Konfigurieren und Identifizieren von Cisco Secure Endpoint-Ausschlüssen

Inhalt

Einleitung

In diesem Dokument werden die Best Practices zum Auffinden und Erstellen von Ausschlüssen für den sicheren Endpunkt beschrieben.

Beiträge von Cisco Technikern.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Zugriff auf die Konsole für sichere Endgeräte
- Konto mit Administratorrechten

- Kenntnisse der Kundenumgebung.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den Betriebssystemen Windows, Linux und MacOS.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Ausschlüsse verstehen

Ein Ausschlusssatz ist eine Liste von Verzeichnissen, Dateierweiterungen oder Namen von Bedrohungen, die Secure Endpoint Connector nicht scannen oder überführen soll. Ausschlüsse sind notwendig, um ein ausgewogenes Verhältnis von Leistung und Sicherheit auf einem System sicherzustellen, wenn Endpunktschutz wie Secure Endpoint aktiviert ist. In diesem Artikel werden die Ausnahmen für Secure Endpoint Cloud, TETRA, SPP und MAP beschrieben.

Jede Umgebung ist einzigartig und auch die sie kontrollierende Einheit, die von strengen bis hin zu offenen Richtlinien reicht, wobei letztere als Honeypot klassifiziert würden. Da solche Ausschlüsse definiert werden, müssen sie auf jede Situation individuell zugeschnitten sein.

Verschiedene Ausschlüsse lassen sich auf zwei Arten kategorisieren**: offensichtliche Ausschlüsse** und **unbestimmte Ausschlüsse**.

Eindeutige Ausnahmen

Offensichtliche Ausschlüsse sind Ausschlüsse, die auf der Grundlage von Recherchen und Tests für häufig verwendete Betriebssysteme, Programme und andere Sicherheitssoftware erstellt wurden. Diese Ausschlüsse finden Sie in der von Cisco verwalteten Ausschlussliste in Ihrer Konsole.

> **Hinweis**: Es wird empfohlen, sich an andere Anti-Virus-Anbieter zu wenden und deren empfohlene Ausschlüsse hinzuzufügen. Dadurch wird sichergestellt, dass Secure Endpoint und AV zusammen funktionieren und die Auswirkungen auf die Leistung minimieren.

Uneindeutige Ausschlüsse

Es wird empfohlen, eine doppelte Richtlinie zu erstellen, um Sicherheitsbedenken und Störungen im Geschäftsbetrieb zu vermeiden, Computer mit Indikatoren für Leistungsprobleme zu identifizieren und sie in eine Gruppe zu unterteilen, um diese doppelte Richtlinie zu verwenden.

> **Achtung**: Konfigurationsänderungen auf dem Dashboard erfordern Zeit, damit Connectors die Richtlinie synchronisieren können. Warten Sie ein Heartbeat-Update ab, oder synchronisieren Sie die Richtlinien auf den Connectors manuell.

Richtlinienerstellung

1. **Konsole für sichere Endgeräte > Registerkarte "Verwaltung" > Richtlinien**
2. Klicken Sie auf **+ Neue Richtlinie...**
3. **Wählen Sie** das Betriebssystem aus dem Dropdown-Menü aus.
4. Geben Sie ihm einen aussagekräftigen Namen, damit Sie diese Richtlinie und Beschreibung unterscheiden können (*optional*).
5. Wählen Sie die Richtlinienaktionen für Ihre Anforderungen aus, und verwenden Sie jetzt die Standardausschlüsse.
6. ***Wichtig*** Legen Sie unter **Erweiterte Einstellungen > Verwaltungsfunktionen** die Ebene des Connector-Protokolls auf **Debuggen fest**.
7. Klicken Sie auf **Speichern**, um die Richtlinienerstellung abzuschließen.

Gruppenerstellung

1. **Konsole für sichere Endgeräte > Registerkarte "Verwaltung" > Gruppen**
2. Klicken Sie auf **Gruppe erstellen.**
3. Geben Sie ihm einen aussagekräftigen Namen, damit Sie diese Gruppe und Beschreibung unterscheiden können (*optional*).
4. **Wählen Sie** die doppelte Richtlinie aus, die Sie erstellt haben.
5. Klicken Sie auf **Speichern**, um die Gruppenerstellung abzuschließen.

So identifizieren Sie Ausschlüsse

Nach dem Erstellen doppelter Richtlinien und Gruppen führen die *Computer* mit der **Debugging-Protokollebene auf den Connectors** wie bei normalen Geschäftsvorgängen aus. Lassen Sie genügend Zeit, um ausreichende Connector-Protokolldaten zu erhalten, während auf Programme und Prozesse zugegriffen wurde. Erstellen Sie ein Support-Diagnosepaket, um Ausschlüsse zu überprüfen und zu identifizieren.

Leitfaden zur Erstellung von Diagnosepaketen für verschiedene verfügbare Betriebssysteme:

- Windows
- Linux
- MAC

MacOS oder Linux

Extrahieren Sie das komprimierte Diagnosepaket. Die Datei **fileops.txt** listet die Pfade auf, über die Dateien Aktivitäten erstellen, ändern und umbenennen, die Secure Endpoint zur Durchführung von Dateiscans ausgelöst haben. Jedem Pfad ist eine Anzahl zugeordnet, die angibt, wie oft er gescannt wurde, und die Liste wird in absteigender Reihenfolge sortiert. Während eine hohe Anzahl nicht unbedingt bedeutet, dass der Pfad ausgeschlossen werden muss (z. B. kann ein Verzeichnis, in dem E-Mails gespeichert sind, häufig gescannt werden, darf jedoch nicht ausgeschlossen werden), bietet die Liste einen Ausgangspunkt zur Identifizierung von Ausschlusskandidaten.

```
31 /Users/eugene/Library/Cookies/Cookies.binarycookies
24 /Users/eugene/.zhistory
9 /Users/eugene/.vim/.temp/viminfo
9 /Library/Application Support/Apple/ParentalControls/Users/eugene/2018/05/10-usage.data
5 /Users/eugene/Library/Cookies/HSTS.plist
5 /Users/eugene/.vim/.temp/viminfo.tmp
4 /Users/eugene/Library/Metadata/CoreSpotlight/index.spotlightV3/tmp.spotlight.state
```

```
 3 /Users/eugene/Library/WebKit/com.apple.Safari/WebsiteData/ResourceLoadStatistics/full_browsir
 3 /Library/Logs/Cisco/supporttool.log
 2 /private/var/db/locationd/clients.plist
 2 /Users/eugene/Desktop/.DS_Store
 2 /Users/eugene/.dropbox/instance1/config.dbx
 2 /Users/eugene/.DS_Store
 2 /Library/Catacomb/DD94912/biolockout.cat
 2 /.fseventsd/000000000029d66b
 1 /private/var/db/locationd/.dat.nosync0063.arg4tq
```

Windows

Das Windows-Betriebssystem ist komplizierter, da aufgrund des übergeordneten und des untergeordneten Prozesses mehr Ausschlussoptionen verfügbar sind. Dies deutet darauf hin, dass eine eingehendere Überprüfung erforderlich ist, um die Dateien zu identifizieren, auf die zugegriffen wurde, aber auch die Programme, die sie generiert haben. Weitere Informationen zur Analyse und Optimierung der Windows-Leistung mit Secure Endpoint finden Sie in diesem Windows Tuning Tool von der Cisco Security-Seite GitHub.

Erstellen von Ausschlüssen

In diesem Abschnitt werden die Best Practices für das Schreiben von Ausschlüssen für Ihre Umgebung beschrieben.

> **Vorsicht**: Verstehen Sie stets die Dateien und Prozesse, bevor Sie einen Ausschluss schreiben, um Sicherheitslücken am Computer zu vermeiden.

> **Hinweis**: Weitere Details finden Sie im Benutzerhandbuch, Kapitel 3 hier durchgehen. In diesem Kapitel werden die Arten der Ausnahmen, die Implementierung und die Navigation des Secure Endpoint-Portals beschrieben.

CSIDL-Pfad und -Prozess

CSIDL ist eine akzeptierte und ermutigte Methode, Ausschlüsse zu schreiben. CSIDL ermöglicht Prozessausschlüsse, die in Umgebungen bestätigt werden können, in denen alternative Laufwerkbuchstaben verwendet werden, und kann die Notwendigkeit von Platzhaltern umgehen, wenn dieser Pfad benutzerspezifisch ist (da Prozessausschlüsse keinen Platzhalter zulassen). Weitere Informationen zu CSIDL . Bei der Verwendung von CSIDL müssen jedoch gewisse Einschränkungen beachtet werden. Wenn Ihre Umgebung Programme auf mehr als einem Laufwerkbuchstaben installiert, bezieht sich der CSIDL-Pfad nur auf das Laufwerk, das als Standard-Installationsort markiert ist. Wenn z. B. das Betriebssystem auf C:\ installiert ist, der Installationspfad für Microsoft SQL jedoch manuell zu D:\ geändert wurde, gilt der CSIDL-basierte Ausschluss in der Liste der verwalteten Ausschlüsse nicht für diesen Pfad. Für Prozessausschlüsse bedeutet dies, dass für jeden Prozess, der sich nicht auf dem Laufwerk C:\ befindet, ein Ausschluss eingegeben werden muss, da CSIDL diesen Prozess nicht zuordnet.

Pfadausschlüsse

Diese Ausschlüsse werden am häufigsten verwendet. Anwendungskonflikte führen in der Regel zum Ausschluss eines Verzeichnisses. Erstellen Sie einen Pfadausschluss mithilfe eines absoluten Pfads oder der CSIDL.

Um beispielsweise eine Antivirenanwendung aus dem Verzeichnis "Programme" auszuschließen, würde der Ausschlusspfad wie folgt lauten:

```
C:\Program Files\MyAntivirusAppDirectory
CSIDL_PROGRAM_FILES\MyAntivirusAppDirectory
```

Ohne einen Schrägstrich stimmt **Windows Connector** auf Pfaden teilweise überein, **Mac und Linux hingegen nicht.**

Beispiel: Wenn Sie die folgenden Pfadausschlüsse "**C:\Program Files"** und "**C:\test" anwenden:**

C:\Program Dateien und **C:\Program Dateien (x86**) sind ausgeschlossen:

<#root>

C:\Program Files

C:\Program Files (x86)

C:\test ist ausgeschlossen, da **C:\test123**:

<#root>

C:\test

C:\test123

Sie können den Ausschluss von "**C:\test"** in "**C:\test\"** ändern, dadurch wird "**C:\test123"** nicht ausgeschlossen.

Hinweis: Pfadausschlüsse sind rekursiv und schließen auch alle Unterverzeichnisse aus.

Dateierweiterung

Diese Ausschlüsse erlauben den Ausschluss aller Dateien mit einer bestimmten Erweiterung.

Wichtigste Punkte:

- Auf der Anschlussseite wird .**extension** erwartet**.**
- Das Dashboard gibt der Dateierweiterung automatisch einen Punkt vor, wenn keine Dateierweiterung hinzugefügt wurde.
- Bei Erweiterungen wird ***nicht*** zwischen Groß- und Kleinschreibung unterschieden.

Um beispielsweise alle Microsoft Access-Datenbankdateien auszuschließen, können Sie den folgenden Ausschluss erstellen:

```
.MDB
```

> **Hinweis**: In der Standardliste stehen Standard-Ausschlüsse zur Verfügung. Es wird **nicht** empfohlen, diese Ausschlüsse zu löschen. Dies kann zu Leistungsänderungen auf Ihren *Computern* führen.

Platzhalter

Diese Ausschlüsse entsprechen denen von Pfad- oder Erweiterungsausschlüssen, mit der Ausnahme, dass ein Sternchen (*) als Platzhalter verwendet wird.

> **Achtung**: Der Platzhalterausschluss endet nicht bei Pfadtrennern, dies kann zu unbeabsichtigten Ausschlüssen führen. Beispiel: **C:*\test** schließt **C:\sample\test** sowie **C:\1\test** oder **C:\sample\test123 aus.**

> **Warnung**: Das Beginnen eines Ausschlusses mit einem Sternchen (*) kann zu schwerwiegenden Leistungsproblemen führen. Bei **7.5.3+** führte die Hinzufügung von Wildcard Process Exclusions zu zusätzlichen Leistungsproblemen bei den mit Sternchen führenden Ausschlüssen. Entfernen oder ändern Sie alle Ausschlüsse in diesem Format, um die Auswirkungen auf die CPU zu minimieren.

Schließen Sie beispielsweise virtuelle Systeme auf einer MAC-Adresse vom Scannen aus. Geben Sie den folgenden Pfadausschluss ein:

```
/Users/johndoe/Documents/Virtual Machines/
```

Dieser Ausschluss funktioniert nur für *johndoe*, um mehrere Benutzer-Übereinstimmungen zu erlauben, ersetzen Sie den Benutzernamen im Pfad durch ein Sternchen (*) in einen Platzhalter-Ausschluss:

```
/Users/*/Documents/Virtual Machines/
```

Schreiben Sie einen Ausschluss für Pfade, die auf separaten Laufwerken vorhanden sind.

Beispiel: **C:\testpath** und **D:\testpath** sind:

```
^[A-Za-z]\testpath
```

Das System generiert automatisch ^[A-Za-z], wenn "Auf alle Laufwerkbuchstaben anwenden" aktiviert ist, nachdem der Platzhalter aus dem Dropdown-Menü Ausschlusstyp ausgewählt wurde, wie im Bild gezeigt:

Prozess

Mit Prozessausschlüssen können Administratoren laufende Prozesse von normalen Dateiprüfungen (Secure Endpoint Windows Connector Version 5.1.1 und höher), Systemprozessschutz (Connector Version 6.0.5 und höher) oder Schutz vor schädlichen Aktivitäten (Connector Version 6.1.5 und höher) ausschließen.

Der Prozessausschluss erfolgt entweder durch Angabe des vollständigen Pfads zur ausführbaren Prozessdatei, des SHA-256-Werts der ausführbaren Prozessdatei oder sowohl des Pfads als auch des SHA-256. Pfade ermöglichen sowohl direkte Pfade als auch die Verwendung eines CSIDL-Werts.

> **Achtung**: Von einem ausgeschlossenen Prozess erstellte untergeordnete Prozesse werden standardmäßig **nicht** in den Ausschluss einbezogen. Beispiel: Prozessausschluss für MS Word würde nicht standardmäßig alle zusätzlichen Prozesse, die von Word.exe erstellt werden, ausschließen und würde gescannt werden. Wenn Sie weitere Prozesse hinzufügen möchten, klicken Sie auf das Kontrollkästchen **Für untergeordnete Prozesse anwenden**. Darüber hinaus, ausgenommen Word.exe wird nicht empfohlen, da Malware regelmäßig versteckt in modernen .docx-Dateien.

> **Hinweis**: Die Angabe von Path und SHA-256 ist erforderlich, damit der Prozess ausgeschlossen werden kann.

Einschränkungen:

- Wenn die Dateigröße des Prozesses größer ist als die in der Richtlinie festgelegte maximale Größe der Scandatei, wird der SHA-256 des Prozesses nicht berechnet, und der Ausschluss **funktioniert nicht**. Einen pfadbasierten Prozessausschluss für Dateien verwenden, die größer als die maximale Größe der Scandatei sind
- Connector-Versionen 5.x.x bis 6.0.3 - 25 Prozessausschlüsse für alle Prozessausschlusstypen
- Connector-Versionen 6.0.5+ - max. 100 Prozessausschlüsse für alle Prozessausschlusstypen
- Connector-Versionen 7.x+ - max. 500 Prozessausschlüsse für alle Prozessausschlusstypen.
- Der Connector berücksichtigt nur die Prozessausschlüsse bis zum Limit, vom Anfang der Liste der Prozessausschlüsse in policy.xml
- Jede Richtlinie enthält einen Prozessausschluss für sfc.exe, der auf das Limit angerechnet wird.

```
3|0||CSIDL_Secure Endpoint_VERSION\sfc.exe|48|
```

Bedrohung

Mit diesen Ausschlüssen kann ein bestimmter Bedrohungsname von der Auslösung von Ereignissen ausgeschlossen werden. Der Ausschluss von Bedrohungen sollte nur verwendet werden, wenn das Suchergebnis eine Fehlalarmerkennung auslöst und bestätigt, dass es sich nicht um eine tatsächliche Bedrohung handelt.

Das Textfeld zum Hinzufügen eines Bedrohungsausschlusses unterscheidet ***nicht*** zwischen Groß- und Kleinschreibung. Beispiel: W32.Zombies.NotAVirus oder w32.zombies.notavirus entsprechen beide demselben Bedrohungsnamen.

> **Warnung:** Schließen Sie Bedrohungen nur aus, wenn die Ermittlung und Bestätigung des Bedrohungsnamens als falsch positiv eingestuft wird. Ausgeschlossene Bedrohungen werden nicht mehr zur Überprüfung und Überprüfung auf der Registerkarte "Ereignisse" angezeigt.

Prozess-Platzhalter

Windows

Endpoint 7.5.3+ ermöglicht zusätzliche Ausschlüsse unter Verwendung der Wildcard-Funktion innerhalb der Process-Ausschlüsse. Dies ermöglicht eine breitere Abdeckung mit weniger Ausschlüssen, kann aber auch gefährlich sein, wenn zu viel undefiniert bleibt. **Verwenden Sie den Platzhalter nur, um die Mindestanzahl an Zeichen einzugeben, die für den erforderlichen Ausschluss erforderlich ist.**

Verwendung von (*) in Prozess-Platzhalter für Windows:

- (*) Kann anstelle eines einzelnen Zeichens oder eines vollständigen Verzeichnisses verwendet werden. Es kann nicht am Anfang des Pfades platziert werden, es wird als ungültig eingestuft. Der Platzhalter funktioniert zwischen zwei definierten Zeichen, Schrägstrichen oder alphanumerischen Zeichen. Wenn Sie es am Ende eines Pfads platzieren, werden die Prozesse in diesem Verzeichnis ausgeschlossen, jedoch nicht die Unterverzeichnisse.
- (**) Kann am Ende eines Pfads verwendet werden, um alle Prozesse in diesem Verzeichnis und die Prozesse in den Unterverzeichnissen auszuschließen. Dies ermöglicht einen viel größeren Ausschlusssatz bei minimalem Input, lässt aber auch eine sehr große Sicherheitslücke für die Transparenz. **Verwenden Sie diese Funktion mit äußerster Vorsicht**.

Beispiele:

```
C:\Windows\*\Tiworker.exe - Excludes all Tiworker.exe found in the subfolders of 'Windows'
C:\Windows\P*t.exe - Excludes Pot.exe, Pat.exe, P1t.exe Etc.
C:\Windows\*chickens.exe - Excludes all Processes in 'Windows' folder ending in chickens.exe
C:\* - Excludes all Processes in the C: drive in the top layer of folders but not the subfolders
C:\** - Excludes every Process on the C: drive.
```

MacOS und Linux

Endpoint 1.15.2+ ermöglicht zusätzliche Ausschlüsse unter Verwendung der Wildcard-Funktion innerhalb der Process-Ausschlüsse. Dies ermöglicht eine breitere Abdeckung mit weniger Ausschlüssen, kann aber auch gefährlich sein, wenn zu viel undefiniert bleibt. **Verwenden Sie den Platzhalter nur, um die Mindestanzahl an Zeichen einzugeben, die für den erforderlichen Ausschluss erforderlich ist.**

Verwendung von (*) in Prozess-Platzhalter für Mac:

- (*) Kann anstelle eines einzelnen Zeichens oder eines vollständigen Verzeichnisses verwendet werden. Es kann nicht am Anfang des Pfades platziert werden, es wird als ungültig eingestuft. Der Platzhalter funktioniert zwischen zwei definierten Zeichen, Schrägstrichen oder alphanumerischen Zeichen.

Beispiele:

```
/Library/Java/JavaVirtualMachines/*/java - Excludes Java within all subfolders of JavaVirtualMac
/Library/Jibber/j*bber - Excludes the Process for jabber, jibber, jobber, etc.
```

Ausschluss von Exploit-Schutz (Anwendung)

Windows

Secure Endpoint 7.5.1+ verwendet V5 der Exploit Prevention Engine, und die Konsole ermöglicht jetzt die Konfiguration von Anwendungsausschlüssen innerhalb der aktuellen Ausschlusslisten-Funktionalität. **Dies ist derzeit nur auf Anwendungen beschränkt, und alle Ausschlüsse in Bezug auf DLLs müssen weiterhin durch das Öffnen eines Tickets mit dem Support erfolgen.**

Die Suche nach den richtigen Ausschlüssen für die Exploit-Prävention ist weitaus aufwändiger als jeder andere Ausschlusstyp und erfordert umfangreiche Tests, um schädliche Sicherheitslücken zu minimieren.

Häufige vermeidbare Fehler

Seien Sie vorsichtig, wenn Sie Ausschlüsse erstellen, da dies das von Cisco Secure Endpoint gebotene Schutzniveau verringert. Ausgeschlossene Dateien werden nicht gehasht, gescannt oder sind im Cache oder in der Cloud verfügbar, die Aktivität wird nicht überwacht, und in den Backend-Engines, Device Trajectory und Advanced Analysis fehlen Informationen.

Ausschlüsse sollten *nur* selten in zielgerichteten Instanzen wie Kompatibilitätsproblemen mit bestimmten Anwendungen oder Leistungsproblemen, die sonst nicht verbessert werden können, verwendet werden.

Im Folgenden finden Sie einige häufige Fehler, die Sie vermeiden sollten, wenn Sie mit Ausschlüssen arbeiten.

- **Proaktive Ausschlüsse**
  - Gehen Sie nicht davon aus, dass ein Ausschluss erforderlich ist, es sei denn, es wurde nachgewiesen, dass es sich um ein Problem handelt, das nicht anderweitig behoben werden kann. Leistungsprobleme, Fehlalarme oder Probleme mit der Anwendungskompatibilität sollten gründlich untersucht und behoben werden, bevor ein Ausschluss angewendet wird.

- **Ein zu umfassender Ausschluss**
  - Große Teile des Endpunkts ausgenommen, z. B. das gesamte Laufwerk C
  - Verwenden eines Platzhalterausschlusses, wenn ein spezifischerer Ausschluss möglich ist
  - Nur den Dateinamen anstelle eines vollqualifizierten Pfads zur Datei verwenden
  - Verwenden Sie Device Trajectory oder Secure Endpoint Diagnostics Package und Performance Tuning Tool, um den erforderlichen Ausschluss zu untersuchen und zu bestimmen.

- **Übermäßige Verwendung von Platzhalterausschlüssen**
  - Der Ausschluss von Platzhaltern führt nicht nur zu mehr Sicherheitslücken, sondern erfordert auch mehr Systemressourcen als jeder andere Ausschlusstyp.
  - Achten Sie darauf, die minimale Anzahl von Platzhaltern in einem Ausschluss zu verwenden. Nur die Ordner, die wirklich variabel sind, sollten mit einem Platzhalter variabel gemacht werden. Beispiele:
    - Programme\Software* schließt alle Dateien im Ordner aus, aber keine Unterordner

    - Programme\Software** schließt alles aus, was sich im Ordner befindet, einschließlich Unterordner

- **Elemente ausschließen, die bei Angriffen verwendet werden**
    - Dateitypen wie CMD, ZIP, JPG usw.
    - Prozesse wie svchost.exe, bash.exe, powershell.exe usw.
    - Ordnerspeicherorte wie C:\Users\, C:\Windows\Temp\, C:\Program Files\Java usw.

- **Doppelte Ausschlüsse**
    - Überprüfen Sie vor dem Erstellen eines Ausschlusses, ob der Ausschluss bereits in den vom Benutzer erstellten benutzerdefinierten Ausschlüssen oder den von Cisco verwalteten Ausschlüssen vorhanden ist.
    - Durch die Beseitigung doppelter Ausschlüsse wird nicht nur die Leistung verbessert, sondern auch das Betriebsmanagement für Ausschlüsse reduziert.

- **Veraltete Ausschlüsse**
    - Ausschlüsse, die vor langer Zeit erstellt wurden und möglicherweise nicht mehr erforderlich sind.
    - Überprüfen und prüfen Sie regelmäßig Ihre Ausschlussliste, und bewahren Sie sicher auf, warum ein bestimmter Ausschluss hinzugefügt wurde.

- **Keine Ausschlüsse nach einer Infektion**
    - Ausschlüsse sollten entfernt werden, sobald eine Infektion erkannt wurde, um wieder ein optimales Maß an Sicherheit und Transparenz zu erreichen.
    - Wenn Sie die Funktion "Automatisierte Aktionen" (Automated Actions) "Computer in Gruppe verschieben" im Voraus verwenden, können Sie nach einer Infektion schnell eine sicherere Richtlinie anwenden, einschließlich der Einrichtung einer Richtlinie ohne Ausnahmen.

- **Fehlende Abwehrstrategien**
    - Wenn Ausschlüsse unbedingt erforderlich sind, überlegen Sie, welche Abwehrstrategien verfolgt werden können, z. B. indem Schreibschutz aktiviert wird, um den ausgeschlossenen Elementen einige Schutzebenen hinzuzufügen.

Weitere Best Practices zu Ausschlüssen oder sicherem Endpunkt finden Sie im Best Practices-Leitfaden.

Ausschlüsse nicht empfohlen

Im Hinblick auf eine gute Sicherheitslage und Sichtbarkeit werden die folgenden Ausschlüsse nicht empfohlen:

AcroRd32.exe
addinprocess.exe
addinprocess32.exe
addinutil.exe

bash.exe
bginfo.exe
Bitsadmin.exe
cdb.exe
csi.exe
dbghost.exe
dbgsvc.exe
dnx.exe
dotnet.exe
Excel.exe
fsi.exe
fsiAnyCpu.exe
iexplore.exe
java.exe
kd.exe
lxssmanager.dll
msbuild.exe
mshta.exe

ntkd.exe
ntsd.exe
outlook.exe
psexec.exe
powerpnt.exe
powershell.exe
rcsi.exe
svchost.exe
schtasks.exe
system.management.automation.dll
windbg.exe
winword.exe
wmic.exe
wuauclt.exe
0,7 z
.bat
.bin
.cab

.cmd
.com
CPL
.dll
.exe
FLA
.gif
.gz
.hta
.inf
Java
.jar
.job
.jpeg
.jpg
.js
.ko
.ko.gz

.msi
OCX
.png
PS1
.py
.rar
.reg
.scr
sys
.tar
.tmp
.url
.vbe
.vbs
.wsf
.zip
Schlag
Java

Python
Python 3color
Sch
zsch
/
/bin
/sbin
/usr/lib
C:
C:\
C:*
D:\
D:*
C:\Program Files\Java
C:\Temp\
C:\Temp*
C:\Users\

C:\Users*
C:\Windows\Prefetch
C:\Windows\Prefetch\
C:\Windows\Prefetch*
C:\Windows\System32\Spool
C:\Windows\System32\CatRoot2
C:\Windows\Temp
C:\Windows\Temp\
C:\Windows\Temp*
C:\Program Dateien\<Firmenname>\
C:\Program (x86)\<Firmenname>\
C:\Users\<UserProfileName>\AppData\Local\Temp\
C:\Users\<UserProfileName>\AppData\LocalLow\Temp\

Zugehörige Informationen

- **Technischer Support und Dokumentation für Cisco Systeme**
- **Cisco Secure Endpoint - Technische Hinweise**
- **Cisco Secure Endpoint - Benutzerhandbuch**
- **Sicheres Endgerät: Prozessausschlüsse in macOS und Linux**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.