Modifiche all'elenco di esclusione gestite da Cisco per Cisco Secure Endpoint Console

Sommario

15 luglio - 2020
Controller di dominio - Windows
Microsoft Teams - Windows
Nuovo elenco creato
26 agosto - 2020
Microsoft SQL Server - Windows
30 settembre - 2020
Malwarebytes - Windows
Digital Guardian - Mac
Nuovo elenco creato
3 marzo - 2021
Kaspersky - Windows
SCCM - Windows
Symantec - Windows
Nuovi elenchi creati
30 giugno - 2021
Impostazioni predefinite di Microsoft Windows
Citrix ICA Client
Citrix Provisioning Server
Nuovi elenchi creati
29 settembre - 2021
Cisco Webex - Windows
Crashplan - Windows
Crashplan - Mac
VMware - Windows
23 marzo - 2022
Impostazioni predefinite di Microsoft Windows
Hyper-V - Windows
Microsoft Windows Defender - Windows
29 giugno - 2022
Impostazioni predefinite di Microsoft Windows
Cisco AnyConnect VPN
Cisco Webex
Microsoft OneDrive (in precedenza One Drive)
Tanium - Windows
Citrix Provisioning Server
Nuovi elenchi creati
14 settembre - 2022
Impostazioni predefinite di Microsoft Windows
Microsoft SQL Server
TrendMicro/Apex One
Nuovi elenchi creati
Ottobre - 2022
14 dicembre - 2022
Impostazioni predefinite di Microsoft Windows
Modifiche back-end - Windows
Nuovi elenchi creati

Introduzione

Questo documento descrive le modifiche aggiunte alle esclusioni gestite da Cisco.

Le esclusioni gestite da Cisco sono create e gestite da Cisco per garantire una migliore compatibilità tra Advanced Malware Protection (AMP) for Endpoints Connector e software antivirus, di sicurezza o di altro tipo. Tali esclusioni possono essere aggiunte alle nuove versioni di un'applicazione.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Esclusioni in AMP for Endpoints
- console AMP

Componenti usati

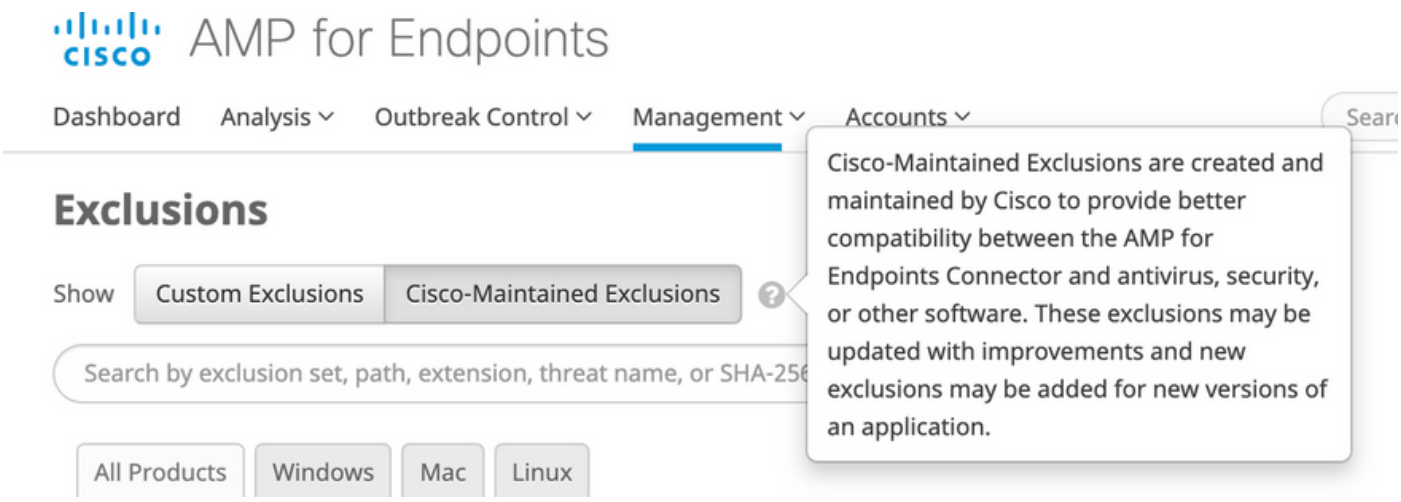
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- AMP for Endpoints console versione 5.4.20190820

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Aspettative in caso di aggiornamento



Quando gli elenchi Cisco-Managed vengono modificati, si verifica un aggiornamento delle policy sul back-end per riflettere la modifica. Man mano che ciascuno degli endpoint utilizza l'elenco archiviato nel proprio heartbeat, recupera il criterio aggiornato. Queste modifiche ai criteri non vengono riflesse nel log di controllo in quanto tecnicamente rappresentano una modifica all'elenco di esclusione, non ai criteri stessi e gli elenchi di esclusione gestiti da Cisco non esistono nel normale log di controllo sulle singole console. Per gli ambienti su larga scala, questo sembra un'ondata di aggiornamenti delle policy e il risultato finale sarà un miglioramento delle prestazioni di ogni endpoint.

Il periodo di aggiornamento dipende da ciascun endpoint. Se tutti i computer sono in linea, gli aggiornamenti avvengono entro 1-2 heartbeat. Se si tratta di un ambiente globale, gli aggiornamenti continuano a verificarsi quando i computer sono in linea, quindi non sorprendetevi di vedere ulteriori aggiornamenti delle policy 24-48 ore dopo il push dell'elenco di manutenzione.

Modifiche

28 agosto - 2019

Impostazioni predefinite di Microsoft Windows:

Rimozione di:

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

Motivo: Ripetitivo. Un'altra esclusione nel set di base la copre.

Aggiunta di:

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

Motivo: aggiornamenti di Windows 10 sporadicamente non riusciti a causa di analisi dei processi.

Venti solari N-Able - Windows:

Aggiunta di:

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

Docker - Mac:

Rimozione di:

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

Motivo: Ulteriori test ci hanno lasciato preoccupati per la sicurezza, quindi lo sviluppo ha individuato esclusioni migliori.

Aggiunta di:

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

Nuovi elenchi creati:

Linux:

- Docker - Connettore 1.10.2
- Docker - Connettore 1.11+
- Zabbix

Mac:

- Scatola virtuale
- Digital Guardian

18 settembre - 2019

Predefinito MacOS Apple:

Aggiunta di:

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

McAfee - Mac

Aggiunta di:

- /Library/McAfee/Agent/bin/CmdAgent

Cisco Jabber - Mac

Rimozione di:

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

Motivo: maggiore sicurezza e funzionalità aggiuntive delle esclusioni basate sui processi.

Aggiunta di:

- **/Applications/Cisco Jabber.app/Contents/MacOS/Cisco Jabber**

Crashplan - Mac

Aggiunta di:

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

JAMF Casper - Mac

Rimozione di:

- /usr/bin/sw_vers

Motivo: maggiore sicurezza e funzionalità aggiuntive delle esclusioni basate sui processi.

Aggiunta di:

- /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

Aggiunta di:

- /Applications/VMware Fusion.app/Contents/MacOS/VMware Fusion

Xcode - Mac

Aggiunta di:

- /Applications/Xcode.app/Contents/SharedFrameworks/XCBuild.framework/Versions/A/PlugIns/XCBBuildService.bundle/Co

- /Applications/Xcode.app/Contents/Developer/usr/bin/xcodebuild

One Drive - Windows

Modifica minore:

- C:*\Users\OneDrive\ (Aggiunta della barra rovesciata per una maggiore sicurezza)

Citrix ICA Client - Windows

Aggiunta di:

- CSIDL_PROGRAM_FILES\Citrix\User Profile Manager\UserProfileManager.exe
- CSIDL_PROGRAM_FILES\Citrix\Virtual Desktop Agent\BrokerAgent.exe
- CSIDL_PROGRAM_FILES\Citrix\ICAService\picaSvc2.exe
- CSIDL_PROGRAM_FILES\Citrix\ICAService\CpSvc.exe

Motivo: recente aggiornamento delle esclusioni suggerite da Citrix.

Nuovi elenchi creati:

Windows

- Citrix Provisioning Server
- Citrix Cloud Connector

11 dicembre - 2019

One Drive - Windows

Aggiunta di:

- CSIDL_LOCAL_APPDATA\Microsoft\OneDrive\OneDrive.exe

Splunk - Windows

Aggiunta di:

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

Splunk - Linux

Aggiunta di:

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

Nuovi elenchi creati:

Azure - Linux

Vagrant - Mac

12 febbraio - 2020

Impostazioni predefinite di Microsoft Windows - Windows

Aggiunta di:

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

Websense - Windows

Aggiunta di:

- [Più unità]:\Programmi*\Websense\
- C:\Program Files (x86)\Websense\Websense Endpoint\dserui.exe
- C:\Program Files\Websense\Websense Endpoint\dserui.exe
- C:\Program Files (x86)\Websense\Websense Endpoint\EndPointClassifier.exe
- C:\Program Files (x86)\Websense\Websense Endpoint\FilterSDK\kvoop.exe
- C:\Program Files (x86)\Websense\Wepsvc.exe

Microsoft SQL Server - Windows

Aggiunta di:

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

10 giugno - 2020

Malwarebytes - Windows

Modifica minore:

- C:\ProgramData\Malwarebytes Endpoint Agent\
- C:\ProgramData\Malwarebytes\MBAMService\

Microsoft Office - Windows

Aggiunta di:

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

IIS - Windows

Aggiunta di:

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

Altiris di Symantec - Windows

Aggiunta di:

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

McAfee - Windows

Aggiunta di:

- C:\Program Files\McAfee\Endpoint Security\Adaptive Threat Protection\mfeature.exe

Nuovi elenchi creati:

NetScout - Windows

IBM - Windows

15 luglio - 2020

Controller di dominio - Windows

Aggiunta di:

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

Microsoft Teams - Windows

Aggiunta di:

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

Nuovo elenco creato

Controllo in alto

26 agosto - 2020

**A causa di ulteriori test, la data di rilascio originale è stata estesa dal 19 al 26

Microsoft SQL Server - Windows

Sostituzione di:

- 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

Aggiunta di:

- 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 settembre - 2020

Malwarebytes - Windows

Aggiunta di:

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

Digital Guardian - Mac

Aggiunta di:

- /usr/local/dgagent
- /dgagent

Nuovo elenco creato

Digital Guardian - Windows

3 marzo - 2021

Kaspersky - Windows

Aggiunta di:

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

SCCM - Windows

Rimozione di:

- WINDOWS\CCM\ServiceData - Percorso duplicato
- Programmi\Microsoft Configuration Manager\EasySetupPayload - Percorso duplicato

Symantec - Windows

Aggiunta di:

- 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\12.1.608.6300.105\Bin\ccSvcHst.exe
- CSIDL_PROGRAM_FILESX86\Symantec\Symantec Endpoint Protection\12.1.7061.600.105\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

Nuovi elenchi creati

Cisco AnyConnect - Windows

Microsoft Defender ATP - Finestre

30 giugno - 2021

Impostazioni predefinite di Microsoft Windows

Aggiunta di:

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

Citrix ICA Client

Aggiunta di:

- 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

Rimozione di:

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

Aggiunta di:

- 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

Nuovi elenchi creati

Commvault - Windows

Registrazione sessioni Citrix - Windows

29 settembre - 2021

Cisco Webex - Windows

Aggiunta di:

- 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

Aggiunta di:

- CSIDL_PROGRAM_FILES\Code42\Code42Service.exe

Crashplan - Mac

Aggiunta di:

- /Applications/Code42.app/Contents/Library/LaunchServices/Code42Service.app/Contents/MacOS/C

VMware - Windows

Aggiunta di:

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

23 marzo - 2022

Impostazioni predefinite di Microsoft Windows

Aggiunta di:

- C:\Windows\System32\SearchIndexer.exe

Hyper-V - Windows

Aggiunta di:

- CSIDL_COMMON_APPDATA\Microsoft\Windows\Hyper-V\
- CSIDL_COMMON_DOCUMENTS\Hyper-V\Dischi rigidi virtuali\

Microsoft Windows Defender - Windows

Aggiunta di:

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

29 giugno - 2022

Impostazioni predefinite di Microsoft Windows

Aggiunta di:

- applocker

Cisco AnyConnect VPN

Aggiunta di:

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

Cisco Webex

Aggiunta di:

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

Microsoft OneDrive (in precedenza One Drive)

Aggiunta di:

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

Tanium - Windows

Aggiunta di:

- C:\Program Files (x86)\Tanium\Tanium Strumenti di notifica per l'utente finale\bin\end-user-notifications.exe

Citrix Provisioning Server

Aggiunta di:

- CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\MgmtDaemon.com

Rimozione di:

- CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\MgmntDaemon.com

Nuovi elenchi creati

Ricerca X1 - Windows

Microsoft Intune - Windows

14 settembre - 2022

Impostazioni predefinite di Microsoft Windows

Aggiunta di:

- 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

Espanso per includere V. 2019

Aggiunta di:

- 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_PROGRAMMI\Microsoft SQL Server*\COM\
- CSIDL_PROGRAM_FILES\Microsoft SQL Server*\DTS\
- CSIDL_PROGRAM_FILES\Microsoft SQL Server*\Shared\

TrendMicro/Apex One

Aggiunta Di:

- CSIDL_PROGRAM_FILESX86\Trend Micro\Security Agent\CSF\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\Security Agent\Temp\LogServer\LogServer.exe
- CSIDL_PROGRAM_FILESX86\Trend Micro\Security 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

Nuovi elenchi creati

DevOps di Azure - Windows

Ottobre - 2022

Nel mese di ottobre le esclusioni in formato non corretto introdotte nell'ambiente Secure Endpoint durante le iterazioni precedenti del prodotto verranno rimosse dagli elenchi di esclusione personalizzati. Per maggiori informazioni sull'iniziativa, cliccare qui.

14 dicembre - 2022

Impostazioni predefinite di Microsoft Windows

Aggiunta di:

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

Modifiche back-end - Windows

- csc_ui.exe aggiunto a Exploit Prevention Global Exclusions per V5 e Script Control.

Rimozione di: Esclusioni che influiscono sulle prestazioni

Nuovi elenchi creati

1Password - Windows, Mac, Linux

McAfee Trellix SolidCore - Windows

12 aprile - 2023

Impostazioni predefinite di Microsoft Windows

Aggiunta di:

- pf
- CSIDL_PROGRAM_FILESX86\Cisco\Cisco Secure Client\acumbrellaagent.exe

Rimozione di:

- CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\.
- CSIDL_SYSTEM\CatRoot2\
- CSIDL_WINDOWS\Prelettura\

Microsoft Intune

Aggiunta di:

- CSIDL_PROGRAM_FILESX86\Estensione di gestione di Microsoft Intune\Microsoft.Management.Services.IntuneWindowsAgent.exe

McAfee Trellix SolidCore

Modifica minore:

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

Cisco Webex

Aggiunta di:

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

Microsoft Defender per MacOS

Aggiunta di:

- /Libreria/Supporto Applicazioni/Microsoft/Defender/

Microsoft Defender per Linux

Aggiunta di:

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

31 maggio - 2023

VEEAM

Aggiunta di:

- CSIDL_PROGRAM_FILES\Common Files\Veeam\Backup and Replication\Explorers Servizio di ripristino\Veeam.StandBy.Service.exe
- CSIDL_PROGRAM_FILES\Common Files\Veeam\Backup and Replication\Mount Service\Veeam.Backup.MountService.exe

- CSIDL_PROGRAM_FILES\Veeam\Backup and Replication\Backup\Veeam.Backup.BrokerService.exe
- CSIDL_PROGRAM_FILES\Veeam\Backup and Replication\Backup\Veeam.Backup.CloudService.exe
- CSIDL_PROGRAM_FILES\Veeam\Backup and Replication\Backup\Veeam.Backup.ExternalInfrastructure.DbProvider.exe
- CSIDL_PROGRAM_FILESX86\Veeam\Backup Transport\GuestInteraction\VSS\VeeamGuestHelperCtrl.exe
- CSIDL_PROGRAM_FILES\Veeam\Backup and Replication\Backup\Veeam.Backup.Service.exe
- CSIDL_PROGRAM_FILES\Veeam\Backup and Replication\Backup Catalog\Veeam.Backup.CatalogDataService.exe
- CSIDL_PROGRAM_FILES\Veeam\Backup and Replication\Backup\Veeam.Backup.ManagerGCServer.exe
- CSIDL_PROGRAM_FILES\Veeam\Backup and Replication\Backup\Veeam.Backup.Cdp.Service.exe
- CSIDL_PROGRAM_FILES\Veeam\Backup and Replication\Console\veeam.backup.shell.exe
- CSIDL_PROGRAM_FILESX86\Veeam\Backup Transport\x64\VeeamAgent.exe
- CSIDL_PROGRAM_FILES\Veeam\Backup and Replication\Backup\Veeam.Backup.Manager.exe
- CSIDL_WINDOWS\Veeam\Backup\VeeamDeploymentSvc.exe
- vbm.temp
- flat

VMware

Aggiunta di:

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

27 settembre - 2023

Cisco Webex

Aggiunta di:

- CSIDL_LOCAL_APPDATA\Programs\Cisco Spark\CiscoCollabHost.exe

Microsoft OneNote

Aggiunta di:

- CSIDL_LOCAL_APPDATA\Microsoft\OneNote*\cache*.bin

Microsoft SQL Server

Aggiunta di:

- CSIDL_PROGRAM_FILES\Microsoft SQL Server*\MSSQL\Binn\sqlagent.exe
- CSIDL_PROGRAM_FILES\Microsoft SQL Server*\MSSQL\Binn\MsDtsSrvr.exe
- CSIDL_PROGRAM_FILES\Microsoft SQL Server*\Shared\sqlbrowser.exe
- FINESTRA_CSIDL\Cluster\
- CSIDL_PROGRAM_FILES\Microsoft SQL Server*\MSSQL\FTDATA\
- CSIDL_WINDOW\Cluster\clussvc.exe
- CSIDL_WINDOW\Cluster\rhs.exe
- trc

Rimozione di:

- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.11\MSSQL\Binn\SQLServr.exe
- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.11\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\MSSQL\Binn\SQLServr.exe
- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.12\OLAP\Bin\MSMDSrv.exe
- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.12\Reporting Services\ReportServer\Bin\ReportingServicesService.exe
- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.13\MSSQL\Binn\SQLServr.exe
- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.13\OLAP\Bin\MSMDSrv.exe
- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.13\Reporting Services\ReportServer\Bin\ReportingServicesService.exe
- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL*.MSSQLSERVER\MSSQL\Binn\SQLServr.exe
- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSAS*.MSSQLSERVER\OLAP\Bin\MSMDSrv.exe
- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSRS*.MSSQLSERVER\Reporting Services\ReportServer\Bin\ReportingServicesService.exe
- abf
- ctl
- dbf
- rdo

Team Microsoft

Aggiunta di:

- CSIDL_LOCAL_APPDATA\Microsoft\Teams\current\squirrel.exe
- CSIDL_LOCAL_APPDATA\Microsoft\TeamsMeetingAddin

Impostazioni predefinite di Microsoft Windows

Aggiunta di:

- CSIDL_WINDOWS\WinSxS*\TiWorker.exe

Splunk

Aggiunta di:

- CSIDL_PROGRAM_FILES\splunk\bin\splunk.exe
- CSIDL_PROGRAM_FILES\splunk\bin\splunk.

Symantec Endpoint Protection

Aggiunta di:

- CSIDL_PROGRAM_FILES\Symantec\Symantec Endpoint Protection*\Bin64\ccSvcHst.exe
- CSIDL_COMMON_APPDATA\Symantec\Symantec Endpoint Protection\
- CSIDL_PROGRAM_FILESX86\Symantec\Symantec Endpoint Protection*\Bin64\Smc.exe

Rimozione di:

- CSIDL_WINDOWS\Temp\TMP*.tmp
- CSIDL_WINDOWS\Temp\musdmys_*
- CSIDL_WINDOWS\Temp\content.zip.tmp\SymDeltaDecompressOptions.xml
- CSIDL_WINDOWS\Temp\content.zip.tmp*.diff
- CSIDL_WINDOWS\Temp\content.zip.tmp\cur.scr
- CSIDL_COMMON_APPDATA\Symantec

Nuovi elenchi creati

- Zscaler Client Connector
- ManageEngine Endpoint Central
- Protezione dalla perdita di dati Symantec

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).