Von Cisco verwaltete Änderungen der Ausschlussliste für die Cisco Secure Endpoint Console

Inhalt

30. September 2020
Malwarebytes - Windows
Digital Guardian - Mac
Neue Liste erstellt
3. März 2021
Kaspersky - Windows
SCCM - Fenster
Symantec - Windows
Neue Listen erstellt
30. Juni 2021
Microsoft Windows-Standard
Citrix ICA-Client
Citrix Provisioning Server
Neue Listen erstellt
29. September 2021
Cisco WebEx - Windows
Crashplan - Windows
Crashplan - Mac
VMware - Windows
23. März 2022
Microsoft Windows-Standard
Hyper-V - Windows
Microsoft Windows Defender - Windows
29. Juni 2022
Microsoft Windows-Standard
Cisco AnyConnect-VPN
Cisco Webex
Microsoft OneDrive (zuvor ein Laufwerk)
Tanium - Windows
Citrix Provisioning Server
Neue Listen erstellt
14. September 2022
Microsoft Windows-Standard
Microsoft SQL Server
TrendMicro/Apex One
Neue Listen erstellt
Oktober 2022
14. Dezember 2022
Microsoft Windows-Standard
Backend-Änderungen - Windows
Neue Listen erstellt
12. April 2023
Microsoft Windows-Standard
Microsoft Intune
McAfee Trellix SolidCore
Cisco Webex
Microsoft Defender für MacOS
Microsoft Defender für Linux
31. Mai 2023
VEEAM
VMware

Einleitung

In diesem Dokument werden die Änderungen beschrieben, die an den von Cisco verwalteten Ausschlüssen vorgenommen wurden.

Von Cisco verwaltete Ausschlüsse werden erstellt und verwaltet, um die Kompatibilität zwischen Advanced Malware Protection (AMP) für Endpoints Connector und Antivirus-, Sicherheits- oder anderer Software zu verbessern. Diese Ausschlüsse können neuen Versionen einer Anwendung hinzugefügt werden.

Voraussetzungen

Anforderungen

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

- Ausschlüsse in AMP für Endgeräte
- AMP-Konsole

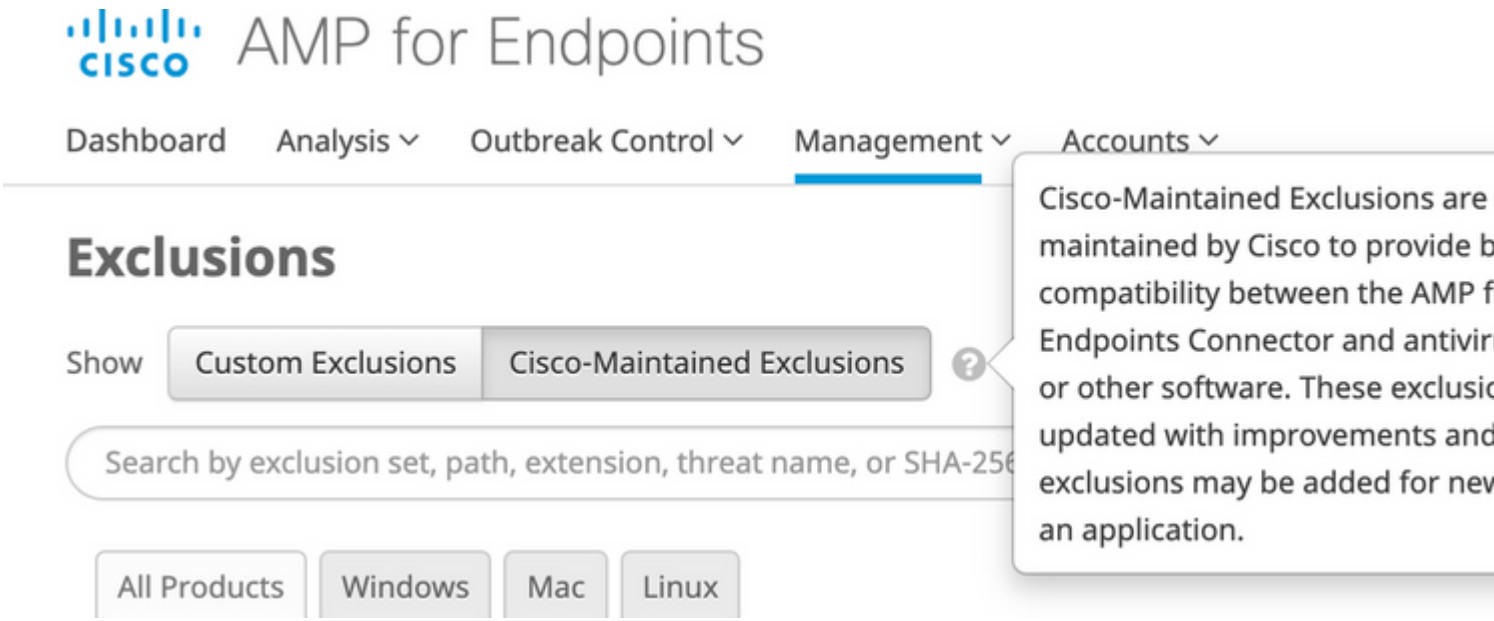
Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- AMP für Endgeräte, Konsolenversion 5.4.20190820

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.

Erwartungen bei Aktualisierung



Wenn die von Cisco verwalteten Listen geändert werden, erfolgt eine Richtlinienaktualisierung am Backend, um diese Änderung widerzuspiegeln. Wenn jeder Endpunkt diese Liste zum Einchecken in seinem Heartbeat verwendet, ruft er die aktualisierte Richtlinie ab. Diese Richtlinienänderungen werden nicht im Prüfprotokoll berücksichtigt, da es sich technisch gesehen um eine Änderung der Ausschlussliste handelt und nicht um die Richtlinie selbst. Von Cisco verwaltete Ausschlusslisten sind nicht im normalen Prüfprotokoll einzelner Konsolen vorhanden. Bei großen Umgebungen sieht dies nach einer Flut von Richtlinien-Updates aus, was zu einer besseren Leistung auf jedem einzelnen Endpunkt führt.

Der Aktualisierungszeitraum hängt von den einzelnen Endpunkten ab. Wenn alle Computer online sind, erfolgen die Updates innerhalb von 1-2 Heartbeats. Wenn es sich um eine globale Umgebung handelt, erfolgen Updates weiterhin, wenn die Systeme online gehen. Seien Sie daher nicht überrascht, wenn 24-48 Stunden nach dem Push der gepflegten Liste weitere Richtlinienaktualisierungen angezeigt werden.

Änderungen

28. August 2019

Microsoft Windows-Standard:

Entfernen von:

- **CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\edb*.log**
- **CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Res1.log**
- **CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Res2.log**

Grund: Wiederholend. Ein weiterer Ausschluss im Basissatz deckt ihn ab.

Hinzugefügt von:

- **C:\$WINDOWS.~BT\Sources\SetupHost.exe**

Grund: Windows 10-Updates sind aufgrund von Prozessscans sporadisch fehlgeschlagen.

N-Able Solar Winds - Fenster:

Hinzugefügt von:

- **C:\Program Dateien (x86)\N-able Technologies\Windows Agent\bin\agent.exe**
- **C:\Program Dateien (x86)\BeAnywhere Support Express\GetSupportService_N-Central\BASupSrvc.exe**
- **C:\Program Dateien (x86)\N-fähig Technologies\PatchManagement\ThirdPartyPatch\ThirdPartyPatch.exe**

Docker - Mac:

Entfernen von:

- **/Users/*/Library/Containers/com.docker.docker/Data/vms/*/Docker.***
- **/usr/local/bin/docker**

Grund: Ein zusätzlicher Test hat uns Bedenken hinsichtlich der Sicherheit gegeben, sodass die Entwicklung bessere Ausschlüsse aufgezeigt hat.

Hinzugefügt von:

- **/Applications/Docker.app/Contents/MacOS/Docker**
- **/Applications/Docker.app/Contents/Resources/bin/docker**

Neue Listen erstellt:

Linux :

- Docker - Anschluss 1.10.2
- Docker - Anschluss 1.11+
- Zabbix

Mac:

- Virtuelle Box
- Digital Guardian

18. September 2019

Apple MacOS-Standard:

Hinzugefügt von:

- **/Anwendungen/Time Machine.app/Contents/MacOS/Time Machine**
- **/System/Library/CoreServices/Spotlight.app/Contents/MacOS/Spotlight**

McAfee - Mac

Hinzugefügt von:

- **/Library/McAfee/Agent/bin/CmdAgent**

Cisco Jabber - Mac

Entfernen von:

- **/usr/bing/grep**
- **/bin/ps**

Grund: Mehr Sicherheit und die zusätzlichen Funktionen von prozessbasierten Ausschlüssen.

Hinzugefügt von:

- **/Anwendungen/Cisco Jabber.app/Inhalte/MacOS/Cisco Jabber**

Crashplan - Mac

Hinzugefügt von:

- **/Applications/CrashPlan.app/Contents/Library/LaunchServices/CrashPlanService.app/Contents/MacOS/CrashPlanService**

JAMF Casper - Mac

Entfernen von:

- **/usr/bin/sw_vers**

Grund: Mehr Sicherheit und die zusätzlichen Funktionen von prozessbasierten Ausschlüssen.

Hinzugefügt von:

- **/Library/Application Support/JAMF/Jamf.app/Contents/MacOS/JamfDaemon.app/Contents/MacOS/JamfDaemon**

- **/usr/local/jamf/bin/jamfAgent**
- **/usr/local/jamf/bin/jamf**
- **/Library/Application Support/JAMF/Jamf.app/Contents/MacOS/JamfAgent.app/Contents/MacOS/JamfAgent**

VMware Fusion - Mac

Hinzugefügt von:

- **/Anwendungen/VMware Fusion.app/Inhalt/MacOS/VMware Fusion**

Xcode - Mac

Hinzugefügt von:

- **/Applications/Xcode.app/Contents/SharedFrameworks/XCBuild.framework/Versions/A/PlugIns/XCBBuildService.bundle/Cont**
- **/Applications/Xcode.app/Contents/Developer/usr/bin/xcodebuild**

Ein Laufwerk - Windows

Geringfügige Änderungen:

- **C:*\Users\OneDrive** (Backslash für mehr Sicherheit hinzugefügt)

Citrix ICA-Client - Windows

Hinzugefügt von:

- **CSIDL_PROGRAM_FILES\Citrix\Benutzerprofil-Manager\Benutzerprofil-Manager.exe**
- **CSIDL_PROGRAM_FILES\Citrix\Virtual Desktop Agent\BrokerAgent.exe**
- **CSIDL_PROGRAM_FILES\Citrix\ICAService\picaSvc2.exe**
- **CSIDL_PROGRAM_FILES\Citrix\ICAService\CpSvc.exe**

Grund: Kürzlich aktualisierte Versionen von Citrix schlugen Ausnahmen vor.

Neue Listen erstellt:

Windows

- Citrix Provisioning Server
- Citrix Cloud Connector

11. Dezember - 2019

Ein Laufwerk - Windows

Hinzugefügt von:

- **CSIDL_LOCAL_APPDATA\Microsoft\OneDrive\OneDrive.exe**

Splunk - Windows

Hinzugefügt von:

- **CSIDL_PROGRAM_FILE\splunkforwarder\bin\splunk-winevtlog.exe**
- **CSIDL_PROGRAM_FILE\splunkforwarder\bin\splunkd.exe**

Splunk - Linux

Hinzugefügt von:

- **/opt/splunkforwarder/bin/splunk**
- **/opt/splunk/bin/splunk**

Neue Listen erstellt:

Azure - Linux

Vagrant - Mac

12. Februar 2020

Microsoft Windows-Standard - Windows

Hinzugefügt von:

- **C:\Program Files\Cisco\Orbital\osqueryd.exe**
- **C:\Program Files\Cisco\Orbital\orbital-ampwin.exe**

Websense - Windows

Hinzugefügt von:

- **[Mehrere Laufwerke]:\Programme*\Websense**
- **C:\Program Dateien (x86)\Websense\Websense Endpoint\dserui.exe**
- **C:\Program Files\Websense\Websense Endpoint\dserui.exe**
- **C:\Program Dateien (x86)\Websense\Websense Endpoint\EndPointClassifier.exe**
- **C:\Program Dateien (x86)\Websense\Websense Endpoint\FilterSDK\kvoop.exe**
- **C:\Program Dateien (x86)\Websense\Websense Endpoint\wepsvc.exe**

Microsoft SQL Server - Windows

Hinzugefügt von:

- **CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL\FTDATA**
- **SQL**

10. Juni 2020

Malwarebytes - Windows

Geringfügige Änderungen:

- **C:\ProgramData\Malwarebytes Endpunkt-Agent**
- **C:\ProgramData\Malwarebytes\MBAMService**

Microsoft Office - Windows

Hinzugefügt von:

- **C:\Program Files\Common Dateien\microsoft shared\ClickToRun\OfficeClickToRun.exe**

IIS - Windows

Hinzugefügt von:

- **C:\Windows\SysWOW64\inetsrv\w3wp.exe**
- **C:\Windows\System32\inetsrv\w3wp.exe**

Altiris von Symantec - Windows

Hinzugefügt von:

- **C:\Program Files\Altiris\Altiris Agent\AeXNSAgent.exe**

McAfee - Windows

Hinzugefügt von:

- **C:\Program Files\McAfee\Endpoint Sicherheit\Adaptive Threat Protection\mfeatp.exe**

Neue Listen erstellt:

NetScout - Windows

IBM - Windows

15. Juli 2020

Domänencontroller - Windows

Hinzugefügt von:

- **CSIDL_WINDOWS\System32\dfsr.exe**
- **CSIDL_WINDOWS\System32\dfsrs.exe**
- **CSIDL_WINDOWS\System32\dns.exe**
- **CSIDL_WINDOWS\System32\ntfrs.exe**

Microsoft Teams - Windows

Hinzugefügt von:

- **CSIDL_LOCAL_APPDATA\Microsoft\Teams\current\teams.exe**
- **CSIDL_LOCAL_APPDATA\Microsoft\Teams\update.exe**

Neue Liste erstellt

Kontrolle Up

26. August 2020

**Aufgrund weiterer Tests wurde das ursprüngliche Veröffentlichungsdatum vom 19. auf den 26. verlängert

Microsoft SQL Server - Windows

Ersetzen:

- **CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.1\MSSQL\Binn\SQLServr.exe**
- **CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.2\OLAP\Bin\MSMDSrv.exe**
- **CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.3\Reporting Services\ReportServer\Bin\ReportingServicesService.exe**

Hinzugefügt von:

- **CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.11\MSSQL\Binn\SQLServr.exe**
- **CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.12\MSSQL\Binn\SQLServr.exe**
- **CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.13\MSSQL\Binn\SQLServr.exe**
- **CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.11\OLAP\Bin\MSMDSrv.exe**
- **CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.12\OLAP\Bin\MSMDSrv.exe**
- **CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.13\OLAP\Bin\MSMDSrv.exe**
- **CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.11\Reporting Services\ReportServer\Bin\ReportingServicesService.exe**
- **CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.12\Reporting Services\ReportServer\Bin\ReportingServicesService.exe**
- **CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.13\Reporting Services\ReportServer\Bin\ReportingServicesService.exe**

30. September 2020

Malwarebytes - Windows

Hinzugefügt von:

- **CSIDL_PROGRAM_FILES\Malwarebytes' Anti-Malware\mbam.exe**
- **CSIDL_PROGRAM_FILESX86\Malwarebytes' Anti-Malware\mbam.exe**

Digital Guardian - Mac

Hinzugefügt von:

- **/usr/local/dgagent**
- **/dgagent**

Neue Liste erstellt

Digital Guardian - Windows

3. März 2021

Kaspersky - Windows

Hinzugefügt von:

- **CSIDL_PROGRAM_FILESX86\Kaspersky Lab\Kaspersky Endpoint Security for Windows\avp.exe**
- **CSIDL_PROGRAM_FILESX86\Kaspersky Lab\NetworkAgent\klnagent.exe**

SCCM - Fenster

Entfernen von:

- **WINDOWS\CCM\ServiceData** - Doppelter Pfad
- **Programmdateien\Microsoft Configuration Manager\EasySetupPayload** - Doppelter Pfad

Symantec - Windows

Hinzugefügt von:

- **CSIDL_PROGRAM_FILES\Symantec\Endpoint Agent\edpa.exe**
- **CSIDL_PROGRAM_FILESX86\Symantec\Symantec Endpoint Protection\12.1.4013.4013.105\Bin64\Smc.exe**
- **CSIDL_PROGRAM_FILESX86\Symantec\Symantec Endpoint Protection\12.1.6608.6300.105\Bin\ccSvcHst.exe**
- **CSIDL_PROGRAM_FILESX86\Symantec\Symantec Endpoint Protection\12.1.7061.6600.105\Bin\ccSvcHst.exe**
- **CSIDL_PROGRAM_FILESX86\Symantec\Symantec Endpoint Protection\12.1.7385.6902.105\Bin\ccSvcHst.exe**
- **CSIDL_PROGRAM_FILESX86\Symantec\Symantec Endpoint Protection**
- **CSIDL_PROGRAM_FILES\Symantec\Endpoint Agent\brkrprcs64.exe**

Neue Listen erstellt

Cisco AnyConnect - Windows

Microsoft Defender ATP - Windows

30. Juni 2021

Microsoft Windows-Standard

Hinzugefügt von:

- **CSIDL_WINDOWS\System32\GroupPolicy\User\registry.pol**
- **CSIDL_WINDOWS\System32\GroupPolicy\Machine\registry.pol**

Citrix ICA-Client

Hinzugefügt von:

- **CSIDL_PROGRAM_FILES\Citrix\Broker\Service\BrokerService.exe**
- **CSIDL_PROGRAM_FILES\Citrix\Broker\Service\HighAvailabilityService.exe**
- **CSIDL_PROGRAM_FILES\Citrix\ConfigSync\ConfigSyncService.exe**
- **CSIDL_PROGRAM_FILESX86\Citrix\ICA-Client**

Citrix Provisioning Server

Entfernen von:

- **C:\System32\drivers\CfsDep2.sys**
- **C:\System32\drivers\CvhdBusP6.sys**
- **C:\System32\drivers\CVhdMp.sys**

Hinzugefügt von:

- **CSIDL_WINDOWS\System32\drivers\CfsDep2.sys**
- **CSIDL_WINDOWS\System32\drivers\CvhdBusP6.sys**
- **CSIDL_WINDOWS\System32\drivers\CVhdMp.sys**
- **CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\BNTFTP.EXE**
- **CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\PVSTSB.EXE**
- **CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\StreamService.exe**
- **CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\StreamProcess.exe**
- **CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\soapserver.exe**
- **CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\Inventory.exe**
- **CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\Notifier.exe**
- **CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\MgmntDaemon.exe**
- **CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\BNPXE.exe**
- **CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\BNDevice.exe**

Neue Listen erstellt

CommVault - Windows

Citrix Sitzungsaufzeichnung - Windows

29. September 2021

Cisco WebEx - Windows

Hinzugefügt von:

- **CSIDL_LOCAL_APPDATA\CiscoSparkLauncher\CiscoCollabHost.exe**
- **CSIDL_LOCAL_APPDATA\CiscoSparkLauncher**
- **CSIDL_LOCAL_APPDATA\WebEx\WebEx\Meetings_01\atmgr.exe**
- **CSIDL_LOCAL_APPDATA\WebEx\WebEx\Meetings_02\atmgr.exe**
- **CSIDL_LOCAL_APPDATA\WebEx\WebEx\Meetings_03\atmgr.exe**
- **CSIDL_LOCAL_APPDATA\WebEx\WebEx\Meetings_04\atmgr.exe**
- **CSIDL_LOCAL_APPDATA\WebEx\WebEx\Meetings_***

Crashplan - Windows

Hinzugefügt von:

- **CSIDL_PROGRAM_FILES\Code42\Code42Service.exe**

Crashplan - Mac

Hinzugefügt von:

- **/Applications/Code42.app/Contents/Library/LaunchServices/Code42Service.app/Contents/MacOS/Cod**

VMware - Windows

Hinzugefügt von:

- **CSIDL_PROGRAM_FILESX86\VMware\VMware DataS Agent\service\DaaSAgent.exe**

23. März 2022

Microsoft Windows-Standard

Hinzugefügt von:

- **C:\Windows\System32\SearchIndexer.exe**

Hyper-V - Windows

Hinzugefügt von:

- **CSIDL_COMMON_APPDATA\Microsoft\Windows\Hyper-V**
- **CSIDL_COMMON_DOCUMENTS\Hyper-V\Virtuelle Festplatten**

Microsoft Windows Defender - Windows

Hinzugefügt von:

- *** \ProgramData\Microsoft\Windows Defender Advanced Threat Protection\DataCollection**

29. Juni 2022

Microsoft Windows-Standard

Hinzugefügt von:

- ***.applocker**

Cisco AnyConnect-VPN

Hinzugefügt von:

- **CSIDL_PROGRAM_FILESX86\Cisco\Cisco AnyConnect Secure Mobility Client\acwebhelper.exe**

Cisco Webex

Hinzugefügt von:

- **C:\Users*\AppData\Local\WebEx\WebEx\Meetings\atmgr.exe**

Microsoft OneDrive (zuvor ein Laufwerk)

Hinzugefügt von:

- **C:\Users*\AppData\Local\Microsoft\OneDrive\OneDrive.exe**

Tanium - Windows

Hinzugefügt von:

- **C:\Program Dateien (x86)\Tanium\Tanium Endbenutzer-Benachrichtigungstools\bin\end-user-notifications.exe**

Citrix Provisioning Server

Hinzugefügt von:

- **CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\MgmtDaemon.com**

Entfernen von:

- **CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\MgmntDaemon.com**

Neue Listen erstellt

X1-Suche - Windows

Microsoft Intune - Windows

14. September 2022

Microsoft Windows-Standard

Hinzugefügt von:

- **CSIDL_PROGRAM_FILESX86\Cisco\Cisco Secure Client**
- **CSIDL_PROGRAM_FILESX86\Cisco\Cisco Secure Client\UI\acumbrellaagent.exe**
- **CSIDL_PROGRAM_FILESX86\Cisco\Cisco Secure Client\UI\acumbrellaagent.exenscrypt-proxy.exe**
- **CSIDL_PROGRAM_FILESX86\Cisco\Cisco Secure Client\NVM\acnvmagent.exe**
- **CSIDL_PROGRAM_FILESX86\Cisco\Cisco Secure Client\vpnagent.exe**
- **CSIDL_PROGRAM_FILESX86\Cisco\Cisco Secure Client\acnamlogonagent.exe**
- **CSIDL_PROGRAM_FILESX86\Cisco\Cisco Secure Client\acnamagent.exe**
- **CSIDL_PROGRAM_FILESX86\Cisco\Cisco Secure Client\UI\csc_ui.exe**
- **CSIDL_PROGRAM_FILES\Cisco\Cisco Secure Client\CM*\CMID*\csc_cmid.exe**
- **CSIDL_PROGRAM_FILES\Cisco\Cisco Secure Client\CM*\CMPM*\csc_pm.exe**
- **CSIDL_PROGRAM_FILES\Cisco\Cisco Secure Client\CM*\Service*\csc_cms.exe**
- **CSIDL_SYSTEM\appidpolicyconverter.exe**

Microsoft SQL Server

Erweiterung um V. 2019

Hinzugefügt von:

- **CSIDL_PROGRAM_FILES\Microsoft SQL Server*\MSSQL\Binn\SQLServr.exe**
- **CSIDL_PROGRAM_FILES\Microsoft SQL Server*\OLAP\Bin\MSMDSrv.exe**
- **CSIDL_PROGRAM_FILES\Microsoft SQL Server*\Reporting Services\ReportServer\Bin\ReportingServicesService.exe**
- **CSIDL_PROGRAM_FILES\Microsoft SQL Server*\Shared\SQLDumper.exe**
- **CSIDL_PROGRAM_FILES\Microsoft SQL Server\MS*.***
- **CSIDL_PROGRAM_FILES\Microsoft SQL Server*\COM**
- **CSIDL_PROGRAM_FILES\Microsoft SQL Server*\DTS**

- **CSIDL_PROGRAM_FILES\Microsoft SQL Server*\Freigegeben**

TrendMicro/Apex One

Hinzufügen von:

- **CSIDL_PROGRAM_FILESX86\Trend Micro\Security Agent\CCSF\TMCCSF.exe**
- **CSIDL_PROGRAM_FILESX86\Trend Micro\Security Agent\TmPfw.exe**
- **CSIDL_PROGRAM_FILESX86\Trend Micro\Security Agent\TmListen.exe**
- **CSIDL_PROGRAM_FILESX86\Trend Micro\Security Agent\Ntrtscan.exe**
- **CSIDL_PROGRAM_FILESX86\Trend Micro\iService\iATAS\ATASAgent.exe**
- **CSIDL_PROGRAM_FILESX86\Trend Micro\iService\iAC\ac_bin\TMiACAgentSvc.exe**
- **CSIDL_PROGRAM_FILESX86\Trend Micro\iService\iES\ESE\ESEServiceShell.exe**
- **CSIDL_PROGRAM_FILESX86\Trend Micro\iService\iES\ESE\ESClient.exe**
- **CSIDL_PROGRAM_FILESX86\Trend Micro\BM\TMBMSRV.exe**
- **CSIDL_PROGRAM_FILESX86\Trend Micro\Security Agent\TMBMSRV.exe**
- **CSIDL_PROGRAM_FILESX86\Trend Micro\iService\iVP\iVPAgent.exe**
- **CSIDL_PROGRAM_FILESX86\Trend Micro\Security Agent\TmSSClient.exe**
- **CSIDL_PROGRAM_FILESX86\Trend Micro\Security Agent\LogServer.exe**
- **CSIDL_PROGRAM_FILESX86\Trend Micro\Agent\Temp\LogServer\LogServer.exe**
- **CSIDL_PROGRAM_FILESX86\Trend Micro\Agent\CCSF\module\BES\TmsaInstance64.exe**
- **CSIDL_PROGRAM_FILESX86\Trend Micro\Security Agent\CNTAoSMgr.exe**
- **CSIDL_PROGRAM_FILESX86\Trend Micro\Security Agent\PccNTMon.exe**
- **CSIDL_PROGRAM_FILESX86\Trend Micro\iService\iES\ESE\ESEFrameworkHost.exe**
- **CSIDL_SYSTEM\ShowMsg.exe**
- **CSIDL_SYSTEM\dsagent.exe**
- .bkf

Neue Listen erstellt

Azure DevOps - Windows

Oktober 2022

Im Laufe des Monats Oktober werden missgebildete Ausschlüsse, die in früheren Versionen des Produkts in die Secure Endpoint-Umgebung eingeführt wurden, aus benutzerdefinierten Ausschlusslisten entfernt. Weitere Informationen zu dieser Initiative finden Sie hier.

14. Dezember 2022

Microsoft Windows-Standard

Hinzugefügt von:

- **C:\Windows\System32\omadmclient.exe**
- **.automaticDestinations-ms**

Backend-Änderungen - Windows

- **csc_ui.exe** hinzugefügt zu Exploit-Prävention Globale Ausschlüsse für V5 und Script Control.

Entfernen von: Ausschlüsse, die sich auf die Leistung auswirken

Neue Listen erstellt

1Kennwort - Windows, Mac, Linux

McAfee Trellix SolidCore - Windows

12. April 2023

Microsoft Windows-Standard

Hinzugefügt von:

- **PDF**
- **CSIDL_PROGRAM_FILESX86\Cisco\Cisco Secure Client\acumbrellaagent.exe**

Entfernen von:

- **CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs*.log**
- **CSIDL_SYSTEM\CatRoot2**
- **CSIDL_WINDOWS\Prefetch**

Microsoft Intune

Hinzugefügt von:

- **CSIDL_PROGRAM_FILESX86\Microsoft Intune Management Extension\Microsoft.Management.Services.IntuneWindowsAgent.exe**

McAfee Trellix SolidCore

Geringfügige Änderungen:

- **CSIDL_PROGRAM_FILESX86\McAfee\Policy Auditor Agent\engineMain.exe**

Cisco Webex

Hinzugefügt von:

- **C:\Users*\AppData\WebEx\WebexHost.exe**

Microsoft Defender für MacOS

Hinzugefügt von:

- **/Library/Application Support/Microsoft/Defender/**

Microsoft Defender für Linux

Hinzugefügt von:

- **/opt/microsoft/mdatp/sbin/wdavdaemon**

- **/opt/microsoft/mdatp/**

31. Mai 2023

VEEAM

Hinzugefügt von:

- **CSIDL_PROGRAM_FILES\Common Files\Veeam\Backup and Replication\Explorers Recovery Service\Veeam.StandBy.Service.exe**
- **CSIDL_PROGRAM_FILES\Common Files\Veeam\Backup and Replication\Mount Service\Veeam.Backup.MountService.exe**
- **CSIDL_PROGRAM_FILES\Veeam\Backup und Replikation\Backup\Veeam.Backup.BrokerService.exe**
- **CSIDL_PROGRAM_FILES\Veeam\Backup und Replikation\Backup\Veeam.Backup.CloudService.exe**
- **CSIDL_PROGRAM_FILES\Veeam\Backup und Replikation\Backup\Veeam.Backup.ExternalInfrastructure.DbProvider.exe**
- **CSIDL_PROGRAM_FILESX86\Veeam\Backup Transport\GuestInteraction\VSS\VeeamGuestHelperCtrl.exe**
- **CSIDL_PROGRAM_FILES\Veeam\Backup und Replikation\Backup\Veeam.Backup.Service.exe**
- **CSIDL_PROGRAM_FILES\Veeam\Backup und Replikation\Backup-Katalog\Veeam.Backup.CatalogDataService.exe**
- **CSIDL_PROGRAM_FILES\Veeam\Backup und Replikation\Backup\Veeam.Backup.ManagerGCServer.exe**
- **CSIDL_PROGRAM_FILES\Veeam\Backup und Replikation\Backup\Veeam.Backup.Cdp.Service.exe**
- **CSIDL_PROGRAM_FILES\Veeam\Backup und Replikation\Console\veeam.backup.shell.exe**
- **CSIDL_PROGRAM_FILESX86\Veeam\Backup Transport\x64\VeeamAgent.exe**
- **CSIDL_PROGRAM_FILES\Veeam\Backup und Replikation\Backup\Veeam.Backup.Manager.exe**
- **CSIDL_WINDOWS\Veeam\Backup\VeeamDeploymentSvc.exe**
- **.vbm.temp**
- **.flach**

VMware

Hinzugefügt von:

- **CSIDL_PROGRAM_FILES\Allgemeine Files\VMware\ScannerRedirection\ftscanmgrhv.exe**
- **CSIDL_PROGRAM_FILESX86\VMware\VMware Horizon View Client\ClientService\horizon_client_service.exe**

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.