Alterações da lista de exclusão mantidas pela Cisco para o console do Cisco Secure Endpoint

Contents

Guardião Digital - Mac
Nova lista criada
3 de março - 2021
Kaspersky - Windows
SCCM - Windows
Symantec - Windows
Novas listas criadas
30 de junho - 2021
Padrão do Microsoft Windows
Cliente Citrix ICA
Servidor de Provisionamento Citrix
Novas listas criadas
29 de setembro - 2021
Cisco Webex - Windows
Plano de travamento - Windows
Plano de travamento - Mac
VMware - Windows
23 de março - 2022
Padrão do Microsoft Windows
Hyper-V - Windows
Microsoft Windows Defender - Windows
29 de junho - 2022
Padrão do Microsoft Windows
Cisco AnyConnect VPN
Cisco Webex
Microsoft OneDrive (anteriormente uma unidade)
Tanium - Windows
Servidor de Provisionamento Citrix
Novas listas criadas
14 de setembro - 2022
Padrão do Microsoft Windows
Microsoft SQL Server
TrendMicro / Apex One
Novas listas criadas
Outubro - 2022
14 de dezembro - 2022
Padrão do Microsoft Windows
Alterações no Back-end - Windows
Novas listas criadas
12 de abril - 2023
Padrão do Microsoft Windows
Microsoft Intune
McAfee Trellix SolidCore
Cisco Webex
Microsoft Defender para MacOS
Microsoft Defender para Linux
31 de maio - 2023
VEEAM
VMWare

Introdução

Este documento descreve as alterações adicionadas às Exclusões Mantidas pela Cisco.

As Exclusões Mantidas pela Cisco são criadas e mantidas pela Cisco para fornecer melhor compatibilidade entre o Advanced Malware Protection (AMP) for Endpoints Connector e antivírus, segurança ou outro software; essas exclusões podem ser adicionadas a novas versões de um aplicativo.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Exclusões no AMP para endpoints
- Console AMP

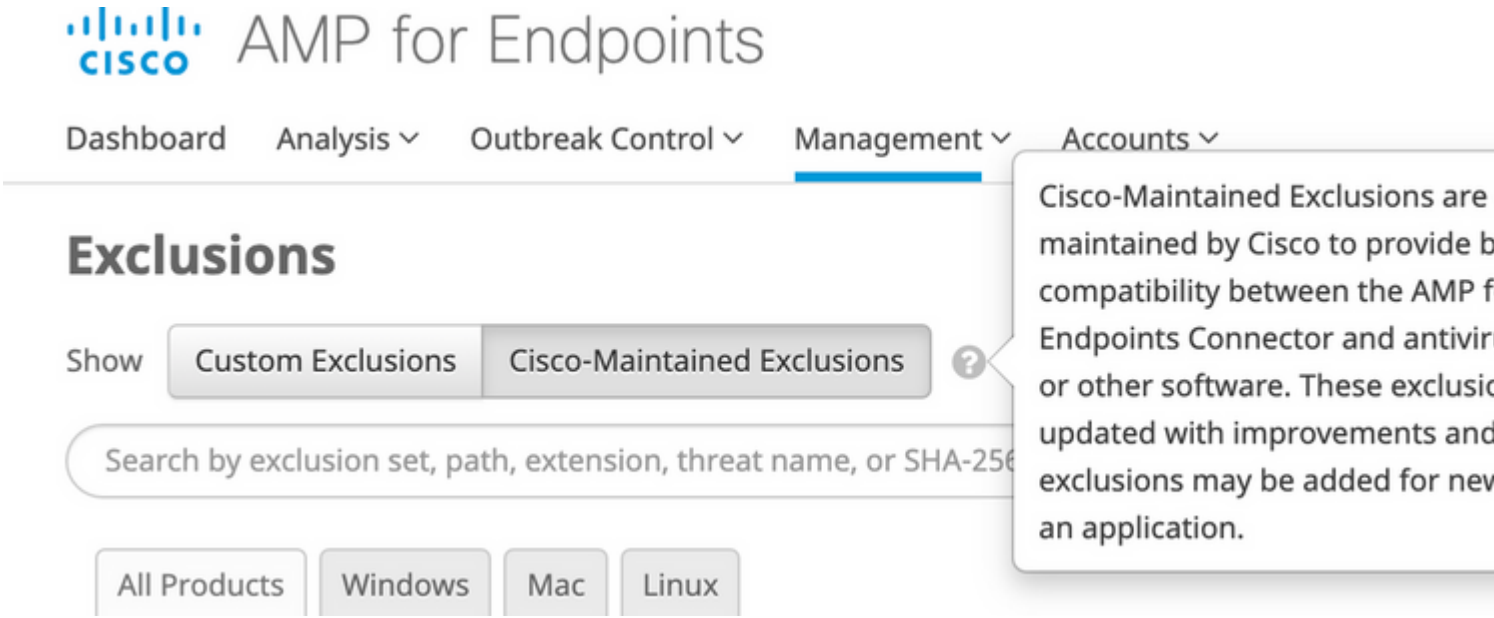
Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Console do AMP para endpoints versão 5.4.20190820

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Expectativas ao atualizar



Quando as listas mantidas pela Cisco são alteradas, ocorre uma atualização de política no back-end para refletir essa alteração. À medida que cada um dos endpoints usa essa lista para fazer check-in em sua pulsação, eles obtêm a política atualizada. Essas alterações de política não são refletidas no log de auditoria, pois é tecnicamente uma alteração na lista de exclusão, não na política em si, e as listas de exclusão mantidas pela Cisco não existem dentro do log de auditoria normal em consoles individuais. Para ambientes de grande escala, isso parece uma enxurrada de atualizações de políticas e o resultado final será um melhor desempenho em cada um dos endpoints.

O período de atualização depende de cada ponto final. Se todas as máquinas estiverem online, as atualizações ocorrerão em 1 a 2 pulsações. Se este for um ambiente global, as atualizações continuarão a ocorrer à medida que as máquinas ficam on-line, portanto,

não se surpreenda ao ver atualizações de política adicionais 24-48 horas após o envio da lista mantida.

Alterações

28 de agosto - 2019

Padrão do Microsoft Windows:

Remoção de:

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

Motivo*:* Repetitivo. Outra exclusão no conjunto de base cobre-o.

Adição de:

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

Motivo: as atualizações do Windows 10 falharam esporadicamente devido a verificações de processo.

Ventos solares N-Able - Windows:

Adição de:

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

Docker - Mac:

Remoção de:

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

Razão: Um teste adicional deixou-nos com preocupações em matéria de segurança, pelo que o desenvolvimento identificou melhores exclusões.

Adição de:

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

Novas listas criadas:

Linux:

- Docker - Conector 1.10.2
- Docker - Conector 1.11+
- Zabbix

Mac:

- Caixa virtual
- Guardião digital

18 de setembro - 2019

Padrão Apple MacOS:

Adição de:

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

McAfee - Mac

Adição de:

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

Cisco Jabber - Mac

Remoção de:

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

Motivo: melhor segurança e a funcionalidade adicional de exclusões baseadas em processos.

Adição de:

- **/Aplicativos/Cisco Jabber.app/Conteúdo/MacOS/Cisco Jabber**

Plano de travamento - Mac

Adição de:

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

JAMF Casper - Mac

Remoção de:

- **/usr/bin/sw_vers**

Motivo: melhor segurança e a funcionalidade adicional de exclusões baseadas em processos.

Adição de:

- **/Biblioteca/Aplicativo Support/JAMF/Jamf.app/Contents/MacOS/JamfDaemon.app/Conteúdo/MacOS/JamfDaemon**
- **/usr/local/jamf/bin/jamfAgent**
- **/usr/local/jamf/bin/jamf**
- **/Biblioteca/Aplicativo Support/JAMF/Jamf.app/Contents/MacOS/JamfAgent.app/Conteúdo/MacOS/JamfAgent**

VMWare Fusion - Mac

Adição de:

- **/Aplicativos/VMware Fusion.app/Conteúdos/MacOS/VMware Fusion**

Xcode - Mac

Adição de:

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

One Drive - Windows

Alteração secundária:

- **C:*\Users\OneDrive** (Adicionada a barra invertida para melhor segurança)

Citrix Cliente ICA - Windows

Adição de:

- **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: atualização recente das exclusões sugeridas pela Citrix.

Novas listas criadas:

Windows

- Servidor de Provisionamento Citrix
- Conector de nuvem da Citrix

11 de dezembro - 2019

One Drive - Windows

Adição de:

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

Splunk - Windows

Adição de:

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

Splunk - Linux

Adição de:

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

Novas listas criadas:

Azure - Linux

Vagrant - Mac

12 de fevereiro - 2020

Padrão do Microsoft Windows - Windows

Adição de:

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

Websense - Windows

Adição de:

- **[Várias Unidades]:\Arquivos De Programas*\Websense**
- **C:\Program Arquivos (x86)\Ponto de Extremidade Websense\Websense\dserui.exe**
- **C:\Program Files\Websense\Websense Endpoint\dserui.exe**
- **C:\Program Arquivos (x86)\Websense\Ponto de Extremidade Websense\EndPointClassifier.exe**
- **C:\Program Arquivos (x86)\Ponto de Extremidade Websense\Websense\FilterSDK\kvoop.exe**
- **C:\Program Arquivos (x86)\Websense\Ponto de Extremidade Websense\wepsvc.exe**

Microsoft SQL Server - Windows

Adição de:

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

10 de junho - 2020

Malwarebytes - Windows

Alteração menor:

- **C:\ProgramData\Malwarebytes Agente de Ponto de Extremidade**
- **C:\ProgramData\Malwarebytes\MBAMService**

Microsoft Office - Windows

Adição de:

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

IIS - Windows

Adição de:

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

Altiris da Symantec - Windows

Adição de:

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

McAfee - Windows

Adição de:

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

Novas listas criadas:

NetScout - Windows

IBM - Windows

15 de julho - 2020

Controladores de Domínio - Windows

Adição de:

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

Equipes da Microsoft - Windows

Adição de:

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

Nova lista criada

Controle Acima

26 de agosto - 2020

**Devido a testes adicionais, a data de lançamento original foi estendida do dia 19 para o dia 26

Microsoft SQL Server - Windows

Substituindo:

- **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**

Adição de:

- **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 de setembro - 2020

Malwarebytes - Windows

Adição de:

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

Guardião Digital - Mac

Adição de:

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

Nova lista criada

Digital Guardian - Windows

3 de março - 2021

Kaspersky - Windows

Adição de:

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

SCCM - Windows

Remoção de:

- **WINDOWS\CCM\ServiceData** - Caminho Duplicado
- **Arquivos de Programas\Microsoft Configuration Manager\EasySetupPayload** - Caminho Duplicado

Symantec - Windows

Adição de:

- **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**

Novas listas criadas

Cisco AnyConnect - Windows

ATP do Microsoft Defender - Windows

30 de junho - 2021

Padrão do Microsoft Windows

Adição de:

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

Cliente Citrix ICA

Adição de:

- **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**

Servidor de Provisionamento Citrix

Remoção de:

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

Adição de:

- **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**

Novas listas criadas

Commvault - Windows

Gravação de sessões do Citrix - Windows

29 de setembro - 2021

Cisco Webex - Windows

Adição de:

- **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_***

Plano de travamento - Windows

Adição de:

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

Plano de travamento - Mac

Adição de:

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

VMware - Windows

Adição de:

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

23 de março - 2022

Padrão do Microsoft Windows

Adição de:

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

Hyper-V - Windows

Adição de:

- **CSIDL_COMMON_APPDATA\Microsoft\Windows\Hyper-V**
- **CSIDL_COMMON_DOCUMENTS\Hyper-V\Discos rígidos virtuais**

Microsoft Windows Defender - Windows

Adição de:

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

29 de junho - 2022

Padrão do Microsoft Windows

Adição de:

- ***.applocker**

Cisco AnyConnect VPN

Adição de:

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

Cisco Webex

Adição de:

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

Microsoft OneDrive (anteriormente uma unidade)

Adição de:

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

Tanium - Windows

Adição de:

- **C:\Program Files (x86)\Tanium\Tanium End User Notification Tools\bin\end-user-notifications.exe**

Servidor de Provisionamento Citrix

Adição de:

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

Remoção de:

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

Novas listas criadas

Pesquisa X1 - Windows

Microsoft Intune - Windows

14 de setembro - 2022

Padrão do Microsoft Windows

Adição de:

- **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

Expandido para incluir V. 2019

Adição de:

- **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*\Shared**

TrendMicro / Apex One

Adição De:

- **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\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

Novas listas criadas

DevOps do Azure - Windows

Outubro - 2022

Até o mês de outubro, as exclusões malformadas que foram introduzidas no ambiente do Secure Endpoint durante as iterações anteriores do produto serão removidas das listas de exclusão personalizadas. Mais informações relacionadas a esta iniciativa podem ser encontradas aqui.

14 de dezembro - 2022

Padrão do Microsoft Windows

Adição de:

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

Alterações no Back-end - Windows

- **csc_ui.exe** adicionado a Exclusões Globais de Prevenção de Exploração para V5 e Controle de Script.

Remoção de: desempenho que afeta exclusões

Novas listas criadas

1Senha - Windows, Mac, Linux

McAfee Trellix SolidCore - Windows

12 de abril - 2023

Padrão do Microsoft Windows

Adição de:

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

Remoção de:

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

Microsoft Intune

Adição de:

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

McAfee Trellix SolidCore

Alteração secundária:

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

Cisco Webex

Adição de:

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

Microsoft Defender para MacOS

Adição de:

- **/Biblioteca/Suporte a aplicativos/Microsoft/Defender/**

Microsoft Defender para Linux

Adição de:

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

31 de maio - 2023

VEEAM

Adição de:

- **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 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

Adição de:

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

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.