren. Wählen Sie in dem Fall eine der beiden folgenden Methoden:

- Konfigurieren Sie den Proxy-Server, und fügen Sie eine Regel hinzu, die den gesamten Datenverkehr an *.cylance.com zulässt.
- Verwenden Sie eine andere Proxy-Richtlinie, die den unberechtigten Proxy-Zugriff auf Cylance-Hosts (*.cylance.com) zulässt.

Auf diese Weise muss sich der Agent nicht authentifizieren, falls kein Benutzer am Gerät angemeldet ist, und kann normalerweise problemlos eine Verbindung zur Cloud herstellen und mit der Konsole kommunizieren.

Geräte

Sobald ein Agent auf einem Endpunkt installiert ist, steht er als Gerät in der Konsole zur Verfügung. Beginnen Sie mit der Verwaltung von Geräten durch die Zuweisung von Richtlinien (zur Bewältigung identifizierter *Bedrohungen*), Gruppengeräten (mithilfe von *Zonen*), und führen Sie manuell Maßnahmen auf jedem Gerät durch (*Quarantäne* und *Freigeben*).

Gerätemanagement

Geräte sind Computer, auf denen ein Threat Defense Agent installiert ist. Sie können die Geräte über die Konsole verwalten.

1. Melden Sie sich als Administrator bei der Konsole (http://dellthreatdefense.com) an. Nur Administratoren können Geräte verwalten.
2. Klicken Sie auf **Geräte**.

3. Markieren Sie das Kontrollkästchen eines Geräts, um die folgenden Maßnahmen zu ermöglichen:
    - **Exportieren:** Erstellt eine CSV-Datei und lädt diese herunter. Die Datei enthält Geräteinformationen (Name, Zustand und Richtlinie) für alle Geräte der Organisation.
    - **Entfernen**: Entfernt die ausgewählten Geräte aus der *Geräteliste*. Durch diesen Vorgang wird der Agent nicht vom Gerät deinstalliert.
    - **Richtlinie zuweisen**: Ermöglicht die Zuweisung ausgewählter Geräte zu einer Richtlinie.
    - **Hinzufügen zu Zonen**: Ermöglicht das Hinzufügen ausgewählter Geräte zu einer oder mehreren Zonen.
4. Klicken Sie auf ein Gerät, um die Seite „Gerätedetails“ anzuzeigen.
    - **Geräteinformationen**: Zeigt Informationen an, wie Hostname, Agentenversion und Betriebssystemversion.
    - **Geräteeigenschaften**: Ermöglicht das Ändern von Gerätename, Richtlinie, Zonen und Protokollierungsebene.
    - **Bedrohungen & Aktivitäten**: Zeigt Bedrohungsinformationen und sonstige Aktivitäten in Verbindung mit dem Gerät an.
5. Klicken Sie auf **Neues Gerät hinzufügen**, um ein Dialogfeld mit einem Installations-Token und Links zum Herunterladen des Agenten-Installationsprogramms aufzurufen.
6. Klicken Sie in der Spalte „Zonen“ auf einen Zonennamen, um die Seite „Zonendetails“ aufzurufen.

Bedrohungen & Aktivitäten

Zeigt Bedrohungsinformationen und sonstige Aktivitäten in Verbindung mit dem ausgewählten Gerät an.

Bedrohungen

Zeigt alle Bedrohungen an, die auf dem Gerät gefunden wurden. Standardmäßig sind die Bedrohungen gruppiert nach Status (*Unsicher, Abnormal*, *in Quarantäne* und *Freigegeben*).

- **Exportieren:** Erstellt eine CSV-Datei mit Informationen zu allen auf dem ausgewählten Gerät gefundenen Bedrohungen und lädt sie herunter. Dazu gehören Informationen wie Name, Dateipfad, Cylance Score und Status.
- **Quarantäne:** Stellt die ausgewählten Bedrohungen unter *Quarantäne*. Hierbei handelt es sich um eine *lokale Quarantäne*, was bedeutet, dass diese Bedrohung nur auf diesem Gerät *unter Quarantäne gestellt* ist. Um eine Bedrohung für alle Geräte in der Organisation unter *Quarantäne* zu stellen, stellen Sie sicher, dass das Kontrollkästchen **Diese Bedrohung auch bei jeder Entdeckung auf jedem beliebigen Gerät unter Quarantäne stellen** ausgewählt ist (*Globale Quarantäne*), wenn eine Datei *unter Quarantäne gestellt* wird.
- **Freigeben:** Ändert den Status der ausgewählten Bedrohungen in *Freigegeben*. Eine Datei mit dem Status *Freigegeben* darf ausgeführt werden. Hierbei handelt es sich um eine *lokale Freigabe*, was bedeutet, dass diese Datei nur auf diesem Gerät ausgeführt werden darf. Damit diese Datei auf allen Geräten in der Organisation ausgeführt werden darf, markieren Sie das Kontrollkästchen **Auch auf allen Geräten als sicher markieren** (*Sichere Liste*), wenn eine Datei den Status *Freigegeben* erhält.

Exploit-Versuche

Zeigt alle Exploit-Versuche auf dem Gerät an. Dazu gehören auch Informationen wie Prozessname, ID, Typ und durchgeführte Maßnahme.

Agentenprotokolle

Zeigt die Protokolldateien an, die der Agent auf dem Gerät hochgeladen hat. Der Name der Protokolldatei entspricht dem Protokolldatum.

So können Sie Agentenprotokolldateien anzeigen:

1. Laden Sie die aktuelle Protokolldatei für ein einzelnes Gerät hoch.
   a. Klicken Sie auf Geräte > Agentenprotokolle.
   b. Klicken Sie auf **Aktuelle Protokolldatei hochladen**. Je nach Größe der Protokolldatei kann dies einige Minuten dauern.

ODER

1. Richtlinieneinstellungen:
   a. Klicken Sie auf Einstellungen > Geräterichtlinie > [Richtlinie auswählen] > Agentenprotokolle.
   b. Klicken Sie auf „Automatisches Hochladen von Protokolldateien aktivieren“.
   c. Klicken Sie auf **Speichern**.

Um ausführliche Protokolle anzuzeigen, ändern Sie vor dem Hochladen der Protokolldateien die Protokollierungsebene des Agenten.

1. Gehen Sie in der Konsole folgendermaßen vor: **Geräte > [klicken Sie auf ein Gerät]**, wählen Sie **Verbose** aus dem Dropdown-Menü Protokollierungsebene des Agenten aus, und klicken Sie auf **Speichern**. Nach dem Hochladen der ausführlichen Protokolldateien empfiehlt Dell, die Protokollierungsebene wieder auf *Informationen* zu ändern.
2. Schließen Sie auf dem Gerät die Threat Defense-Benutzeroberfläche (klicken Sie dazu mit der rechten Maustaste auf das Threat Defense-Symbol in der Taskleiste, und klicken Sie anschließend auf **Beenden**).

ODER

1. Öffnen Sie die Befehlszeile als Administrator. Geben Sie die folgende Befehlszeile ein, und drücken Sie anschließend die **Eingabetaste**.

   ```
   cd C:\Program Files\Cylance\Desktop
   ```

2. Geben Sie die folgende Befehlszeile ein, und drücken Sie anschließend die **Eingabetaste**.

   ```
   Dell.ThreatDefense.exe –a
   ```

3. Das Threat Defense-Symbol wird in der Taskleiste angezeigt. Klicken Sie mit der rechten Maustaste, wählen Sie **Protokollierung** aus und klicken Sie anschließend auf **Alle** (wie Verbose in der Konsole).

ODER (bei Verwendung von Mac OS X)

1. Beenden Sie die derzeit ausgeführte Benutzeroberfläche.
2. Geben Sie den folgenden Befehl am Terminal ein.

   ```
   sudo /Applications/Cylance/CylanceUI.app/Contents/MacOS/CylanceUI -a
   ```

3. Klicken Sie mit der rechten Maustaste in die neue Benutzeroberfläche, sobald diese angezeigt wird. Wählen Sie **Protokollierung > Alle**.

Skriptsteuerung

Zeigt alle Aktivitäten an, die für die Skriptsteuerung relevant sind, z. B. verweigerte Skripte.

Doppelte Geräte

Wird der Threat Defense Agent zum ersten Mal auf einem Gerät installiert, wird eine eindeutige Kennung angelegt, die von der Konsole zum Identifizieren des Geräts und Verweisen auf das Gerät genutzt wird. Bestimmte Ereignisse können jedoch dazu führen, dass eine zweite Kennung für dasselbe Gerät generiert wird, z. B. die Verwendung des Images einer virtuellen Maschine zur Erstellung mehrerer Systeme. Wählen Sie das Gerät aus, und klicken Sie auf **Entfernen**, wenn ein doppelter Eintrag auf der Seite Geräte in der Konsole angezeigt wird.

Verwenden Sie die Spaltensortierung, um solche Geräte einfacher zu identifizieren. Mit dieser Funktion können Sie die Geräte sortieren und vergleichen, in der Regel nach Gerätename. Alternativ dazu kann die *Geräteliste* als .CSV-Datei exportiert und in Microsoft Excel oder einem ähnlichen Programm mit leistungsfähigen Sortierungsfunktionen angezeigt werden.

Beispiel unter Verwendung von Microsoft Excel

1. Öffnen Sie die Geräteliste im CSV-Format in Microsoft Excel.
2. Wählen Sie die Spalte mit dem Gerätenamen aus.
3. Wählen Sie auf der Registerkarte „Start“ die Option Bedingte Formatierung > Regeln zum Hervorheben von Zellen > Doppelte Werte aus.
4. Stellen Sie sicher, dass **Doppelt** ausgewählt ist, und wählen Sie dann eine Markierungsoption aus.
5. Klicken Sie auf **OK**. Die doppelten Elemente werden hervorgehoben.

Hinweis: Mit dem Befehl „Entfernen“ wird das Gerät lediglich von der Seite „Gerät“ entfernt. Es wird kein Deinstallationsbefehl an den Threat Defense Agent gesendet. Der Agent muss am Endpunkt deinstalliert werden.

Agentenaktualisierung

Wartung und Verwaltung der Threat Defense Agents sind ein einfaches Unterfangen. Die Agenten laden automatisch Aktualisierungen von der Konsole herunter, und die Konsole wird von Cylance verwaltet.

Der Agent meldet sich alle 1 bis 2 Minuten an der Konsole an. Die Konsole meldet den aktuellen Status des Agenten (*Online* oder *Offline*, *Unsicher* oder *Geschützt*), Versionsinformationen, Betriebssystem und Bedrohungsstatus.

Threat Defense gibt monatlich Aktualisierungen für den Agenten heraus. Diese Aktualisierungen können Konfigurationsüberarbeitungen, neue Module und Programmänderungen beinhalten. Wenn eine Agentenaktualisierung verfügbar ist (siehe Meldung der Konsole unter Einstellungen > Agentenaktualisierungen), lädt der Agent die Aktualisierung automatisch herunter und wendet sie an. Zur Steuerung des Netzwerkdatenverkehrs während einer Agentenaktualisierung sind alle Organisationen so eingerichtet, dass bis zu 1.000 Geräteaktualisierungen gleichzeitig stattfinden können. Benutzer können auch die automatische Aktualisierung deaktivieren, falls gewünscht.

Hinweis: Die maximale Anzahl der gleichzeitig aktualisierbaren Geräte kann von Dell Support modifiziert werden.

Zonenbasierte Aktualisierung

Die zonenbasierte Aktualisierung ermöglicht einer Organisation, einen neuen Agenten zunächst auf einem Teil der Geräte zu bewerten, bevor er für die gesamte Umgebung (Produktion) bereitgestellt wird. Eine oder mehrere aktuelle Zonen können vorübergehend einer oder zwei Testzonen hinzugefügt werden (Test und Pilot), die einen anderen Agenten verwenden können, als die Produktion.

So konfigurieren Sie zonenbasierte Aktualisierungen:

1. Melden Sie sich mit einem Administratorkonto bei der Konsole (http://dellthreatdefense.com) an.
2. Wählen Sie **Einstellungen** > **Agentenaktualisierung** aus. Die drei letzten Agentenversionen werden angezeigt.

   Wenn die Produktionszone auf **Automatisch aktualisieren** eingestellt ist, sind die Test- und Pilotzonen nicht verfügbar. Ändern Sie die Option zum automatischen Aktualisieren in der Produktivzone in eine andere Einstellung, um die Test- und Pilotzonen zu aktivieren.
3. Wählen Sie aus der Dropdown-Liste „Produktion“ eine bestimmte Agentenversion aus.
4. Wählen Sie für die Produktion auch „Automatisch aktualisieren“ oder „Nicht aktualisieren“ aus.
   a. Über die **Automatische Aktualisierung** können alle Produktionsgeräte automatisch auf die neueste Version in der *Liste der unterstützten Agentsoftware-Versionen* aktualisiert werden.
   b. **Nicht aktualisieren** verbietet die Agenten-Aktualisierung aller Produktionsgeräte.
5. Wählen Sie für die Testzone eine oder zwei Zonen aus der Dropdown-Liste „Zonen“ aus, und geben Sie anschließend eine Agentenversion der Dropdown-Liste „Version“ an.
6. Sie können Schritt 5 für die Pilotzone wiederholen.

Hinweis: Wenn ein Gerät einer Zone hinzugefügt wurde, die Teil der Test- oder Pilotzone ist, startet dieses Gerät in der Agentenversion der jeweiligen Test- oder Pilotzone. Gehört ein Gerät mehreren Zonen an, von denen eine Teil der Test- oder Pilotzone ist, dann hat die Agentenversion dieser Test- oder Pilotzone Vorrang.

So lösen Sie eine Agentenaktualisierung aus:

So können Sie eine Agentenaktualisierung vor dem nächsten Stundenintervall auslösen:

1. Klicken Sie mit der rechten Maustaste auf das Threat Defense-Symbol in der Taskleiste, und wählen Sie **Auf Aktualisierungen überprüfen** aus.
2. Starten Sie den Threat Defense-Dienst neu. Durch diese Maßnahme wird der Dienst gezwungen, sich sofort an der Konsole anzumelden.

ODER

- Aktualisierungen können auch über die Befehlszeile initiiert werden. Führen Sie den folgenden Befehl über das Cylance-Verzeichnis aus:

  ```
  Dell.ThreatDefense.exe – update
  ```

Dashboard

Nach der Anmeldung an der Threat Defense Console wird die Seite „Dashboard“ angezeigt. Das Dashboard bietet eine Übersicht über die Bedrohungen in der Umgebung sowie Zugriff auf verschiedene Konsoleninformationen über eine einzige Seite.

Bedrohungsstatistik

Bedrohungsstatistiken geben Aufschluss über die Anzahl der gefundenen Bedrohungen in den *letzten 24 Stunden* und die *Gesamt*zahl für die Organisation. Klicken Sie auf eine *Bedrohungsstatistik*, um zur Seite Schutz zu gelangen, und die Liste der mit dieser Statistik zusammenhängenden Bedrohungen anzuzeigen.

- **Ausgeführte Bedrohungen**: Dateien, die als Bedrohung identifiziert wurden und derzeit auf Geräten der Organisation ausgeführt werden.
- **Automatisch ausgeführte Bedrohungen**: Bedrohungen, die für eine automatische Ausführung konfiguriert sind.
- **Unter Quarantäne gestellte Bedrohungen**: Bedrohungen, die innerhalb der letzten 24 Stunden *unter Quarantäne gestellt* wurden, und die Gesamtzahl.
- **Spezifisch für Cylance**: Bedrohungen, die von Cylance identifiziert wurden, jedoch von keiner anderen Virenschutzquelle.

Prozentuale Verteilung

Zeigt Prozentsätze für Threat Protection und Device Protection an.

- **Threat Protection**: Der Anteil der Bedrohungen, für die eine Maßnahme durchgeführt wurde (Quarantäne, globale Quarantäne, Freigabe und sichere Liste).
- **Device Protection**: Der Anteil der Geräte, die mit einer Richtlinie mit aktivierter automatischer Quarantäne verknüpft sind.

Bedrohungen nach Priorität

Zeigt die Gesamtanzahl der Bedrohungen an, die eine Maßnahme erfordern (*Quarantäne*, *Globale Quarantäne*, *Freigabe* und *Sichere Listen*). Die Bedrohungen sind nach Priorität zusammengefasst (Hoch, Mittel und Niedrig). In dieser Übersicht wird die Gesamtzahl der Bedrohungen, unterteilt nach Priorität, angezeigt, für die eine Maßnahme erforderlich ist. Ferner werden der prozentuale Anteil von der Gesamtzahl und die Anzahl der betroffenen Geräte angezeigt.

In der linken unteren Ecke der Seite „Dashboard“ werden die Bedrohungen nach Priorität aufgeführt. Angegeben ist die Gesamtzahl der Bedrohungen in der Organisation, unterteilt nach Priorität.

Einer Bedrohung wird basierend auf der Anzahl der nachfolgenden Attribute, die auf sie zutreffen, eine von drei Klassifizierungen (Niedrig, Mittel oder Hoch) zugewiesen:

- Die Datei hat einen Cylance Score von über 80.
- Die Datei wird gerade ausgeführt.
- Die Datei wurde zuvor ausgeführt.
- Die Datei ist für die automatische Ausführung konfiguriert.
- Die Priorität der Zone, in der die Bedrohung gefunden wurde.

Diese Klassifizierung hilft Administratoren bei der Bestimmung, welche Bedrohungen und Geräte zuerst behandelt werden müssen. Klicken Sie auf die Bedrohung oder die Gerätenummer, um Details zur Bedrohung und zum Gerät anzuzeigen.

Bedrohungsereignisse

Zeigt ein Liniendiagramm mit der Anzahl der Bedrohungen an, die in den letzten 30 Tagen gefunden wurden. Zeilen sind farblich gekennzeichnet für Dateien mit dem Status *Unsicher*, *Abnormal*, *in Quarantäne*, *Freigegeben*, und *Gelöscht*.

- Bewegen Sie den Mauszeiger über die Grafik, um Details anzuzeigen.
- Klicken Sie in der Legende auf eine der Farben, um die betreffende Linie ein- oder auszublenden.

Bedrohungsklassifizierungen

Zeigt eine Karte der in der Organisation gefundenen Bedrohungstypen an, z. B. Viren oder Malware. Klicken Sie auf ein Element der Karte, um die Seite „Schutz“ aufzurufen. Diese enthält eine Liste mit Bedrohungen von diesem Typ.

Top 5-Listen

Zeigt verschiedene Top 5-Listen an, darunter die Top 5-Bedrohungen, die auf den meisten Geräten gefunden wurden, die Top 5-Geräte mit den meisten Bedrohungen und die Top 5-Zonen mit den meisten Bedrohungen in der Organisation. Klicken Sie auf ein Element der Liste, um weitere Details aufzurufen.

Die Top 5-Listen auf dem Dashboard markieren als *Unsicher* eingestufte Bedrohungen in der Organisation, gegen die keine Maßnahmen ergriffen wurden, z. B. *in Quarantäne* oder *Freigegeben*. Diese Listen sind in der Regel leer. Bedrohungen der Kategorie *Abnormal* erfordern zwar auch Maßnahmen, der Schwerpunkt der Top 5-Listen liegt jedoch darauf, Sie auf kritische Bedrohungen aufmerksam zu machen.

Schutz – Bedrohungen

Threat Defense kann mehr als nur Dateien als *Unsicher* oder *Abnormal* zu klassifizieren. Threat Defense liefert zusätzlich Details zu den statischen und dynamischen Merkmalen von Dateien. Dadurch können Administratoren Bedrohungen nicht nur blockieren, sondern auch ihr Verhalten besser verstehen und so die Bedrohungen weiter eindämmen oder entsprechend auf sie reagieren.

Dateityp

Unsicher: Eine Datei mit einem Score zwischen 60 und 100. Eine Datei der Kategorie *Unsicher* ist eine Datei, in der Threat Defense Attribute gefunden hat, die sehr stark an die Attribute von Malware erinnern.

Abnormal: Eine Datei mit einem Score zwischen 1 und 59. Eine Datei der Kategorie *Abnormal* weist einige Malware-Attribute auf, allerdings weniger als eine Datei der Kategorie *Unsicher*. Es ist also weniger wahrscheinlich, dass es sich um Malware handelt.

Hinweis: Es kann vorkommen, dass eine Datei als *Unsicher* oder *Abnormal* klassifiziert wird, obwohl der angezeigte Score dem Wertebereich für die Klassifizierung nicht entspricht. Dies kann auf neuere Erkenntnisse oder eine zusätzliche Dateianalyse im Anschluss an die anfängliche Erkennung zurückzuführen sein. Um die neueste Analyse zu erhalten, aktivieren Sie in der Geräterichtlinie die Option „Automatisch hochladen“.

Cylance Score

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.

Anzeigen von Bedrohungsinformationen

Auf der Registerkarte „Schutz“ der Konsole werden ausführliche Bedrohungsinformationen angezeigt, die Geräte, auf denen die Bedrohungen gefunden wurden, sowie die Maßnahmen, die auf den betreffenden Geräten in Bezug auf die Bedrohungen durchgeführt wurden.

Hinweis: Die *Bedrohungsliste* auf der Registerkarte Schutz verfügt über konfigurierbare Spalten. Klicken Sie in einer beliebigen Spalte auf den Pfeil nach unten, um das Menü aufzurufen. Anschließend können Sie verschiedene Bedrohungsdetails ein- oder ausblenden. Das Menü enthält ein Untermenü mit Filterfunktion.

So zeigen Sie Bedrohungsdetails an:

1. Melden Sie sich bei der Konsole an (http://dellthreatdefense.com).
2. Klicken Sie auf die Registerkarte **Schutz**, um eine Liste der in dieser Organisation gefundenen Bedrohungen anzuzeigen.
3. Mit dem Filter in der linken Menüleiste können Sie nach Priorität (Hoch, Mittel, Niedrig) und nach Status (*In Quarantäne*, *Freigegeben*, *Unsicher* oder *Abnormal*) filtern.

   Hinweis: Zahlen, die im linken Bereich rot dargestellt sind, weisen auf unbehandelte Bedrohungen hin, die noch nicht *in Quarantäne* gestellt oder *freigegeben* wurden. Filtern Sie diese Elemente, um eine Liste der Dateien anzuzeigen, die untersucht werden müssen.
4. Wenn Sie weitere Spalten hinzufügen möchten, um zusätzliche Bedrohungsinformationen anzuzeigen, klicken Sie neben einem der Spaltennamen auf den Pfeil nach unten, und wählen Sie einen Spaltennamen aus.
5. 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 in die Zeile mit der Bedrohung (Details werden auf derselben Seite unten angezeigt). Beide Ansichten enthalten

dieselben Informationen, sind aber unterschiedlich aufgebaut. Die Details umfassen eine Übersicht über die Metadaten der Datei, eine Liste der Geräte, die diese Bedrohung aufweisen, und Nachweisberichte.

a. Dateimetadaten

- Klassifizierung [zugewiesen vom Cylance Advanced Threat and Alert Management (ATAM) Team]
- Cylance Score (Vertrauensstufe)
- Einstufung der Virenschutzbranche (Link zu VirusTotal.com zum Vergleich mit anderen Anbietern)
- Zuerst gefundene Daten, zuletzt gefundene Daten
- SHA256
- MD5
- Dateiinformationen (Autor, Beschreibung, Version usw.)
- Signaturdetails

b. Geräte

Die *Geräte-/Zonenliste* zu einer Bedrohung kann nach Zustand der Bedrohung gefiltert werden (*Unsicher*, *In Quarantäne*, Freigegeben, *Abnormal*). Klicken Sie auf die Links für den Zustandsfilter, um die Geräte anzuzeigen, auf denen die Bedrohung in dem jeweiligen Zustand vorhanden ist.

- *Unsicher:* Die Datei wird als *Unsicher* klassifiziert, aber es wurden keine Maßnahmen ergriffen.
- *In Quarantäne*: Die Datei befindet sich aufgrund einer Richtlinieneinstellung bereits *in Quarantäne*.
- *Freigegeben:* Die Datei wurde von Administrator *freigegeben* oder *auf die White List gesetzt*.
- *Abnormal*: Die Datei wurde als A*bnormal* klassifiziert, aber es wurden keine Maßnahmen ergriffen.

c. Nachweisberichte

- **Bedrohungsindikatoren**: Beobachtungen zu einer Datei, die vom Cylance Infinity-Modul analysiert wurde. Anhand dieser Indikatoren kann einfacher nachvollzogen werden, weshalb eine Datei wie klassifiziert wurde, und sie geben Aufschluss über die Attribute und das Verhalten einer Datei. Bedrohungsindikatoren sind in Kategorien unterteilt, um mehr Kontext zu liefern.
- **Detaillierte Bedrohungsdaten**: Die detaillierten Bedrohungsdaten bieten eine umfassende Darstellung der statischen und dynamischen Eigenschaften einer Datei, einschließlich zusätzlicher Dateimetadaten, Details zur Dateistruktur und dynamischer Verhaltensweisen, wie aufgegebene Dateien, erstellte oder modifizierte Registrierungsschlüssel und URLs, mit denen die Datei versucht hat zu kommunizieren.

So zeigen Sie Bedrohungsindikatoren an:

1. Melden Sie sich bei der Konsole an (http://dellthreatdefense.com).
2. Klicken Sie im oberen Menü auf **Schutz** zum Anzeigen einer Liste der Bedrohungen (oder klicken Sie auf **Geräte**, und wählen Sie anschließend ein Gerät aus).

3. Klicken Sie auf den Namen einer Bedrohung. Daraufhin wird die Seite „Bedrohungsdetails“ angezeigt.
4. Klicken Sie auf **Nachweisberichte**.

Kategorien für Bedrohungsindikatoren:

Jede Kategorie stellt einen Bereich dar, der häufig in bösartiger Software angetroffen wird, und basiert auf einer eingehenden Analyse von mehr als 100 Millionen Binärdateien. Der Bericht „Bedrohungsindikatoren“ zeigt an, wie viele dieser Kategorien in der Datei vorhanden waren.

Anomalien
Die Datei verfügt über Elemente, die in irgendeiner Form inkonsistent oder nicht normal nicht. Häufig sind Inkonsistenzen hinsichtlich der Dateistruktur vorhanden.

Erfassung
Die Datei enthält Anzeichen von Datenerfassungsaktivitäten. Dies kann eine Aufzählung von Gerätekonfigurationen oder eine Erfassung sensibler Informationen sein.

Datenverlust
Die Datei enthält Anzeichen von Datenexfiltration. Dies können ausgehende Netzwerkverbindungen sein, Anzeichen für die Übernahme von Browseraktivitäten oder sonstige Netzwerkdatenübertragungen.

Verschleierung
Die Datei enthält Anzeichen von versuchter Verschleierung. Die Verschleierung kann durch Ausblendung von Abschnitten erfolgen oder durch Einfügung von Code, der die Erkennung verhindern soll. Es können ferner Anzeichen für eine unsachgemäße Bezeichnung in den Metadaten oder anderen Abschnitten vorhanden sein.

Vernichtung
Die Datei enthält Anzeichen von zerstörerischen Funktionen. Dazu gehört auch die Fähigkeit, Geräteressourcen zu vernichten, wie z. B. Dateien und Verzeichnisse.

Sonstiges
Alle sonstigen Indikatoren, die keiner dieser Kategorien zugeordnet werden können.

Hinweis: Es kann vorkommen, dass die Abschnitte „Bedrohungsindikatoren“ und „Detaillierte Bedrohungsdaten“ keine Ergebnisse aufweisen oder nicht verfügbar sind. Dies ist der Fall, wenn die Datei nicht hochgeladen wurde. Die Debug-Protokollierung kann Aufschluss darüber geben, warum die Datei nicht hochgeladen wurde.

Behandeln von Bedrohungen

Die Art der Maßnahme, die für bestimmte Bedrohungen zu ergreifen ist, kann vom Benutzer abhängig sein, der dem Gerät zugewiesen ist. Maßnahmen für Bedrohungen können auf Geräteebene oder auf globaler Ebene angewendet werden. Nachfolgend sind die Maßnahmen aufgeführt, die für erkannte Bedrohungen oder Dateien durchgeführt werden können:

- ***Quarantäne:*** Das Verschieben der Datei in *Quarantäne*, sodass die Datei nicht auf dem Gerät ausgeführt werden kann.

  Hinweis: Sie können Bedrohungen mit der Befehlszeile auf einem Gerät in Quarantäne verschieben. Diese Funktion steht nur mit dem Windows Agent zur Verfügung. Siehe Quarantäne durch Befehlszeile für weitere Informationen.

- ***Globale Quarantäne:*** Das Verschieben der Datei in *globale Quarantäne*, sodass die Datei auf keinem Gerät in der gesamten Organisation ausgeführt werden kann.

Hinweis: Das Verschieben einer Datei in *Quarantäne* bedeutet, dass die Datei vom ursprünglichen Speicherort in das *Quarantäneverzeichnis* verschoben wird (`C:\ProgramData\Cylance\Desktop\q`).

- ***Freigeben:*** Das *Freigeben* einer Datei bewirkt, dass sie auf dem angegebenen Gerät ausgeführt werden kann.
- ***Globale sichere Liste:*** Das Verschieben der Datei in die *globale sichere Liste* bewirkt, dass die Datei auf jedem Gerät der Organisation ausgeführt werden kann.

  Hinweis: Gelegentlich kommt es vor, dass eine „gutartige" Datei von Threat Defense in *Quarantäne* verschoben oder 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 *globale sichere Liste* hilfreich sein.
- ***Datei hochladen:*** Sie können eine Datei manuell zur Analyse auf Cylance Infinity hochladen. Wenn die Option für automatisches Hochladen aktiviert ist, werden neue Dateien (die nicht von Cylance analysiert wurden) automatisch auf Cylance Infinity hochgeladen. Ist die Datei in Cylance Infinity vorhanden, steht die Schaltfläche „Datei hochladen" nicht zur Verfügung (ausgegraut).
- ***Datei herunterladen:*** Sie können eine Datei herunterladen, um sie selbst zu analysieren. Diese Funktion muss für die Organisation aktiviert sein. Der Benutzer muss ein Administrator sein. Die Bedrohung muss unter Verwendung der Agentenversion 1320 oder höher erkannt werden.

  Hinweis: Die Datei muss in Cylance Infinity verfügbar sein und alle drei Hashes (SHA256, SHA1 und MD5) zwischen Cylance Infinity und dem Agenten müssen übereinstimmen. Ist dies nicht der Fall, steht die Schaltfläche „Datei herunterladen" nicht zur Verfügung.

Behandeln von Bedrohungen auf einem bestimmten Gerät

1. Melden Sie sich bei der Konsole (http://dellthreatdefense.com) als Administrator oder Zonenmanager an.
2. Klicken Sie auf die Registerkarte **Geräte**.
3. Suchen Sie nach dem gewünschten Gerät, und wählen Sie es aus.
4. Möglicherweise ist auf der Registerkarte „Schutz" ein Link zum Gerät verfügbar, falls es mit einer bestimmten Bedrohung aufgeführt wird.
5. Sämtliche Bedrohungen auf diesem Gerät werden im unteren Bereich der Seite aufgeführt. Wählen Sie entweder das Stellen unter *Quarantäne* oder die *Freigabe* der Datei auf diesem Gerät aus.

Globales Behandeln von Bedrohungen

Dateien, die zur *globalen Quarantäneliste* oder *globalen sicheren Liste* hinzugefügt wurden, werden entweder *in Quarantäne* verschoben, oder die Datei *darf* auf allen Geräten in allen Zonen ausgeführt werden.

1. Melden Sie sich als Administrator bei der Konsole (http://dellthreatdefense.com) an.
2. Klicken Sie auf **Einstellungen** > **Globale List**e.
3. Klicken Sie auf „Globale Quarantäne" oder „Sicher".
4. Klicken Sie auf **Datei hinzufügen**.
5. Geben Sie SHA256 (erforderlich), MD5 und den Namen der Datei an sowie den Grund für die Aufnahme in die *globale Liste*.
6. Klicken Sie auf **Senden**.

Schutz – Skriptsteuerung

Threat Defense stellt Details zu aktiven Skripten und PowerShell-Skripten bereit, die blockiert oder gemeldet wurden. Wenn die Skriptsteuerung aktiviert ist, werden die Ergebnisse auf der Registerkarte „Skriptsteuerung“ der Seite „Schutz“ angezeigt. Sie geben Aufschluss über das Skript und die betroffenen Geräte.

So zeigen Sie die Ergebnisse der Skriptsteuerung an:

1. Melden Sie sich als Administrator bei der Konsole (http://dellthreatdefense.com) an.
2. Klicken Sie auf „Schutz“.
3. Klicken Sie auf „Skriptsteuerung“.
4. Wählen Sie ein Skript aus der Tabelle aus. Daraufhin wird die Tabelle „Details“ mit einer Liste der betroffenen Geräte aktualisiert.

Beschreibung der Spalte „Skriptsteuerung“

- **Dateiname:** Der Name des Skripts.
- **Interpretierer:** Die Skriptsteuerungsfunktion, die das Skript identifiziert hat.
- **Zuletzt gefunden:** Das Datum und die Uhrzeit der letzten Skriptausführung.
- **Laufwerktyp:** Typ des Laufwerks, auf dem das Skript gefunden wurde (z. B. interne Festplatte).
- **SHA256:** Der SHA 256-Hash des Skripts.
- **Anzahl der Geräte:** Die Anzahl der von diesem Skript betroffenen Geräte.
- **Warnung:** Die Anzahl der Warnungen, die für das Skript ausgegeben wurden. Dies kann mehrere Blockierungen für ein und dasselbe Gerät beinhalten.
- **Blockieren:** Gibt an, wie häufig das Skript blockiert wurde. Dies kann mehrere Blockierungen für ein und dasselbe Gerät beinhalten.

Beschreibung der Spalte „Details“

- **Gerätename:** Der Name des von dem Skript betroffenen Geräts. Klicken Sie auf den Gerätenamen, um die Seite „Gerätedetails“ aufzurufen.
- **Status:** Der Zustand des Geräts (online oder offline).
- **Agenten-Version:** Die Versionsnummer des derzeit auf dem Gerät installierten Agenten.
- **Dateipfad:** Der Dateipfad, an dem das Skript ausgeführt wurde.
- **Wann:** Das Datum und die Uhrzeit der Skriptausführung.
- **Benutzername:** Der Name des Benutzers, der bei der Ausführung des Skripts angemeldet war.
- **Maßnahme:** Maßnahme, die auf dem Skript ausgeführt wurde (Warnen oder Blockieren).

Globale Liste

Globale Liste ermöglicht die Markierung einer Datei für die *Quarantäne* oder das *Zulassen* dieser Dateien auf allen Geräten in der Organisation.

- **Globale Quarantäne:** Alle Agenten in der Organisation stellen alle Dateien auf der *globalen Quarantäneliste*, die auf dem Gerät erkannt werden, in *Quarantäne*.
- **Sicher:** Alle Agenten in der Organisation *lassen* alle Dateien auf der *sicheren Liste*, die auf dem Gerät erkannt werden, *zu*.
- **Nicht zugewiesen:** Bedrohungen, die in der Organisation identifiziert, aber weder der Liste *Globale Quarantäne* noch der *sicheren Liste* zugewiesen wurden.

Ändern des Bedrohungsstatus

So ändern Sie den Bedrohungsstatus (*Globale Quarantäne*, *Sicher* oder *Nicht zugewiesen*):

1. Melden Sie sich als Administrator bei der Konsole (http://dellthreatdefense.com) an.
2. Wählen Sie **Einstellungen > Globale Liste** aus.
3. Wählen Sie die Liste aus, der die Bedrohung derzeit zugewiesen ist. Beispiel: Klicken Sie auf „Nicht zugewiesen“, um eine nicht zugewiesene Bedrohung mit dem Status *Sicher* oder *Globale Quarantäne zu ändern*.

4. Markieren Sie die Kontrollkästchen der Bedrohungen, deren Status Sie ändern möchten, und klicken Sie auf eine Statusschaltfläche.
    a. Sicher: Verschiebt die Dateien in die *sichere Liste*.
    b. Globale Quarantäne: Verschiebt die Dateien in die *globale Quarantäneliste*.
    c. Aus Liste entfernen: Verschiebt die Dateien in die *Liste „Nicht zugewiesen“*.

Hinzufügen einer Datei

Manuelles Hinzufügen einer Datei zur *globalen Quarantäneliste* oder *sicheren Liste*. Dazu werden die SHA256-Hash-Informationen für die hinzuzufügende Datei benötigt.

1. Melden Sie sich als Administrator bei der Konsole (http://dellthreatdefense.com) an.
2. Wählen Sie **Einstellungen > Globale Liste** aus.
3. Wählen Sie die Liste aus, zu der Sie die Datei hinzufügen möchten (*Globale Quarantäne* oder *Sicher*).
4. Klicken Sie auf **Datei hinzufügen**.
5. Geben Sie die SHA256-Hash-Informationen ein. Geben Sie optional die MD5-Informationen und den Dateinamen an.
6. Geben Sie einen Grund für das Hinzufügen der Datei an.
7. Klicken Sie auf **Senden**.

Verschieben in die sichere Liste per Zertifikat

Kunden haben die Möglichkeit, Dateien nach signiertem Zertifikat auf die *sichere Liste* zu setzen, wodurch jegliche benutzerdefinierte Software, die ordnungsgemäß signiert ist, ohne Unterbrechung ausgeführt werden kann.

Hinweis: Diese Funktion ist derzeit nur für Windows-Betriebssysteme verfügbar.

- Diese Funktion ermöglicht Kunden das Erstellen einer *White List*/*sicheren Liste* nach signiertem Zertifikat, das vom SHA1- Fingerabdruck des Zertifikats dargestellt wird.
- Die Zertifikatinformationen werden von der Konsole extrahiert (Zeitstempel, Betreff, Herausgeber und Fingerabdruck). Das Zertifikat wird nicht hochgeladen oder auf der Konsole gespeichert.
- Der Zeitstempel des Zertifikats gibt an, wann das Zertifikat erstellt wurde.
- Die Konsole überprüft nicht, ob das Zertifikat aktuell oder abgelaufen ist.
- Ändert sich das Zertifikat (Verlängerung oder neues Zertifikat), sollte es in der Konsole zur *sicheren Liste* hinzugefügt werden.

1. Fügen Sie die Zertifikatdetails zum Zertifikat-Repository hinzu.
    a. Identifizieren Sie den Fingerabdruck des Zertifikats für die signierte PE-Datei (Portable Executable).
    b. Wählen Sie **Einstellungen > Zertifikate** aus.
    c. Klicken Sie auf **Zertifikat hinzufügen**.
    d. Klicken Sie entweder auf **Zertifikate zum Hinzufügen suchen** oder platzieren Sie das Zertifikat per Drag-and-Drop im Meldungsfenster.
    e. Falls Sie die Option zum Suchen nach Zertifikaten ausgewählt haben, wird das Fenster „Öffnen“ angezeigt, und Sie können die Zertifikate auswählen.

f. Optional können Sie Anmerkungen zum Zertifikat hinzufügen.

g. Klicken Sie auf **Senden**. Herausgeber, Betreff, Fingerabdruck und Anmerkungen (falls eingegeben) werden zum Repository hinzugefügt.

2. Fügen Sie das Zertifikat zur *sicheren Liste* hinzu.

   a. Wählen Sie **Einstellungen > Globale Liste** aus.

   b. Wählen Sie die Registerkarte **Sicher** aus.

   c. Klicken Sie auf **Zertifikate**.

   d. Klicken Sie auf **Zertifikat hinzufügen**.

   e. Wählen Sie ein Zertifikat aus der *sicheren Liste* aus. Wählen Sie optional eine Kategorie aus, und geben Sie einen Grund für das Hinzufügen des Zertifikats an.

   f. Klicken Sie auf **Senden**.

Anzeigen von Fingerabdrücken für eine Bedrohung

Auf der Registerkarte „Schutz“ wird nunmehr der Fingerabdruck des Zertifikats bei den Bedrohungsdetails angezeigt. Wählen Sie auf dem Bildschirm **Zu Zertifikat hinzufügen** aus, um das Zertifikat zum Repository hinzuzufügen.

Berechtigungen

Die Funktion **Zu Zertifikat hinzufügen** ist nur für Administratoren verfügbar. Falls das Zertifikat bereits im Repository enthalten ist, wird in der Konsole **Zu Zertifikat wechseln** angezeigt. Zertifikate sind für Zonenmanager schreibgeschützt. Für sie wird die Option **Zu Zertifikat wechseln** angezeigt.

Profil

Im Menü „Profil“ (obere rechte Ecke) können Sie Ihr Konto verwalten, Überprüfungsprotokolle der Konsole anzeigen und die Produkthilfe aufrufen.

Mein Konto

Auf der Seite „Mein Konto“ können Sie Ihr Passwort und die Einstellungen für E-Mail-Benachrichtigungen ändern.

1. Melden Sie sich bei der Konsole an (http://dellthreatdefense.com).
2. Klicken Sie in der oberen rechten Ecke auf das Menü „Profil“, und wählen Sie **Mein Konto** aus.
3. So ändern Sie Ihr Passwort:

   a. Klicken Sie auf „Passwort ändern“.

   b. Geben Sie Ihr altes Passwort ein.

   c. Geben Sie Ihr neues Passwort ein, und bestätigen Sie es durch erneute Eingabe.

   d. Klicken Sie auf Aktualisieren.

4. Markieren bzw. deaktivieren Sie das Kontrollkästchen, um E-Mail-Benachrichtigungen zu aktivieren bzw. zu deaktivieren. Das Aktivieren und Deaktivieren des Kontrollkästchens wird automatisch gespeichert. E-Mail-Benachrichtigungen sind nur für Administratoren verfügbar.

Überprüfungsprotokollierung

Dropdown-Liste mit Benutzersymbol (obere rechte Ecke der Konsole)

Das Überprüfungsprotokoll enthält Informationen zu den folgenden auf der Konsole durchgeführten Maßnahmen:

- Anmeldung (erfolgreich, fehlgeschlagen)
- Richtlinie (hinzufügen, bearbeiten, entfernen)
- Gerät (bearbeiten, entfernen)
- Bedrohung (Quarantäne, freigeben, globale Quarantäne, sichere Liste)
- Benutzer (hinzufügen, bearbeiten, entfernen)
- Agentenaktualisierung (bearbeiten)

Das Überprüfungsprotokoll kann über die Konsole aufgerufen werden. Wechseln Sie dazu in die Dropdown-Liste „Profil“ in der oberen rechten Ecke der Konsole, und wählen Sie **Auditprotokoll** aus. Überprüfungsprotokolle sind nur für Administratoren verfügbar.

Einstellungen

Auf der Seite „Einstellungen“ sind die Registerkarten „Anwendung“, „Benutzerverwaltung“, „Geräterichtlinie“, „Globale Liste“ und „Agentenaktualisierung“ enthalten. Das Menü „Einstellungen“ ist nur für Administratoren verfügbar.

ANWENDUNG

Threat Defense Agent

Geräte werden durch Installieren von Threat Defense Agent auf den einzelnen Endpunkten zur Organisation hinzugefügt. Nachdem die Verbindung zur Konsole hergestellt wurde, können Sie Richtlinien anwenden (um identifizierte Bedrohungen zu verwalten) und die Geräte nach den Anforderungen der Organisation anordnen.

Threat Defense Agent ist auf einen minimalen Verbrauch von Systemressourcen ausgelegt. Der Agent behandelt vorrangig Dateien oder Prozesse, die gerade ausgeführt werden, da diese Ereignisse besonders riskant sind. Dateien, die lediglich im Speicher abgelegt sind, aber nicht ausgeführt werden, haben eine geringere Priorität. Diese könnten zwar bösartig sein, stellen jedoch keine akute Bedrohung dar.

Windows-Agent

Systemanforderungen

Dell empfiehlt eine Endpunkthardware (CPU, GPU usw.), die mindestens den Anforderungen des Zielbetriebssystems entspricht. Ausnahmen sind unten angegeben (RAM, verfügbarer Festplattenspeicherplatz und zusätzliche Software/Anforderungen).

Betriebssysteme	• Windows 7 *(32-Bit und 64-Bit)* • Windows Embedded Standard 7 *(32-Bit)* und Windows Embedded Standard 7 Pro *(64-Bit)* • Windows 8 und 8.1 *(32-Bit und 64-Bit)** • Windows 10 *(32-Bit und 64-Bit)***** • Windows Server 2008 und 2008 R2 *(32-Bit und 64-Bit)**** • Windows Server 2012 und 2012 R2 *(64-Bit)**** • Windows Server 2016 – Standard, Data Center und Essentials*****
RAM	• 2 GB
Verfügbarer Festplattenspeicherplatz	• 300 MB
Zusätzliche Software/Anforderungen	• .NET Framework 3.5 (SP1) oder höher (*nur Windows*) • Internet-Browser • Internetzugang für Anmeldung, Zugriff auf das Installationsprogramm und Produktregistrierung • Lokale Administratorrechte zur Installation der Software
Weitere Anforderungen	• TLS 1.2 wird mit Agent 1422 oder höher unterstützt und erfordert .NET Framework 4.5 oder höher

Tabelle 2: Systemanforderungen für Windows

*Nicht unterstützt: Windows 8.1 RT
**Windows 10 Anniversary Update erfordert Agent 1402 oder höher.
***Nicht unterstützt: Server Core (2008 und 2012) und Minimal Server (2012).
**** Erfordert Agent 1412 oder höher.

So laden Sie die Installationsdatei herunter:

1. Melden Sie sich an der Konsole an (http://dellthreatdefense.com).
2. Wählen Sie **Einstellungen** > **Anwendung** aus.
3. Kopieren Sie den **Installations-Token**.

   Das Installationstoken ist eine willkürlich generierte Zeichenkette, die dem Agenten die Berichterstattung an das ihm zugewiesene Konto auf der Konsole ermöglicht. Das Installationstoken wird im Rahmen der Installation benötigt, entweder im Installationsassistenten oder als Parametereinstellung.
4. Laden Sie das Installationsprogramm herunter.
   a. Wählen Sie das Betriebssystem aus.
   b. Wählen Sie den Dateityp aus, der heruntergeladen werden soll.

      Bei Verwendung von Windows empfiehlt Dell für die Installation des Agenten die MSI-Datei.

Tipp: Wenn eine Zonenregel eingerichtet ist, können Geräte automatisch einer Zone zugewiesen werden, falls sie den Kriterien der Zonenregel entsprechen.

Installieren des Agenten – Windows

Stellen Sie vor der Installation von Threat Defense sicher, dass alle Voraussetzungen erfüllt sind. Siehe Systemanforderungen.

1. Doppelklicken Sie auf die Datei „DellThreatDefenseSetup.exe“ (oder MSI), um mit der Installation zu beginnen.
2. Klicken Sie im Threat Defense-Setup-Fenster auf **Installieren**.
3. Geben Sie das Installationstoken ein, das vom Threat Defense-Mandanten bereitgestellt wurde. Klicken Sie auf **Weiter**.

   Anmerkung: Wenden Sie sich an Ihren Threat Defense-Administrator, oder lesen Sie den Artikel in der Wissensdatenbank How To: Threat Defense verwalten, falls der Zugriff auf das Installations-Token nicht verfügbar ist.
4. Ändern Sie optional den Zielordner von Threat Defense.

   Klicken Sie auf **OK**, um mit der Installation zu beginnen.
5. Klicken Sie auf **Fertigstellen**, um die Installation abzuschließen. Markieren Sie das Kontrollkästchen, um Threat Defense zu starten.

Installationsparameter für Windows

Der Agent kann interaktiv oder nicht interaktiv über GPO, Microsoft System Center Configuration Manager (kurz SCCM) und MSIEXEC installiert werden. Die MSIs können mithilfe von integrierten Parametern angepasst werden (siehe unten). Die Parameter können auch über die Befehlszeile bereitgestellt werden.

Eigenschaft	Wert	Beschreibung
PIDKEY	<Installationstoken>	Automatische Eingabe des Installationstokens
LAUNCHAPP	0 oder 1	0: Das Taskleistensymbol und der Startmenüordner

Eigenschaft	Wert	Beschreibung
		werden während der Laufzeit ausgeblendet. 1: Das Taskleistensymbol und der Startmenüordner werden während der Laufzeit nicht ausgeblendet (Standardeinstellung).
SELFPROTECTIONLEVEL	1 oder 2	1: Nur lokale Administratoren können Änderungen an der Registrierung und an den Diensten vornehmen. 2: Nur der Systemadministrator kann Änderungen an der Registrierung und an den Diensten vornehmen (Standardeinstellung).
APPFOLDER	<Zielordner für Installation>	Gibt das Installationsverzeichnis für den Agenten an. Der Standardspeicherort ist C:\Programme\Cylance\Desktop.
VenueZone	„Zone_Name“	Erfordert Agenten-Version 1382 oder höher • Dient zum Hinzufügen von Geräten zu einer Zone. • Wenn die Zone nicht vorhanden ist, wird die Zone unter Verwendung des angegebenen Namens erstellt. • Ersetzen Sie zone_name mit den Namen einer vorhandenen Zone oder einer Zone, die Sie erstellen möchten. **Warnung**: Durch das Hinzufügen von Leerzeichen vor oder nach dem Zonennamen wird eine neue Zone erstellt.

Tabelle 3: Installationsparameter für Windows

Das folgende Befehlszeilenbeispiel veranschaulicht die Ausführung des Microsoft Windows-Installationstools (MSIEXEC) unter Verwendung der Parameter PIDKEY, APPFOLDER und LAUNCHAPP:

```
msiexec /i DellThreatDefenseSetup_x64.msi /qn PIDKEY=<INSTALLATION TOKEN>
LAUNCHAPP=0 /L*v C:\temp\install.log
```

Die Installation erfolgt im Hintergrund, und das Installationsprotokoll wird unter **`C:\temp`** gespeichert. Während der Agent ausgeführt wird, sind das Taskleistensymbol und der Threat Defense-Startmenüordner ausgeblendet. Weitere Informationen zu verschiedenen von MSIEXEC akzeptierten Befehlszeilenoptionen finden Sie im Artikel KB 227091.

Installieren des Windows-Agenten unter Verwendung von Wyse Device Manager (WDM)

In diesem Abschnitt wird erläutert, wie Sie ein Installationsskript erstellen, wie Sie ein RSP-Paket für WDM erstellen und es zu WDM hinzufügen, um eine Installation auf mehreren Thin Clients gleichzeitig und ohne Benutzereingriff durchzuführen.

Erstellen Sie ein Stapeldateiskript für die Installation von Threat Defense über die Befehlszeile. WDM führt dieses Skript während der Bereitstellung aus.

1. Öffnen Sie Notepad. Verwenden Sie die oben aufgeführten Befehlszeilenparameter, und geben Sie den folgenden Befehl ein, um die Installation auszuführen. Ersetzen Sie dabei den Eintrag **`<INSTALLATION TOKEN>`** mit Ihrem bereitgestellten Token:

msiexec /i C:\TDx86\DellThreatDefense_x86.msi PIDKEY=<INSTALLATION TOKEN> /q

C:\TDx86 wird für unser Verzeichnis verwendet, da dieser Ordner bei der Installation an diesen Speicherort auf dem Thin Client kopiert wird.

2. Speichern Sie die Datei mit einer **.bat**-Erweiterung im TDx86-Ordner. Beispiel: **TDx86_Install.bat**.

   Erstellen Sie ein RSP-Paket, mit dem die Anwendung Threat Defense Agent auf mehreren Thin Clients gleichzeitig ohne Benutzerinteraktion installiert werden kann.

3. Öffnen Sie Scriptbuilder auf einem Computer, auf dem WDM installiert ist.
4. Geben Sie einen Namen für das Paket und eine Beschreibung ein.
   - Wählen Sie unter „Paketkategorie“ den Eintrag „Sonstige Pakete“ aus.
   - Wählen Sie als Betriebssystem „Windows Embedded Standard 7“ aus.
5. Fügen Sie Skriptbefehle hinzu, um sicherzustellen, dass es sich beim Zielsystem um WES7 oder WES7p handelt.
   - Wählen Sie den Skriptbefehl
   - Geben Sie als Wert für das Gerätebetriebssystem das jeweilige Betriebssystem ein.
6. Fügen Sie Elemente mithilfe der Doppelpfeile hinzu.
7. Drücken Sie **OK** bei Eingabeaufforderung.
8. Fügen Sie einen Befehl hinzu, um den Thin Client zu sperren und Benutzereingriffe zu verhindern.
   - Wählen Sie **Skriptbefehl**> **Lockout User (LU)** aus. Es muss kein Wert angegeben werden. Jedoch wird in diesem Beispiel ein **Wert** von **Ja** eingegeben, sodass der Startbildschirm entfernt wird, wenn das Installationsprogramm fehlschlägt oder ein Fehler auftritt.
9. Fügen Sie einen Befehl hinzu, um Dateien auf den schlanken Client zu kopieren.
   - Wählen Sie den Skriptbefehl **X Copy (XC**) aus.
   - Geben Sie als Wert für **Repository-Verzeichnis *** am Ende des vorhandenen Eintrags **<regroot>** ein.
   - Geben Sie als Wert für **Gerät-Directory** den Pfad zu den auf die Ziel-Thin Clients zu kopierenden Dateien ein. In diesem Beispiel wird der Paketname verwendet.
10. Fügen Sie einen Befehl hinzu, um das .bat-Installationsskript auszuführen.
    - Wählen Sie **Skriptbefehl** > **Execute on Device (EX)** aus.
    - Geben Sie als Wert für den Gerätedateinamen den Pfad **C:\TDx86\TDx86_install.bat**. ein. Der Ordner TDx86 wird über den vorhin eingegebenen XC-Befehl kopiert.
    - Fügen Sie **+** als Wert für die synchrone Ausführung hinzu. Dadurch wird WDM veranlasst, solange zu warten, bis die ausgeführte Datei vollständig abgeschlossen ist.
11. Fügen Sie einen Befehl hinzu, um kopierte Dateien vom schlanken Client zu löschen.
    12. Fügen Sie den Skriptbefehl **Delete Tree (DT)** hinzu.
12. Fügen Sie einen Befehl hinzu, um die Sperrung aufzuheben.

13. Fügen Sie den Skriptbefehl **End Lockout (EL**) hinzu.

13. Überprüfen Sie das Skriptpaket. Dieses sollte in etwa wie folgt aussehen.
    a. Falls Sie Threat Defense auf WES7P-Systemen bereitstellen möchten, aktualisieren Sie den Abschnitt mit dem Betriebssystem auf WES7P. Anderenfalls schlägt die Installation fehl.
14. Speichern Sie das Paket.
    14. Klicken Sie auf **Speichern,** und navigieren Sie zum Speicherort des **TDx86**-Ordners. Wenn diese Anweisungen befolgt wurden, befindet sich der Ordner auf dem Desktop.
15. Schließen Sie Scriptbuilder.
16. Starten Sie **WyseDeviceManager** zum Hinzufügen des Pakets zu WDM.
17. Navigieren Sie zu **WyseDeviceManager > Package Manager > andere Pakete**.
18. Wählen Sie **Aktion > Neu > Paket** aus der Menüleiste aus.
19. Wählen Sie **Ein Paket aus einer Skriptdatei registrieren (.RSP)** aus, und klicken Sie auf **Weiter**.
20. Navigieren Sie an den Speicherort der im vorherigen Schritt erstellen RSP-Datei, und klicken Sie auf **Weiter**.
21. Stellen Sie sicher, dass **Aktiv** ausgewählt ist, und klicken Sie auf **Weiter.**
22. Klicken Sie auf **Weiter**, sobald WDM zur Registrierung des Pakets bereit ist.
23. Klicken Sie auf **Fertig stellen,** wenn das Paket erfolgreich registriert wurde.
24. Das Paket wird unter **Andere Pakete** angezeigt.
25. Überprüfen Sie den Inhalt des Pakets:
    a. Öffnen Sie den Datei-Explorer, navigieren Sie zu **C:\inetpub\ftproot\Rapport** und suchen Sie den **TDx86-Ordner**.
    b. Öffnen Sie den TDx86-Ordner, und stellen Sie sicher, dass das Installationsprogramm und die .bat-Datei enthalten sind.

In WDM ist jetzt ein Paket vorhanden, mit dem Threat Defense ohne Benutzereingriff auf mehreren WES7-basierten Thin Clients bereitgestellt werden kann.

Quarantäne unter Verwendung der Befehlszeile

Sie können eine Datei mit der Befehlszeile auf einem Gerät in Quarantäne verschieben. Hierfür muss der SHA256-Hash der Gefahr bekannt sein.

Hinweis: Diese Funktion ist nur für Windows und erfordert Agent 1432 oder höher.

1. Öffnen Sie auf dem Windows-Gerät die Befehlszeile. Beispiel: Suchen Sie im Startmenü nach cmd.exe.
2. Rufen Sie Dell.ThreatDefense.exe auf, und fügen Sie das Argument **-q: <hash>** ein, wobei <hash> der SHA256-Hash für die Datei ist. Diese fordert den Agenten auf, die Datei in den Quarantäneordner zu verschieben.

   Beispiel-Befehlszeile (Dell Threat Defense im Standardpfad installiert):

   ```
   "C:\Program Files\Cylance\Desktop\Dell.ThreatDefense.exe" -q:
   14233D4875e148c370a6bbe40fccabccdbfa194dac9e8bd41b0eadcf2351f941
   ```

Mac OS X-Agent

Systemanforderungen

Dell empfiehlt eine Endpunkthardware (CPU, GPU usw.), die mindestens den Anforderungen des Zielbetriebssystems entspricht. Ausnahmen sind unten angegeben (RAM, verfügbarer Festplattenspeicherplatz und zusätzliche Software/Anforderungen).

Betriebssysteme	• Mac OS X 10.9 • Mac OS X 10.10 • Mac OS X 10.11 • macOS 10.12*
RAM	• 2 GB
Verfügbarer Festplattenspeicherplatz	• 300 MB

Tabelle 4: Systemanforderungen für Mac OS X

*Erfordert Agent 1412 oder höher.

So laden Sie die Installationsdatei herunter:

1. Melden Sie sich an der Konsole an (http://dellthreatdefense.com).
2. Wählen Sie **Einstellungen** > **Anwendung** aus.
3. Kopieren Sie den **Installations-Token**.

   Das Installationstoken ist eine willkürlich generierte Zeichenkette, die dem Agenten die Berichterstattung an das ihm zugewiesene Konto auf der Konsole ermöglicht. Das Installationstoken wird im Rahmen der Installation benötigt, entweder im Installationsassistenten oder als Parametereinstellung.
4. Laden Sie das Installationsprogramm herunter.
   a. Wählen Sie das Betriebssystem aus.
   b. Wählen Sie den Dateityp aus, der heruntergeladen werden soll.

Tipp: Wenn eine Zonenregel eingerichtet ist, können Geräte automatisch einer Zone zugewiesen werden, falls sie den Kriterien der Zonenregel entsprechen.

Installieren des Agenten – Mac OS X

Stellen Sie vor der Installation von Threat Defense sicher, dass alle Voraussetzungen erfüllt sind. Siehe Systemanforderungen.

Anmerkung: Der Mac OS X-Agent wird in einer künftigen Version unter der Marke Dell vertrieben.

1. Doppelklicken Sie auf **`DellThreatDefense.dmg`**, um das Installationsprogramm aufzurufen.
2. Doppelklicken Sie auf das Symbol *Schützen* in der PROTECT-Benutzeroberfläche, um mit der Installation zu beginnen.
3. Klicken Sie auf **Fortfahren**, um festzustellen, ob Betriebssystem und Hardware die Anforderungen erfüllen.
4. Klicken Sie auf dem Begrüßungsbildschirm auf **Fortfahren**.

5. Geben Sie das Installationstoken ein, das vom Threat Defense-Mandanten bereitgestellt wurde. Klicken Sie auf **Weiter**.

Anmerkung: Wenden Sie sich an Ihren Threat Defense-Administrator, oder lesen Sie den Artikel in der Wissensdatenbank How To: Threat Defense verwalten, falls der Zugriff auf das Installations-Token nicht verfügbar ist.

6. Ändern Sie optional den Installationsspeicherort von Threat Defense.

   Klicken Sie auf **Installieren**, um mit der Installation zu beginnen.

7. Geben Sie den Benutzernamen und das Passwort eines Administrators ein. Klicken Sie auf **Software installieren**.

8. Klicken Sie auf dem Übersichtsbildschirm auf **Schließen**.

Installationsparameter für Mac OS X

Threat Defense Agent kann unter Verwendung von Befehlszeilenoptionen im Terminal installiert werden. In den nachfolgenden Beispielen wird das Installationsprogramm PKG verwendet. Bei Verwendung von DMG ändern Sie einfach die Dateierweiterung im Befehl.

Hinweis: Stellen Sie sicher, dass die Zielendpunkte die Systemanforderungen erfüllen, und dass die Person, die die Software installiert, über die entsprechenden Anmeldeinformationen verfügt.

Eigenschaft	Wert	Beschreibung
InstallToken		Installationstoken, das in der Konsole verfügbar ist.
NoCylanceUI		Das Agentensymbol wird beim Start nicht angezeigt. Die Standardeinstellung ist „Sichtbar“.
SelfProtectionLevel	0 oder 1	1: Nur lokale Administratoren können Änderungen an der Registrierung und an den Diensten vornehmen. 2: Nur der Systemadministrator kann Änderungen an der Registrierung und an den Diensten vornehmen (Standardeinstellung).
LogLevel	0, 1, 2 oder 3	0: Fehler – Nur Fehlermeldungen werden protokolliert. 1: Warnung – Es werden Fehlermeldungen und Warnmeldungen protokolliert. 2: Informationen (Standardeinstellung) – Es werden Fehlermeldungen, Warnmeldungen und Informationsmeldungen protokolliert. Diese Details können für die Fehlerbehebung hilfreich sein. 3: Ausführlich – Alle Meldungen werden protokolliert. Dies ist die empfohlene Protokollierungsebene für die Fehlerbehebung. Ausführliche Protokolldateien können jedoch sehr umfangreich sein. Dell empfiehlt daher, die ausführliche Protokollierung nur für die Fehlerbehebung zu aktivieren und anschließend auf die Ebene „Informationen“ zurückzusetzen.
VenueZone	„Zone_Name“	Erfordert Agenten-Version 1382 oder höher • Dient zum Hinzufügen von Geräten zu einer Zone. • Wenn die Zone nicht vorhanden ist, wird die Zone

Eigenschaft	Wert	Beschreibung
		unter Verwendung des angegebenen Namens erstellt. • Ersetzen Sie zone_name mit den Namen einer vorhandenen Zone oder einer Zone, die Sie erstellen möchten. **Warnung**: Durch das Hinzufügen von Leerzeichen vor oder nach dem Zonennamen wird eine neue Zone erstellt.

Tabelle 5: Installationsparameter für Mac OS X

Installieren des Agenten

Installation ohne Installationstoken

```
sudo installer –pkg DellThreatDefense.pkg –target/
```

Installation mit Installationstoken

```
echo [install_token] > cyagent_install_token

sudo installer –pkg DellThreatDefense.pkg –target/
```

Hinweis: Ersetzen Sie **`[install_token]`** durch das Installations-Token. Der Echo-Befehl gibt eine **`cyagent_install_token`**-Datei aus, bei der es sich um eine Textdatei mit einer Installationsoption pro Zeile handelt. Diese Datei muss sich im selben Ordner befinden, wie das Installationspaket. Seien Sie vorsichtig bei Dateierweiterungen, das obige Beispiel zeigt, dass die Datei cyagent_install_token keine Dateierweiterung hat. Standardeinstellungen innerhalb Mac OSX und macOS sorgen für die Ausblendung der Erweiterungen. Beim manuellen Erstellen dieser Datei mit Text Edit oder einem anderen Texteditor kann automatisch eine Dateinamenserweiterung angefügt werden, die entfernt werden muss.

Optionale Installationsparameter

Geben Sie zum Erstellen einer Datei (**`cyagent_install_token`**), die das Installationsprogramm verwendet, um die eingegebenen Optionen anzuwenden, Folgendes im Terminal ein. Jeder Parameter muss in einer eigenen Zeile eingegeben werden. Diese Datei muss sich im selben Ordner befinden, wie das Installationspaket.

Die folgende Konfiguration ist ein Beispiel. Es müssen nicht alle Parameter in der Datei vorhanden sein. Terminal berücksichtigt alles, was in der Datei zwischen einfache Anführungszeichen gesetzt wird. Drücken Sie nach jedem Parameter die Eingabetaste/Rücktaste, um sicherzustellen, dass sich jeder Parameter in der Datei in einer eigenen Zeile befindet.

Sie können auch einen Texteditor verwenden, um die Datei mit den einzelnen Parametern (jeweils in einer eigenen Zeile) zu erstellen. Diese Datei muss sich im selben Ordner befinden, wie das Installationspaket.

Beispiel:

```
echo 'InstallToken

NoCylanceUI

SelfProtectionLevel=2

LogLevel=2'> cyagent_install_token
```

```
sudo installer –pkg DellThreatDefense.pkg –target/
```

Deinstallieren des Agenten

Ohne Passwort

```
sudo /Applications/Cylance/Uninstall\
DellThreatDefense.app/Contents/MacOS/Uninstall\ DellThreatDefense
```

Mit Passwort

```
sudo /Applications/Cylance/Uninstall\
DellThreatDefense.app/Contents/MacOS/Uninstall\ DellThreatDefense --
password=thisismypassword
```

Hinweis: Ersetzen Sie **`thisismypassword`** durch das Deinstallationskennwort, das in der Konsole erstellt wurde.

Agentendienst

Starten des Dienstes

```
sudo launchctl load
/Library/launchdaemons/com.cylance.agent_service.plist
```

Beenden des Dienstes

```
sudo launchctl unload
/Library/launchdaemons/com.cylance.agent_service.plist
```

Überprüfung der Installation

Überprüfen Sie die folgenden Dateien, um sicherzustellen, dass der Agent erfolgreich installiert wurde.

1. Der Programmordner wurde angelegt.
    - Standard-Speicherort unter Windows: **`C:\Programme\Cylance\Desktop`**
    - Standard-Speicherort unter Mac OS X: **`/Applications/DellThreatDefense/`**
2. Das Threat Defense-Symbol wird in der Taskleiste des Zielgeräts angezeigt.

   Dies gilt nicht, wenn der Parameter LAUNCHAPP=0 (Windows) oder NoCylanceUI (Mac OS X) verwendet wurde.
3. Auf dem Zielgerät wird im Startmenü unter „Alle Programme“ ein Threat Defense-Ordner angezeigt.

   Dies gilt nicht, wenn der Parameter LAUNCHAPP=0 (Windows) oder NoCylanceUI (Mac OS X) verwendet wurde.
4. Der Threat Defense-Dienst wurde hinzugefügt und wird ausgeführt. Auf dem Zielgerät wird der Threat Defense-Dienst im Bereich „Windows-Dienste“ als ausgeführt angezeigt.
5. Der Prozess „Dell.ThreatDefense.exe“ wird ausgeführt. Auf dem Zielgerät wird der Prozess „Dell.ThreatDefense.exe“ im Windows Task Manager auf der Registerkarte „Prozesse“ aufgeführt.
6. Das Gerät gibt Berichte an die Konsole aus. Melden Sie sich an der Konsole an, und klicken Sie auf die Registerkarte „Geräte“. Das Gerät müsste dort aufgeführt werden und sollte online sein.

Agenten-Benutzeroberfläche

Die Agenten-Benutzeroberfläche ist standardmäßig aktiviert. Klicken Sie in der Taskleiste auf das Agentensymbol, um die Benutzeroberfläche aufzurufen. Der Agent kann auch so installiert werden, dass das Agentensymbol in der Taskleiste ausgeblendet wird.

Registerkarte „Bedrohungen“

Zeigt alle auf dem Gerät erkannten Bedrohungen sowie die durchgeführten Maßnahmen an. *Unsicher* bedeutet, dass bezüglich der Bedrohung keine Maßnahmen ergriffen wurden. *In Quarantäne* bedeutet, dass die Bedrohung modifiziert wurde (um die Ausführung der Datei zu verhindern) und in den Ordner *Quarantäne* verschoben wurde. *Freigegeben* bedeutet, dass die Datei vom Administrator als sicher klassifiziert wurde und zur Ausführung auf dem Gerät *zugelassen* ist.

Registerkarte „Ereignisse“

Zeigt Bedrohungsereignisse an, die auf dem Gerät stattgefunden haben.

Registerkarte „Skripte“

Zeigt bösartige Skripte an, die auf dem Gerät ausgeführt wurden, sowie die Maßnahmen, die an dem Skript durchgeführt wurden.

Menü „Agent“

Das Menü „Agent“ bietet Zugriff auf die Hilfe und auf Aktualisierungen für Threat Defense. Außerdem besteht Zugriff auf die erweiterte Benutzeroberfläche, die weitere Menüoptionen enthält.

Menü „Agent“

Mithilfe des Menüs „Agent“ können Benutzer bestimmte Maßnahmen auf dem Gerät durchführen. Klicken Sie mit der rechten Maustaste auf das Agentensymbol, um das Menü anzuzeigen.

- **Auf Aktualisierungen überprüfen**: Der Agent überprüft, ob Aktualisierungen verfügbar sind, und installiert diese gegebenenfalls. Aktualisierungen sind auf die Agentenversion begrenzt, die in der Zone, der das Gerät angehört, zulässig ist.
- **Auf Richtlinienaktualisierung überprüfen**: Der Agent prüft, ob eine Richtlinienaktualisierung verfügbar ist. Es könnte sich um Änderungen der vorhandenen Richtlinien oder eine neue Richtlinie für den Agenten handeln.

  Hinweis: Das Überprüfen auf Richtlinienaktualisierungen wird in Version 1422 (oder höher) für Windows und Version 1432 (oder höher) für macOS unterstützt.
- **Über**: Zeigt ein Dialogfeld an, in dem die Agentenversion, der Name der dem Gerät zugewiesenen Richtlinie, der Zeitpunkt der letzten Suche nach Aktualisierungen und das bei der Installation verwendete Token aufgeführt sind.
- **Beenden**: Schließt das Agentensymbol in der Taskleiste. Durch diesen Vorgang wird keiner der Threat Defense-Dienste deaktiviert.
- **Optionen > Benachrichtigungen anzeigen**: Wählen Sie diese Option aus, um neue Ereignisse als Benachrichtigungen anzuzeigen.

Aktivieren erweiterter Optionen auf der Agenten-Benutzeroberfläche

Threat Defense Agent bietet auf der Benutzeroberfläche einige erweiterte Optionen an, mit deren Hilfe Funktionen auf dem Gerät ohne Konnektivität zur Konsole ausgeführt werden können. Die Datei „CylanceSVC.exe“ muss ausgeführt werden, wenn die erweiterten Optionen aktiviert sind.

Windows

1. Wenn das Agentensymbol in der Taskleiste angezeigt wird, klicken Sie mit der rechten Maustaste auf das Symbol, und wählen Sie **Beenden** aus.
2. Starten Sie die Befehlseingabeaufforderung, und geben Sie den folgenden Befehl ein. Drücken Sie die Eingabetaste, wenn Sie fertig sind.

   ```
   cd C:\Program Files\Cylance\desktop
   ```

   Falls die Anwendung an einem anderen Speicherort installiert wurde, navigieren Sie in der Eingabeaufforderung zu diesem Speicherort.
3. Geben Sie den folgenden Befehl ein, und drücken Sie die Eingabetaste, wenn Sie fertig sind.

   ```
   Dell.ThreatDefense.exe –a
   ```

   Das Agentensymbol wird in der Taskleiste angezeigt.
4. Klicken Sie mit der rechten Maustaste auf das Symbol. Die Optionen *Protokollierung, Erkennung ausführen*, und *Threat Management* werden angezeigt.

Mac OSX/macOS

1. Wenn das Agentensymbol im oberen Menü angezeigt wird, klicken Sie mit der rechten Maustaste auf das Symbol, und wählen Sie **Beenden** aus.
2. Terminal öffnen und ausführen

   a. Sudo /Applications/DellThreatDefense/DellThreatDefense.app/Contents/MacOS/ DellThreatDefenseUI –a

   Hinweis: Dies ist der Standardinstallationspfad für Dell Threat Defense. Sie müssen den Pfad möglicherweise bearbeiten, um ihn ordnungsgemäß an Ihre Umgebung anzupassen.
3. Die Agenten-Benutzeroberfläche wird jetzt mit zusätzlichen Optionen angezeigt.

Protokollierung

Wählen Sie die Ebene der Protokollinformationen aus, die über den Agenten erfasst werden sollen. Die Standardeinstellung ist „Informationen“. Dell empfiehlt, für die Fehlerbehebung die Protokollebene „Alles“ (Ausführlich) zu verwenden. Setzen Sie nach Abschluss der Fehlerbehebung die Ebene zurück auf „Informationen“, da durch die Protokollierung aller Informationen sehr große Protokolldateien generiert werden können.

Erkennung ausführen

Ermöglicht Benutzern die Angabe eines Ordners für die Überprüfung von Bedrohungen.

1. Wählen Sie **Erkennung ausführen > Ordner angeben** aus.
2. Wählen Sie den zu überprüfenden Ordner aus, und klicken Sie auf **OK**. Die gefundenen Bedrohungen werden auf der Agenten-Benutzeroberfläche angezeigt.

Bedrohungsverwaltung

Ermöglicht Benutzern das Löschen von Dateien *in Quarantäne* auf dem Gerät.

1. Wählen Sie **Threat Management > Dateien in Quarantäne löschen** aus.
2. Klicken Sie zum Bestätigen auf **OK**.

Virtuelle Maschinen

Bei der Nutzung von Threat Defense Agent auf dem Image einer virtuellen Maschine sollten einige Empfehlungen beachtet werden.

Wenn Sie das Image einer virtuellen Maschine erstellen möchten, um es als Vorlage zu verwenden, trennen Sie die Netzwerkverbindung der virtuellen Maschine, bevor Sie den Agenten installieren. Dadurch wird verhindert, dass der Agent mit der Konsole kommuniziert und die Gerätedetails konfiguriert. Dies verhindert doppelte Geräte auf der Konsole.

Passwortgeschützte Deinstallation

EINSTELLUNGEN > Anwendung

Administratoren können ein Passwort für die Deinstallation des Agenten verlangen. Folgendes gilt bei der Deinstallation des Agenten mit Passwort:

- Falls für die Installation das MSI-Installationsprogramm verwendet wurde, können Sie die Deinstallation mit dem MSI oder über die Systemsteuerung durchführen.
- Falls für die Installation das EXE-Installationsprogramm verwendet wurde, verwenden Sie dieses auch für die Deinstallation. Die Deinstallation über die Systemsteuerung ist nicht möglich, wenn das EXE-Installationsprogramm verwendet wurde und ein Passwort für die Deinstallation erforderlich ist.
- Wenn Sie die Deinstallation über die Befehlszeile durchführen möchten, fügen Sie die folgende Deinstallationszeichenkette hinzu: **`UNINSTALLKEY = [MyUninstallPassword]`**.

So erstellen Sie ein Passwort für die Deinstallation:

1. Melden Sie sich mit einem Administratorkonto bei der Konsole (http://dellthreatdefense.com) an.
2. Wählen Sie **Einstellungen > Anwendung** aus.
3. Aktivieren Sie das Kontrollkästchen **Kennwort für die Agenten-Deinstallation verlangen**.
4. Geben Sie ein Passwort ein.
5. Klicken Sie auf **Speichern**.

Integrationen

Threat Defense Console kann in bestimmte Drittanbieterprogramme integriert werden.

Syslog/SIEM

Threat Defense kann unter Verwendung der Syslog-Funktion in die Software „Security Information Event Management“ (SIEM) integriert werden. Syslog-Ereignisse werden zum selben Zeitpunkt permanent, zu dem die Agentenereignisse für die Konsole permanent werden.

Die neuesten IP-Adressen für Syslog-Meldungen erhalten Sie beim Dell Support.

Ereignistypen

Überprüfungsprotokoll

Wählen Sie diese Option aus, um das Überprüfungsprotokoll der in der Konsole (Website) durchgeführten Benutzermaßnahmen an den Syslog-Server zu senden. Ereignisse des Überprüfungsprotokolls werden immer im Bildschirm „Überprüfungsprotokoll“ angezeigt, auch wenn diese Option nicht markiert ist.

Beispielmeldung für die Weiterleitung des Überprüfungsprotokolls an Syslog

Geräte

Wählen Sie diese Option aus, um Geräteereignisse an den Syslog-Server zu senden.

- Wenn ein neues Gerät registriert wird, werden zwei Meldungen für dieses Ereignis empfangen: Registrierung und Systemsicherheit.

  Beispielmeldung für ein Geräteregistrierungsereignis

- Bei Entfernung eines Geräts.

  Beispielmeldung für ein Geräteentfernungsereignis

- Wenn sich Richtlinie, Zone, Name oder Protokollierungsebene des Geräts ändern.

  Beispielmeldung für ein Geräteaktualisierungsereignis

Bedrohungen

Wählen Sie diese Option aus, um neu erkannte Bedrohungen oder festgestellte Veränderungen bezüglich einer vorhandenen Bedrohung auf dem Syslog-Server zu protokollieren. Die Änderungen umfassen eine Bedrohung, die *entfernt*, *in Quarantäne* gestellt, *freigegeben* oder *ausgeführt* wird.

Es werden fünf Arten von Bedrohungsereignissen unterschieden:

- **Bedrohung_gefunden**: Eine neue Bedrohung mit dem Status *Unsiche*r wurde gefunden.
- **Bedrohung_entfernt**: Eine vorhandene Bedrohung wurde *entfernt*.
- **Bedrohung_unter_Quarantäne**: Eine neue Bedrohung wurde *in Quarantäne* gefunden.
- **Bedrohung_freigegeben**: Eine neue Bedrohung mit dem Status *Freigegeben* wurde gefunden.
- **Bedrohung_geändert**: Das Verhalten einer vorhandenen Bedrohung hat sich verändert (z. B. Score, Quarantänestatus, Ausführungsstatus).
- **threat_cleared**: Eine Bedrohung, die *freigegeben*, zur *sicheren Liste* hinzugefügt oder aus der *Quarantäne* auf einem Gerät gelöscht wurde.

Beispielmeldung für Bedrohungsereignis

Bedrohungsklassifizierungen
Täglich werden Hunderte von Bedrohungen als Malware oder potenziell unerwünschte Programme (Potentially Unwanted Programs, PUPs) eingestuft. Wenn Sie diese Option auswählen, werden Sie benachrichtigt, wenn derartige Ereignisse eintreten.

Beispielmeldung für Bedrohungsklassifizierung

SIEM (Security Information and Event Management)
Gibt den Typ des Syslog-Servers oder die SIEM-Software an, an den/die Ereignisse gesendet werden sollen.

Protokoll
Dieser Eintrag muss mit der Konfiguration des Syslog-Servers übereinstimmen. Zur Auswahl stehen UDP und TCP. UDP wird im Allgemeinen nicht empfohlen, da die Nachrichtenzustellung nicht garantiert wird. Dell empfiehlt TCP (Standardeinstellung).

TLS/SSL
Steht nur zur Verfügung, wenn als Protokoll TCP ausgewählt wurde. Mit TLS/SSL wird sichergestellt, dass die Syslog-Meldung während der Übertragung von Threat Defense an den Syslog-Server verschlüsselt wird. Dell empfiehlt seinen Kunden, diese Option auszuwählen. Stellen Sie sicher, dass der Syslog-Server für die Überwachung der TLS/SSL-Meldungen konfiguriert ist.

IP/Domäne
Gibt die IP-Adresse oder den vollständig qualifizierten Domänennamen des Syslog-Servers an, den der Kunde eingerichtet hat. Überprüfen Sie gemeinsam mit Ihren internen Netzwerkexperten, ob Firewall- und Domäneneinstellungen richtig konfiguriert sind.

Port
Gibt die Portnummer auf den Geräten an, die der Syslog-Server auf Nachrichten überwacht. Der Port muss eine Zahl im Bereich 1 bis 65535 sein. Typische Werte: 512 für UDP, 1235 oder 1468 für TCP und 6514 für sicheres TCP (Beispiel: TCP mit aktiviertem TLS/SSL).

Schweregrad
Gibt den Schweregrad der Meldungen an, die auf dem Syslog-Server angezeigt werden sollen. Dieses Feld kann subjektiv belegt werden. Geben Sie einen beliebigen Schweregrad ein. Der Wert, der für den Schweregrad angegeben wird, hat keinen Einfluss darauf, welche Meldungen an Syslog weitergeleitet werden.

Fazilität
Gibt an, welche Art von Anwendung die Meldung protokolliert. Die Standardeinstellung ist „Intern“ (oder Syslog). Dieser Wert dient der Kategorisierung der Meldungen, wenn sie vom Syslog-Server empfangen werden.

Testen der Verbindung
Klicken Sie auf die **Testverbindung**, um die IP/Domäne, den Port und die Protokolleinstellungen zu testen. Wenn gültige Werte eingegeben wurden, wird nach einiger Zeit eine *Bestätigungsmeldung* angezeigt.

Benutzerdefinierte Authentifizierung

Melden Sie sich über einen externen Identitätsanbieter (Identity Provider, IdP) an der Konsole an. Dies erfordert die Konfiguration von Einstellungen mit Ihrem IdP, um ein X.509-Zertifikat und eine URL für die Überprüfung Ihrer IdP-Anmeldung zu erhalten. Die benutzerdefinierte Authentifizierung funktioniert mit Microsoft SAML 2.0. Die Verwendbarkeit der Funktion mit OneLogin, OKTA, Microsoft Azure und PingOne wurde bestätigt. Die Funktion beinhaltet auch eine benutzerdefinierte Einstellung und ist normalerweise mit anderen Identitätsanbietern kompatibel, die Microsoft SAML 2.0 verwenden.

Hinweis: Die benutzerdefinierte Authentifizierung bietet keine Unterstützung für Active Directory Federation Services (ADFS).

- **Starke Authentifizierung**: Bietet Zugriff mit mehrstufiger Authentifizierung.
- **Einmaliges Anmelden**: Bietet Zugriff mit einmaliger Anmeldung (Single Sign-On, SSO).

  Hinweis: Die Auswahl von „Starke Authentifizierung“ oder „Single Sign-On“ hat keinen Einfluss auf die Einstellungen für die benutzerdefinierte Authentifizierung, da sämtliche Konfigurationseinstellungen vom Identitätsanbieter (IdP) gehandhabt werden.
- **Kennwortanmeldung zulassen**: Wählen Sie diese Option aus, um die direkte Anmeldung an der Konsole über SSO zuzulassen. Dies ermöglicht SSO-Einstellungstests ohne Aussperrung von der Konsole. Dell empfiehlt, diese Funktion nach der erfolgreichen Anmeldung an der Konsole über SSO zu deaktivieren.
- **Anbieter:** Wählen Sie den Dienstanbieter für die benutzerdefinierte Authentifizierung aus.
- **X. 509-Zertifikat**: Geben Sie die X.509-Zertifikatinformationen ein.
- **Anmelde-URL**: Geben Sie die URL für die benutzerdefinierte Authentifizierung ein.

Bedrohungsdatenbericht

Der Bericht besteht aus einer Kalkulationstabelle, die folgende Informationen zur Organisation enthält:

- **Bedrohungen**: Führt alle Bedrohungen auf, die in der Organisation erkannt wurden. Diese Informationen umfassen Dateiname und Datei-Status (*Unsicher*, *Abnormal*, *Freigegeben* und *in Quarantäne*).
- **Geräte**: Führt alle Geräte der Organisation auf, auf denen Threat Defense Agent installiert ist. Ebenfalls aufgeführt werden Gerätename, Betriebssystemversion, Agentenversion und angewendete Richtlinie.
- **Bedrohungsindikatoren**: Führt die einzelnen Bedrohungen und die zugehörigen Bedrohungseigenschaften auf.
- **Gelöscht**: Listet alle Dateien auf, die in der Organisation *gelöscht* wurden. Zu diesen Informationen gehören Dateien mit dem Status *Freigegeben*, Dateien, die zur *sicheren Liste* hinzugefügt wurden und Dateien, die aus dem Ordner *Quarantäne* auf einem Gerät *gelöscht* wurden.
- **Ereignisse**: Führt alle Ereignisse der letzten 30 Tage auf, die einen Bezug zum Bedrohungsereignisdiagramm im Dashboard haben. Ebenfalls angezeigt werden Datei-Hash, Gerätename, Dateipfad und das Datum, an dem das Ereignis stattgefunden hat.

Wenn diese Funktion aktiviert ist, wird der Bericht automatisch um 01:00 Uhr PST-Zeit (Pacific Standard Time) aktualisiert. Klicken Sie auf **Bericht neu generieren** zur manuellen Generierung einer Aktualisierung.

Der Bedrohungsdatenbericht enthält eine URL und ein Token, mit deren Hilfe der Bericht ohne Anmeldung an der Konsole heruntergeladen werden kann. Das Token kann bei Bedarf auch gelöscht oder neu generiert werden. Auf diese Weise kann gesteuert werden, wer Zugriff auf den Bericht hat.

FEHLERBEHEBUNG

In diesem Abschnitt ist eine Liste mit Fragen und Dateien enthalten, die bei der Behebung von Fehlern in Verbindung mit Threat Defense beantwortet bzw. erfasst werden müssen. Mithilfe dieser Informationen kann Dell Support die Problemlösung unterstützen.

Der Abschnitt enthält außerdem eine Beschreibung allgemeiner Probleme und die hierfür vorgeschlagenen Lösungen.

Support

Installationsparameter

- Mit welcher Methode wurde das Produkt installiert? Geben Sie die verwendeten Parameter an.
    - Beispiel für Windows: Verwenden Sie bei der Installation über die Befehlszeile den Parameter LAUNCHAPP=0, um das Agentensymbol und den Startmenüordner während der Laufzeit auszublenden.
    - Beispiel für Mac OS X: Verwenden Sie bei der Installation über die Befehlszeile den Parameter SelfProtectionLevel=1, um den Selbstschutz auf dem Agenten zu deaktivieren.
- Welche Installationsschritte konnten überprüft werden?
    - Beispiel für Windows: Wurde das MSI- oder das EXE-Installationsprogramm verwendet?
    - Beispiel für beliebiges Betriebssystem: Wurden Befehlszeilenoptionen verwendet? Z. B. Stiller Modus oder Benutzeroberfläche ohne Agentensymbol.
- Aktivieren Sie für die Installation die ausführliche Protokollierung.

Leistungsaspekte

- Erstellen Sie einen Screenshot des Task-Managers (Windows) oder der Aktivitätsanzeige (Mac OS X), aus dem die Threat Defense-Prozesse und die Speicherauslastung hervorgehen.
- Erstellen Sie eine Sicherungskopie des Threat Defense-Prozesses.
- Erfassen Sie Debugging-Protokolle.
- Erfassen Sie während des Problems die Ausgabe der Systeminformationen.
    - Bei Windows: msinfo32 oder winmsd
    - Bei Mac OS X: Systeminformationen
- Erfassen Sie relevante Ereignisprotokolle (Windows) bzw. Konsoleninformationen (Mac OS X).

Probleme in Verbindung mit Aktualisierungen, Status und Konnektivität

- Stellen Sie sicher, dass Port 443 auf der Firewall geöffnet ist und das Gerät die Website Cylance.com auflösen und eine Verbindung zu ihr herstellen kann.
- Wird das Gerät auf der Seite „Geräte“ der Konsole angezeigt? Ist es online oder offline? Wann war es zuletzt verbunden?
- Verwendet das Gerät für die Verbindung mit dem Internet einen Proxy-Server? Sind die Anmeldeinformationen auf dem Proxy-Server richtig konfiguriert?
- Starten Sie den Threat Defense-Dienst neu, damit er versucht, eine Verbindung zur Konsole herzustellen.
- Erfassen Sie Debugging-Protokolle.

- Erfassen Sie während des Problems die Ausgabe der Systeminformationen.
    - Bei Windows: msinfo32 oder winmsd
    - Bei Mac OS X: Systeminformationen

Aktivieren der Debugging-Protokollierung

Standardmäßig speichert Threat Defense Protokolldateien unter **`C:\Programme\Cylance\Desktop\log`**. Zur Fehlerbehebung kann Threat Defense für die Generierung ausführlicherer Protokolle konfiguriert werden.

Inkompatibilitäten bei der Skriptsteuerung

Problem:

Wenn die Skriptsteuerung auf bestimmten Geräten aktiviert ist, kann dies zu Konflikten mit anderen Softwareprogrammen führen, die ebenfalls auf diesen Geräten ausgeführt werden. Diese Konflikte werden in der Regel dadurch verursacht, dass der Agent in bestimmte Prozesse eingreift, auf die eine andere Software zugreift.

Lösung:

Je nach Software kann dieses Problem behoben werden, indem bestimmte Prozessausschlüsse zur Geräterichtlinie auf der Konsole hinzugefügt werden. Eine weitere Möglichkeit ist die Aktivierung des Kompatibilitätsmodus (Registrierungsschlüssel) auf den betroffenen Geräten. Falls die Ausschlüsse keine Wirkung haben, empfiehlt Dell jedoch, die Skriptsteuerung in der Geräterichtlinie zu deaktivieren, die sich auf die Geräte auswirkt, um die normale Gerätefunktionalität wiederherzustellen.

Hinweis: Diese Kompatibilitätsmodus-Lösung ist für Agent Version 1370. Beginnend mit Agent 1382 und höher wurde der Injektionsvorgang zum Zweck der Kompatibilität mit anderen Produkten aktualisiert.

Kompatibilitätsmodus

Fügen Sie den folgenden Registrierungsschlüssel hinzu, um den Kompatibilitätsmodus zu aktivieren:

1. Wechseln Sie mithilfe des Registrierungs-Editors zu **`HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop`**.
2. Klicken Sie mit der rechten Maustaste auf **Desktop**, klicken Sie auf **Berechtigungen**, übernehmen Sie dann den Besitz und gewähren Sie **Vollzugriff**. Klicken Sie auf **OK**.
3. Klicken Sie mit der rechten Maustaste auf **Desktop**, wählen Sie dann **Neu** > **Binärwert** aus.
4. Geben Sie der Datei den Namen **CompatibilityMode**.
5. Öffnen Sie die Einstellung der Registrierungsdatei und ändern Sie den Wert in **01**.
6. Klicken Sie auf **OK**, und schließen Sie dann den Registrierungs-Editor.
7. Möglicherweise muss der Dienst neu gestartet werden.

Befehlszeilenoptionen

Bei Verwendung von Psexec:

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

Um einen Befehl für mehrere Geräte auszugeben, verwenden Sie das **Invoke-Command-cmdlet**:

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

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

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

ANHANG A: GLOSSAR

Abnormal	Eine verdächtige Datei mit einem niedrigeren Score (1 bis 59), bei der es sich weniger wahrscheinlich um Malware handelt.
Administrator	Mandantenmanager für Threat Defense.
Agent	Threat Defense-Endpunkthost, der mit der Konsole kommuniziert.
Überprüfungsprotokoll	Protokoll, das Maßnahmen erfasst, die auf der Threat Defense Console durchgeführt wurden.
Automatische Quarantäne	Automatische Verhinderung der Ausführung aller als *Unsicher* und/oder *Abnormal* klassifizierten Dateien
Automatisch hochladen	Automatischer Upload aller unbekannten PE-Dateien (Portable Executable), die als *unsicher* oder *abnormal* erkannt wurden, in die Cylance Infinity Cloud zur Analyse.
Konsolen-Benutzerhandbuch	Die Threat Defense Management-Benutzeroberfläche.
Geräterichtlinie	Threat Defense-Richtlinie, die vom Administrator der Organisation konfiguriert werden kann, und die festlegt, wie Bedrohungen auf den Geräten zu behandeln sind.
Globale Quarantäne	Verhindert die Ausführung einer Datei auf globaler Ebene (auf allen Geräten der Organisation).
Globale sichere Liste	Lässt die Ausführung einer Datei auf globaler Ebene zu (auf allen Geräten der Organisation).
Infinity	Mathematisches Modell zur Bewertung von Dateien.
Organisation	Ein Mandantenkonto, das den Threat Defense-Dienst verwendet.
Quarantäne	Verhindert die Ausführung einer Datei auf lokaler Ebene (auf einem bestimmten Gerät).
Bedrohungen	Potenziell bösartige Dateien, die von Threat Defense erkannt und als *Unsicher* oder *Abnormal* klassifiziert wurden
Unsicher	Eine verdächtige Datei mit einem hohen Score (60 bis 100), bei der es sich wahrscheinlich um Malware handelt.
Freigeben	Lässt die Ausführung einer Datei auf lokaler Ebene zu (auf einem bestimmten Gerät).
Zone	Möglichkeit der Strukturierung und Gruppierung von Geräten innerhalb einer Organisation nach Priorität, Funktionalität usw.
Zonenregel	Funktion, die eine automatisierte Zuweisung von Dateien zu einer Zone, basierend auf IP-Adresse, Betriebssystem und Gerätename ermöglicht.

ANHANG B: HANDHABEN VON AUSNAHMEN

In bestimmten Situationen müssen Benutzer eine Datei manuell in *Quarantäne* verschieben oder *zulassen* (*freigeben*). Threat Defense bietet Möglichkeiten zur Behandlung von Ausnahmen für jedes Gerät (*lokal*), für eine Gruppe von Geräten (*Richtlinie*),oder für die gesamte Organisation (*global*).

Dateien

Lokal: *Quarantäne* oder *Freigabe* (auf die *sichere Liste setzen*) einer Datei auf dem Gerät. Nützlich, um eine Datei vorübergehend zu *blockieren* oder *zuzulassen*, bis es Zeit ist, sie zu analysieren. Die *Freigabe* einer Datei auf einem Gerät ist auch nützlich, wenn das Gerät das einzige Gerät ist, auf dem das *Ausführen* dieser Datei zulässig ist. Dell empfiehlt die Verwendung von *Richtlinie* oder *Global*, wenn diese Aktion auf mehreren Geräten durchgeführt werden muss.

Richtlinie: Setzen einer Datei auf die *sichere Liste*, auf allen Geräten, die einer Richtlinie zugewiesen sind. Dies bietet sich an, um eine Datei oder eine Gerätegruppe zuzulassen (z. B. Ausführung von Tools auf IT-Geräten zulassen, die für bösartige Zwecke verwendet werden könnten, wie PsExec). Das Stellen einer Datei unter *Quarantäne* auf der Richtlinienebene ist nicht verfügbar.

Global: *Quarantäne* oder *Freigabe* (auf die sichere *Liste setzen* einer Datei für die Organisation. *Quarantäne* einer bekannten bösartige Datei in der Organisation. Setzen einer Datei, die nachweislich gutartig ist und in der Organisation verwendet wird, aber der Agent als schädlich klassifiziert hat, auf die *sichere Liste*.

Skripte

Richtlinie: Die Skriptsteuerung ermöglicht die Genehmigung von Skripten zur Ausführung in einem bestimmten Ordner. Wird ein Skript für die Ausführung in einem Ordner genehmigt, werden auch die Skripte in den Unterordnern genehmigt.

Zertifikate

Global: Fügen Sie Zertifikate zur Konsole und anschließend zur *globalen sicheren Liste* hinzu. Dadurch können Anwendungen, die von diesem Zertifikat signiert sind, in der Organisation ausgeführt werden.

Um ein Zertifikat hinzuzufügen, wählen Sie **Einstellungen > Zertifikate** aus, und klicken anschließend auf **Zertifikat Hinzufügen**.

Zum Hinzufügen des Zertifikats zur *globalen sicheren Liste* wählen Sie **Einstellungen > Globale Liste**, dann die Registerkarte **Sicher** und die Registerkarte **Zertifikate** aus und klicken anschließend auf **Zertifikat hinzufügen**.

ANHANG C: BENUTZERBERECHTIGUNGEN

Welche Maßnahmen ein Benutzer durchführen kann, ist davon abhängig, welche Berechtigung (Rolle) ihm zugewiesen wurde. Im Allgemeinen können Administratoren Maßnahmen in der gesamten Organisation durchführen. Zonenmanager und Benutzer sind auf die ihnen zugewiesene Zone beschränkt. Dies bedeutet, dass nur auf die in der Zone enthaltenen Geräte zugegriffen und nur die Bedrohungsdaten zu diesen Geräten angezeigt werden können. Wenn ein Zonenmanager oder Benutzer ein Gerät oder eine Bedrohung nicht anzeigen kann, gehört das Gerät sehr wahrscheinlich nicht der Zone an, der der Zonenmanager oder Benutzer zugewiesen ist.

	BENUTZER	ZONENMANAGER	ADMIN
Agentenaktualisierung			
Anzeigen/bearbeiten			x
Überprüfungsprotokollierung			
Anzeigen			x
Geräte			
Geräte hinzufügen – global			x
Geräte einer Zone hinzufügen			x
Geräte entfernen – global			x
Geräte aus einer Zone entfernen		x	x
Gerätename bearbeiten		x	x
Zonen			
Zone erstellen			x
Zone löschen			x
Zonennamen bearbeiten – alle			x
Name der zugewiesenen Zone bearbeiten		x	x
Richtlinien			
Richtlinie erstellen – global			x
Richtlinie für eine Zone erstellen			x
Richtlinie hinzufügen – global			x
Richtlinie einer Zone hinzufügen		x	x
Richtlinie entfernen – global			x
Richtlinie aus einer Zone entfernen		x	x
Bedrohungen			
Dateien in Quarantäne verschieben – global			x
Dateien innerhalb einer Zone in Quarantäne verschieben	x	x	x
Dateien freigeben – global			x
Dateien innerhalb einer Zone freigeben	x	x	x
Globale Quarantäne/globale sichere Liste			x
Einstellungen			
Installationstoken generieren oder löschen			x
Anmelde-URL generieren oder löschen			x
Installationstoken kopieren	x	x	x
Anmelde-URL kopieren			x

	BENUTZER	ZONENMANAGER	ADMIN
Benutzerverwaltung			
Benutzer einer beliebigen Zone zuweisen			X
Benutzer einer verwalteten Zone zuweisen		X	X
Zonenmanager zuweisen – global			X
Zonenmanager einer verwalteten Zone zuweisen		X	X
Benutzer aus Konsole löschen			X
Benutzer aus Konsole entfernen – global			X
Benutzer aus einer verwalteten Zone entfernen		X	X

ANHANG D: DATEIBASIERTER SCHREIBFILTER

Der Dell Threat Defense Agent kann auf einem System installiert werden, auf dem Windows Embedded Standard 7 (Thin Client) ausgeführt wird. Auf integrierten Geräten ist das Schreiben in den Systemspeicher möglicherweise nicht zulässig. In diesem Fall verwendet das System möglicherweise einen dateibasierten Schreibfilter (FBWF), um Schreibvorgänge im Systemspeicher in den Cache der Systemarbeitsspeicher umzuleiten. Das kann zu Problemen mit dem Agenten und folglich zu Verlusten von Änderungen bei jedem System-Neustart führen.

Bei der Verwendung des Agenten auf einem integrierten System verwenden Sie das folgende Verfahren:

1. Deaktivieren Sie den FBWF vor der Installation des Agenten mithilfe des folgenden Befehls: `fbwfmgr/disable`.
2. Starten Sie das System neu. Dadurch wird die Deaktivierung des FBWF wirksam.
3. Installieren Sie den Dell Threat Defense Agent.
4. Nach der Installation des Agenten, reaktivieren Sie den FBWF mithilfe des folgenden Befehls: `fbwfmgr/enable`.
5. Starten Sie das System neu. Dadurch wird die Aktivierung des FBWF wirksam.
6. Schließen Sie im FBWF die folgenden Ordner aus:
    a. C:\Programme\Cylance\Desktop – Durch das Ausschließen dieses Ordners können Agentenaktualisierungen nach einem Systemneustart weiter bestehen.
7. Verwenden Sie den folgenden Befehl, um den Desktop-Ordner auszuschließen: `fbwfmgr/addexclusion C: "\Programme\Cylance\Desktop\"`
    a. Dies setzt voraus, dass Sie die Installation im Standardverzeichnis durchführen. Ändern Sie den Ausschluss in den Ordner, in dem Sie den Agenten installiert haben.
8. Wenn Sie planen, Bedrohungen zu Testzwecken mit dem Agenten auf dem Rechner zu speichern, achten Sie darauf, den Speicherort des FBWF ebenfalls auszuschließen (z. B. `C:\Samples`).

ANHANG E: KENNTNIS BASIS ARTIKEL

Weitere Informationen finden Sie in diesen Knowledge Base-Artikeln:

Freigabemitteilungen nach Version:

http://www.dell.com/support/article/de/de/19/SLN305419/?lang=DE

Allgemeines Wissen und Verwaltung:

http://www.dell.com/support/article/de/de/19/SLN302194/?lang=DE

Allgemeine Systemanforderungen:

http://www.dell.com/support/article/de/de/19/SLN301914/?lang=DE

Ausschlüsse, die für andere Anti-Viren benötigt werden können:

http://www.dell.com/support/article/de/de/19/SLN301134/?lang=DE

Data Security Gemeinschaftsforen:

http://en.community.dell.com/techcenter/security/datasecurity/f