Modifications apportées à la liste d'exclusion de Cisco pour Cisco Secure Endpoint Console

Table des matières

26 août - 2020

- Microsoft SQL Server - Windows

30 septembre - 2020

- Octets malveillants - Windows
- Digital Guardian - Mac
- Nouvelle liste créée

3 mars - 2021

- Kaspersky - Windows
- SCCM - Windows
- Symantec - Windows
- Nouvelles listes créées

30 juin - 2021

- Microsoft Windows par défaut
- Client Citrix ICA
- Citrix Provisioning Server
- Nouvelles listes créées

29 septembre - 2021

- Cisco Webex - Windows
- Plan de secours - Windows
- Crashplan - Mac
- VMware - Windows

23 mars - 2022

- Microsoft Windows par défaut
- Hyper-V - Windows
- Microsoft Windows Defender - Windows

29 juin - 2022

- Microsoft Windows par défaut
- VPN Cisco AnyConnect
- Cisco Webex
- Microsoft OneDrive (anciennement One Drive)
- Tanium - Fenêtres
- Citrix Provisioning Server
- Nouvelles listes créées

14 sept. - 2022

- Microsoft Windows par défaut
- Microsoft SQL Server
- TrendMicro / Apex One
- Nouvelles listes créées

Octobre - 2022

14 décembre - 2022

- Microsoft Windows par défaut
- Modifications du serveur principal - Windows
- Nouvelles listes créées

12 avril - 2023

- Microsoft Windows par défaut
- Microsoft Intune
- McAfee Trellix SolidCore
- Cisco Webex
- Microsoft Defender pour MacOS
- Microsoft Defender pour Linux

31 mai - 2023

Introduction

Ce document décrit les modifications apportées aux exclusions maintenues par Cisco.

Les exclusions maintenues par Cisco sont créées et maintenues par Cisco afin d'assurer une meilleure compatibilité entre Advanced Malware Protection (AMP) for Endpoints Connector et les logiciels antivirus, de sécurité ou autres. Ces exclusions peuvent être ajoutées aux nouvelles versions d'une application.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Exclusions dans AMP for Endpoints
- console AMP

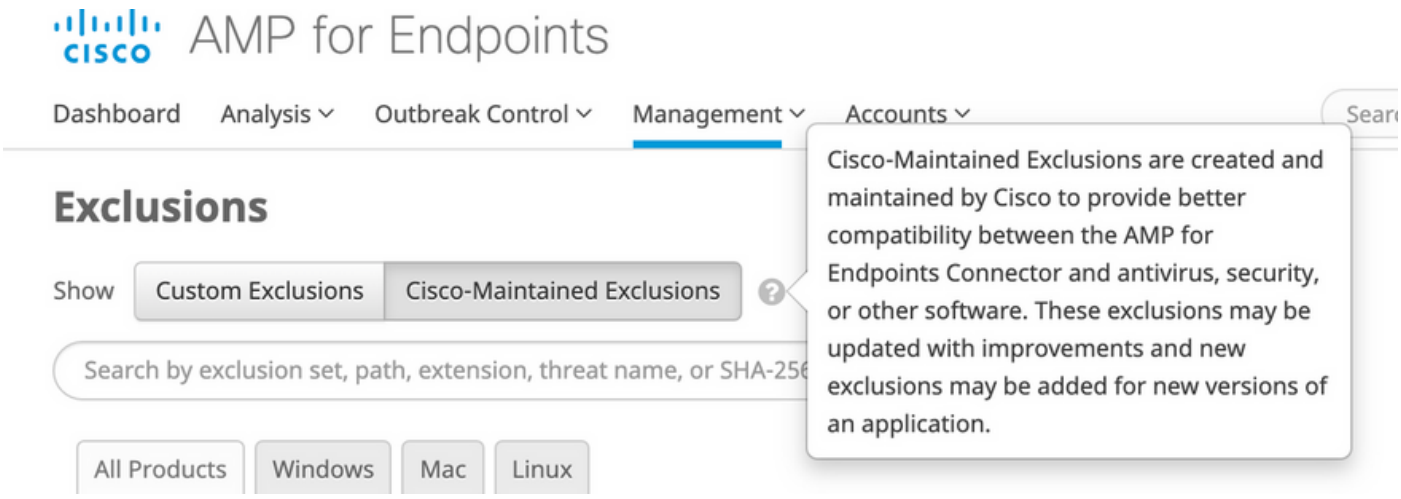
Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Console AMP for Endpoints version 5.4.20190820

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Attentes lors de la mise à jour



Lorsque les listes gérées par Cisco sont modifiées, une mise à jour de la stratégie est effectuée sur le serveur principal pour refléter cette modification. Lorsque chacun des terminaux utilise cette liste pour s'archiver sur leur pulsation, ils extraient la stratégie mise à jour. Ces modifications de stratégie ne sont pas reflétées dans le journal d'audit, car il s'agit techniquement d'une modification de la liste d'exclusion, et non de la stratégie elle-même, et les listes d'exclusion gérées par Cisco n'existent pas dans le journal d'audit normal sur les consoles individuelles. Pour les environnements à grande échelle, cela ressemble à un déluge de mises à jour de politiques et le résultat final sera de meilleures performances sur chacun des terminaux.

La période de mise à jour dépend de chaque terminal. Si toutes les machines sont en ligne, les mises à jour s'effectueront en 1 à 2 pulsations. S'il s'agit d'un environnement global, les mises à jour continuent à se produire lorsque les machines se mettent en ligne. Ne soyez donc pas surpris de voir des mises à jour de stratégie supplémentaires 24 à 48 heures après la diffusion de la liste mise à jour.

Modifications

28 août - 2019

Microsoft Windows par défaut :

Suppression de :

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

Motif : Répétitif. Une autre exclusion de l'ensemble de base le couvre.

Ajout de :

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

Raison : les mises à jour de Windows 10 ont échoué sporadiquement en raison des analyses de processus.

N-Able Solar Winds - Fenêtres :

Ajout de :

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

Docker - Mac :

Suppression de :

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

Motif: Un test supplémentaire nous a laissé avec des préoccupations sur la sécurité donc le développement a identifié de meilleures exclusions.

Ajout de :

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

Nouvelles listes créées :

Linux :

- Docker - Connecteur 1.10.2
- Docker - Connecteur 1.11+
- Zabbix

Mac :

- Boîte virtuelle
- Gardien numérique

18 septembre - 2019

Apple MacOS par défaut :

Ajout de :

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

McAfee - Mac

Ajout de :

- /Library/McAfee/Agent/bin/CmdAgent

Cisco Jabber - Mac

Suppression de :

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

Raison : une meilleure sécurité et la fonctionnalité supplémentaire des exclusions basées sur les processus.

Ajout de :

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

Crashplan - Mac

Ajout de :

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

JAMF Casper - Mac

Suppression de :

- /usr/bin/sw_vers

Raison : une meilleure sécurité et la fonctionnalité supplémentaire des exclusions basées sur les processus.

Ajout de :

- /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

Ajout de :

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

Xcode - Mac

Ajout de :

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

One Drive - Windows

Modification mineure :

- C:*\Users\OneDrive\ (ajout de la barre oblique inverse pour une meilleure sécurité)

Citrix Client ICA - Windows

Ajout 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

Raison : Mise à jour récente des exclusions suggérées par Citrix.

Nouvelles listes créées :

Fenêtres

- Citrix Provisioning Server
- Citrix Cloud Connector

11 décembre - 2019

One Drive - Windows

Ajout de :

- CSIDL_LOCAL_APPDATA\Microsoft\OneDrive\OneDrive.exe

Splunk - Windows

Ajout de :

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

Splunk - Linux

Ajout de :

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

Nouvelles listes créées :

Azure - Linux

Vagabond - Mac

12 février - 2020

Microsoft Windows par défaut - Windows

Ajout de :

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

Websense - Windows

Ajout de :

- [Plusieurs lecteurs]:\Program Files*\Websense\
- C:\Program Fichiers (x86)\Websense\Websense Endpoint\dserui.exe
- C:\Program Files\Websense\Websense Terminal\dserui.exe
- C:\Program Fichiers (x86)\Websense\Websense Endpoint\EndPointClassifier.exe
- C:\Program Fichiers (x86)\Websense\Websense Endpoint\FilterSDK\kvoop.exe
- C:\Program Fichiers (x86)\Websense\Websense Endpoint\wepsvc.exe

Microsoft SQL Server - Windows

Ajout de :

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

10 juin - 2020

Octets malveillants - Windows

Modification mineure :

- C:\ProgramData\Malwarebytes Agent de point d'extrémité\
- C:\ProgramData\Malwarebytes\MBAMService\

Microsoft Office - Windows

Ajout de :

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

IIS - Windows

Ajout de :

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

Altiris de Symantec - Windows

Ajout de :

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

McAfee - Windows

Ajout de :

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

Nouvelles listes créées :

NetScout - Windows

IBM - Windows

15 juillet - 2020

Contrôleurs de domaine - Windows

Ajout de :

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

Microsoft Teams - Windows

Ajout de :

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

Nouvelle liste créée

Contrôle actif

26 août - 2020

**En raison de tests supplémentaires, la date de sortie initiale a été prolongée du 19 au 26

Microsoft SQL Server - Windows

Remplacement :

- 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

Ajout 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 septembre - 2020

Octets malveillants - Windows

Ajout de :

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

Digital Guardian - Mac

Ajout de :

- /usr/local/dgagent
- /dgagent

Nouvelle liste créée

Digital Guardian - Windows

3 mars - 2021

Kaspersky - Windows

Ajout de :

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

SCCM - Windows

Suppression de :

- WINDOWS\CCM\ServiceData - Chemin dupliqué
- Program Files\Microsoft Configuration Manager\EasySetupPayload - Chemin dupliqué

Symantec - Windows

Ajout 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\12.1.608.6300.105\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

Nouvelles listes créées

Cisco AnyConnect - Windows

Microsoft Defender ATP - Windows

30 juin - 2021

Microsoft Windows par défaut

Ajout de :

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

Client Citrix ICA

Ajout 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\

Citrix Provisioning Server

Suppression de :

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

Ajout 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

Nouvelles listes créées

Commvault - Windows

Enregistrement de sessions Citrix - Windows

29 septembre - 2021

Cisco Webex - Windows

Ajout 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_*\

Plan de secours - Windows

Ajout de :

- CSIDL_PROGRAM_FILES\Code42\Code42Service.exe

Crashplan - Mac

Ajout de :

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

VMware - Windows

Ajout de :

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

23 mars - 2022

Microsoft Windows par défaut

Ajout de :

- C:\Windows\System32\SearchIndexer.exe

Hyper-V - Windows

Ajout de :

- CSIDL_COMMON_APPDATA\Microsoft\Windows\Hyper-V\
- CSIDL_COMMON_DOCUMENTS\Hyper-V\Disques durs virtuels\

Microsoft Windows Defender - Windows

Ajout de :

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

29 juin - 2022

Microsoft Windows par défaut

Ajout de :

- *.applocker

VPN Cisco AnyConnect

Ajout de :

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

Cisco Webex

Ajout de :

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

Microsoft OneDrive (anciennement One Drive)

Ajout de :

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

Tanium - Fenêtres

Ajout de :

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

Citrix Provisioning Server

Ajout de :

- CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\MgmtDaemon.com

Suppression de :

- CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\MgmntDaemon.com

Nouvelles listes créées

Recherche X1 - Windows

Microsoft Intune - Windows

14 sept. - 2022

Microsoft Windows par défaut

Ajout 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\appidpolicy converter.exe

Microsoft SQL Server

Étendu pour inclure V. 2019

Ajout 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

Ajout 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

Nouvelles listes créées

Azure DevOps - Windows

Octobre - 2022

Au cours du mois d'octobre, les exclusions malformées introduites dans l'environnement Secure Endpoint au cours des précédentes itérations du produit seront supprimées des listes d'exclusions personnalisées. Vous trouverez de plus amples renseignements sur cette initiative ici.

14 décembre - 2022

Microsoft Windows par défaut

Ajout de :

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

Modifications du serveur principal - Windows

- csc_ui.exe ajouté à Exclusions globales de prévention des exploits pour V5 et le contrôle de script.

Suppression des exclusions ayant une incidence sur les performances

Nouvelles listes créées

1Mot de passe - Windows, Mac, Linux

McAfee Trellix SolidCore - Windows

12 avril - 2023

Microsoft Windows par défaut

Ajout de :

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

Suppression de :

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

Microsoft Intune

Ajout de :

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

McAfee Trellix SolidCore

Modification mineure :

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

Cisco Webex

Ajout de :

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

Microsoft Defender pour MacOS

Ajout de :

- /Bibliothèque/Prise en charge des applications/Microsoft/Defender/

Microsoft Defender pour Linux

Ajout de :

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

31 mai - 2023

VEEAM

Ajout 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\Sauvegarde et réplication\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
- .plat

VMWare

Ajout de :

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

27 septembre - 2023

Cisco Webex

Ajout de :

- CSIDL_LOCAL_APPDATA\Programs\Cisco Spark\CiscoCollabHost.exe

Microsoft OneNote

Ajout de :

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

Microsoft SQL Server

Ajout de :

- 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
- CSIDL_WINDOW\Cluster\
- CSIDL_PROGRAM_FILES\Microsoft SQL Server*\MSSQL\FTDATA\
- CSIDL_WINDOW\Cluster\clussvc.exe
- CSIDL_WINDOW\Cluster\rhs.exe
- .trc

Suppression de :

- 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

Microsoft Teams

Ajout de :

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

Microsoft Windows par défaut

Ajout de :

- CSIDL_WINDOWS\WinSxS*\TiWorker.exe

Splunk

Ajout de :

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

Symantec Endpoint Protection

Ajout de :

- 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

Suppression de :

- 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\

Nouvelles listes créées

- Connecteur client Zscaler
- Gestion du moteur Endpoint Central
- Protection Symantec contre la perte de données

22 novembre - 2023

Microsoft Windows par défaut

Ajout de :

- CSIDL_PROGRAM_FILES\Cisco\Orbital\python\python.exe

Client Citrix ICA

Ajout de :

- CSIDL_PROGRAM_FILESX86\Citrix\ICA Client\SelfServicePlugin\SelfService.exe
- CSIDL_PROGRAM_FILESX86\Citrix\ICA Client\SelfServicePlugin\SelfServicePlugin.exe
- CSIDL_PROGRAM_FILESX86\Citrix\ICA Client\Receiver\FeatureFlag\CWAFeatureFlagUpdater.exe
- CSIDL_PROGRAM_FILESX86\Citrix\ICA Client\wfcrun32.exe
- CSIDL_PROGRAM_FILESX86\Citrix\ICA Client\Receiver\Receiver.exe

Nouvelles listes créées

- Ivanti LANDesk
- Agent Atera

24 janvier - 2024

Microsoft SQL Server et Azure DevOps ont nécessité des ajustements mineurs liés aux modifications du traitement des exclusions pour Windows Endpoint 8.2.1+. Aucune exclusion n'a été ajoutée.

Nouvelle liste créée

- loup arctique

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.