

Cisco Secure Endpoint Console에 대한 Cisco 유지 관리 제외 목록 변경 사항

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[업데이트 시 기대치](#)

[변경 사항](#)

[2019년 8월 28일](#)

[Microsoft Windows 기본값:](#)

[N-Able Solar Winds - 창:](#)

[도커 - Mac:](#)

[새로 만든 목록:](#)

[2019년 9월 18일](#)

[Apple MacOS 기본값:](#)

[McAfee - Mac](#)

[Cisco Jabber - Mac](#)

[크래쉬플랜 - Mac](#)

[JAMF 캐스퍼 - Mac](#)

[VMWare Fusion - Mac](#)

[Xcode - Mac](#)

[단일 드라이브 - Windows](#)

[Citrix ICA 클라이언트 - Windows](#)

[새로 만든 목록:](#)

[2019년 12월 11일](#)

[단일 드라이브 - Windows](#)

[Splunk - Windows](#)

[Splunk - Linux](#)

[새로 만든 목록:](#)

[2020년 2월 12일](#)

[Microsoft Windows 기본값 - Windows](#)

[Websense - Windows](#)

[Microsoft SQL Server - Windows](#)

[2020년 6월 10일](#)

[Malwarebytes - Windows](#)

[마이크로소프트 오피스 - 윈도우](#)

[IIS - Windows](#)

[Symantec의 Altiris - Windows](#)

[McAfee - Windows](#)

[새로 만든 목록:](#)

[2020년 7월 15일](#)

[도메인 컨트롤러 - Windows](#)

[Microsoft 팀 - Windows](#)

[새 목록 생성됨](#)

[2020년 8월 26일](#)

[Microsoft SQL Server - Windows](#)

[2020년 9월 30일](#)

[Malwarebytes - Windows](#)

[Digital Guardian - Mac](#)

[새 목록 생성됨](#)

[2021년 3월 3일](#)

[카스퍼스키 - Windows](#)

[SCCM - Windows](#)

[Symantec - Windows](#)

[새로 만든 목록](#)

[2021년 6월 30일](#)

[Microsoft Windows 기본값](#)

[Citrix ICA 클라이언트](#)

[Citrix Provisioning 서버](#)

[새로 만든 목록](#)

[2021년 9월 29일](#)

[Cisco Webex - Windows](#)

[Crashplan - Windows](#)

[크래쉬플랜 - Mac](#)

[VMware - Windows](#)

[2022년 3월 23일](#)

[Microsoft Windows 기본값](#)

[Hyper-V - Windows](#)

[Microsoft Windows Defender - Windows](#)

[2022년 6월 29일](#)

[Microsoft Windows 기본값](#)

[Cisco AnyConnect VPN](#)

[Cisco Webex](#)

[Microsoft OneDrive\(이전 드라이브 1개\)](#)

[Tanium - Windows](#)

[Citrix Provisioning 서버](#)

[새로 만든 목록](#)

[2022년 9월 14일](#)

[Microsoft Windows 기본값](#)

[Microsoft SQL Server](#)

[TrendMicro/Apex One](#)

[새로 만든 목록](#)

[2022년 10월 - 10월](#)

[2022년 12월 14일](#)

[Microsoft Windows 기본값](#)

[백엔드 변경 사항 - Windows](#)

[새로 만든 목록](#)

[2023년 4월 12일](#)

[Microsoft Windows 기본값](#)

[Microsoft Intune](#)

[McAfee Trellix 솔리드 코어](#)

[Cisco Webex](#)

[MacOS용 Microsoft Defender](#)

[Linux용 Microsoft Defender](#)

[2023년 5월 31일 ~ 5월 31일](#)

[비안](#)

[VMware](#)

[2023년 9월 27일](#)

[Cisco Webex](#)

[Microsoft OneNote](#)

[Microsoft SQL Server](#)

[Microsoft 팀](#)

[Microsoft Windows 기본값](#)

[스플링크](#)

[Symantec 엔드포인트 보호](#)

[새로 만든 목록](#)

[2023년 11월 22일](#)

[Microsoft Windows 기본값](#)

[Citrix ICA 클라이언트](#)

[새로 만든 목록](#)

[2024년 1월 24일](#)

[새 목록 생성됨](#)

소개

이 문서에서는 Cisco-Maintained Exclusions에 추가된 변경 사항에 대해 설명합니다.

Cisco-Maintained Exclusions(Cisco 유지 관리 제외)는 AMP(Advanced Malware Protection) for Endpoints Connector와 안티바이러스, 보안 또는 기타 소프트웨어 간의 더 나은 호환성을 제공하기 위해 Cisco에서 생성하고 유지 관리하며, 이러한 제외 항목을 애플리케이션의 새 버전에 추가할 수 있습니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- AMP for Endpoints의 제외 항목
- AMP 콘솔

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- AMP for Endpoints 콘솔 버전 5.4.20190820

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

업데이트 시 기대치

Exclusions

Show Custom Exclusions Cisco-Maintained Exclusions ?

Search by exclusion set, path, extension, threat name, or SHA-256

All Products Windows Mac Linux

Cisco-Maintained Exclusions are created and maintained by Cisco to provide better compatibility between the AMP for Endpoints Connector and antivirus, security, or other software. These exclusions may be updated with improvements and new exclusions may be added for new versions of an application.

Cisco 유지 보수 목록이 변경되면 변경 사항을 반영하기 위해 백엔드에서 정책 업데이트가 수행됩니다. 각 엔드포인트가 해당 목록을 사용하여 하트비트에 체크 인하면 업데이트된 정책을 가져옵니다. 이러한 정책 변경은 정책 자체가 아니라 제외 목록의 변경이므로 감사 로그에 반영되지 않으며, Cisco에서 유지 관리하는 제외 목록은 개별 콘솔의 일반 감사 로그 내에 존재하지 않습니다. 대규모 환경에서는 정책 업데이트가 폭주하는 것처럼 보이며, 최종 결과는 각 엔드포인트의 성능이 향상됩니다.

업데이트 기간은 각 엔드포인트에 따라 다릅니다. 모든 시스템이 온라인 상태이면 1~2개의 하트비트 내에서 업데이트가 이루어집니다. 글로벌 환경인 경우 시스템이 온라인 상태가 되면 업데이트가 계속 발생하므로 유지 관리 목록이 푸시된 후 24~48시간 내에 추가 정책 업데이트를 확인해도 놀라지 않습니다.

변경 사항

2019년 8월 28일

Microsoft Windows 기본값:

제거:

- CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\ledb*.log
- CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Res1.log을 참조하십시오.
- CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Res2.log을 참조하십시오.

이유: 반복 베이스 세트의 또 다른 제외 사항은 그것을 포함합니다.

추가:

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

이유: 프로세스 검사 때문에 Windows 10 업데이트가 간헐적으로 실패했습니다.

N-Able Solar Winds - 창:

추가:

- C:\Program 파일(x86)\N지원 기술\Windows 에이전트\bin\agent.exe

- C:\Program 파일(x86)\BeAnywhere 지원 Express\GetSupportService_N-Central\BASupSrv.exe
- C:\Program 파일(x86)\N포 Technologies\PatchManagement\ThirdPartyPatch\ThirdPartyPatch.exe

도커 - Mac:

제거:

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

이유: 추가 테스트로 인해 보안에 대한 우려가 생겨서 개발에서는 더 나은 제외 사항을 정확히 찾아냈습니다.

추가:

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

새로 만든 목록:

Linux:

- Docker - 커넥터 1.10.2
- Docker - 커넥터 1.11+
- 자브릭스

Mac:

- 가상 박스
- 디지털 가디언

2019년 9월 18일

Apple MacOS 기본값:

추가:

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

McAfee - Mac

추가:

- /Library/McAfee/Agent/bin/CmdAgent

Cisco Jabber - Mac

제거:

- /usr/bin/grep
- /bin/ps

이유: 더 우수한 보안 및 프로세스 기반 제외의 추가 기능

추가:

- /애플리케이션/Cisco Jabber.app/콘텐츠/MacOS/Cisco Jabber

크래쉬플랜 - Mac

추가:

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

JAMF 캐스퍼 - Mac

제거:

- /usr/bin/sw_vers

이유: 더 우수한 보안 및 프로세스 기반 제외의 추가 기능

추가:

- /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

추가:

- /애플리케이션/VMware Fusion.app/콘텐츠/MacOS/VMware Fusion

Xcode - Mac

추가:

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

단일 드라이브 - Windows

사소한 변경:

- C:*Users\OneDrive\ (보안 강화를 위해 백슬래시를 추가함)

Citrix ICA 클라이언트 - Windows

추가:

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

이유: Citrix의 최근 업데이트에서 제외가 제안되었습니다.

새로 만든 목록:

창

- Citrix Provisioning 서버
- Citrix 클라우드 커넥터

2019년 12월 11일

단일 드라이브 - Windows

추가:

- CSIDL_LOCAL_APPDATA\Microsoft\OneDrive\OneDrive.exe을 참조하십시오.

Splunk - Windows

추가:

- CSIDL_PROGRAM_FILE\splunkforwarder\bin\splunk-winevtlog.exe을 참조하십시오.
- CSIDL_PROGRAM_FILE\splunkforwarder\bin\splunkd.exe을 참조하십시오.

Splunk - Linux

추가:

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

새로 만든 목록:

Azure - Linux

Vagrant - Mac

2020년 2월 12일

Microsoft Windows 기본값 - Windows

추가:

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

Websense - Windows

추가:

- [여러 드라이브]:\Program Files*\Websense\
• C:\Program 파일(x86)\Websense\Websense 엔드포인트\dserui.exe
• C:\Program Files\Websense\Websense 엔드포인트\dserui.exe
• C:\Program 파일(x86)\Websense\Websense 엔드포인트\EndPointClassifier.exe
• C:\Program 파일(x86)\Websense\Websense 엔드포인트\FilterSDK\kvoop.exe
• C:\Program 파일(x86)\Websense\Websense 엔드포인트\wepsvc.exe

Microsoft SQL Server - Windows

추가:

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

2020년 6월 10일

Malwarebytes - Windows

사소한 변경:

- C:\ProgramData\Malwarebytes 엔드포인트 에이전트\
• C:\ProgramData\Malwarebytes\MBAMService\

마이크로소프트 오피스 - 윈도우

추가:

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

IIS - Windows

추가:

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

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

Symantec의 Altiris - Windows

추가:

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

McAfee - Windows

추가:

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

새로 만든 목록:

NetScout - 창

IBM - Windows

2020년 7월 15일

도메인 컨트롤러 - Windows

추가:

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

Microsoft 팀 - Windows

추가:

- CSIDL_LOCAL_APPDATA\Microsoft\Teams\current\teams.exe을 참조하십시오.
- CSIDL_LOCAL_APPDATA\Microsoft\Teams\update.exe을 참조하십시오.

새 목록 생성됨

위로 제어

2020년 8월 26일

**추가 검사로 원래 출시일이 19일에서 26일로 연장됐다

Microsoft SQL Server - Windows

교체:

- 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

추가:

- 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

2020년 9월 30일

Malwarebytes - Windows

추가:

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

Digital Guardian - Mac

추가:

- /usr/local/dgagent
- /dgagent

새 목록 생성됨

디지털 보호 - Windows

2021년 3월 3일

카스퍼스키 - Windows

추가:

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

SCCM - Windows

제거:

- WINDOWS\CCM\ServiceData - 중복 경로
- 프로그램 파일\Microsoft Configuration Manager\EasySetupPayload - 중복 경로

Symantec - Windows

추가:

- CSIDL_PROGRAM_FILES\Symantec\Endpoint Agent\ledpa.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

새로 만든 목록

Cisco AnyConnect - Windows

Microsoft Defender ATP - Windows

2021년 6월 30일

Microsoft Windows 기본값

추가:

- CSIDL_WINDOWS\System32\GroupPolicy\User\registry.pol을 참조하십시오.
- CSIDL_WINDOWS\System32\GroupPolicy\Machine\registry.pol을 참조하십시오.

Citrix ICA 클라이언트

추가:

- CSIDL_PROGRAM_FILES\Citrix\Broker\Service\BrokerService.exe을 참조하십시오.
- CSIDL_PROGRAM_FILES\Citrix\Broker\Service\HighAvailabilityService.exe을 참조하십시오.
- CSIDL_PROGRAM_FILES\Citrix\ConfigSync\ConfigSyncService.exe을 참조하십시오.
- CSIDL_PROGRAM_FILESX86\Citrix\ICA 클라이언트\

Citrix Provisioning 서버

제거:

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

추가:

- CSIDL_WINDOWS\System32\drivers\CfsDep2.sys을 참조하십시오.
- CSIDL_WINDOWS\System32\drivers\CvhdBusP6.sys을 참조하십시오.
- CSIDL_WINDOWS\System32\drivers\CVhdMp.sys을 참조하십시오.
- 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\MgmtDaemon.exe
- CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\BNPXE.exe
- CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\BNDevice.exe

새로 만든 목록

Commvault - Windows

Citrix 세션 녹음 - Windows

2021년 9월 29일

Cisco Webex - Windows

추가:

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

Crashplan - Windows

추가:

- CSIDL_PROGRAM_FILES\Code42\Code42Service.exe

크래쉬플랜 - Mac

추가:

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

VMware - Windows

추가:

- CSIDL_PROGRAM_FILEESX86\VMware\VMware DataS Agent\service\DataSAgent.exe

2022년 3월 23일

Microsoft Windows 기본값

추가:

- C:\Windows\System32\SearchIndexer.exe

Hyper-V - Windows

추가:

- CSIDL_COMMON_APPDATA\Microsoft\Windows\Hyper-V\을 참조하십시오.
- CSIDL_COMMON_DOCUMENTS\Hyper-V가상 하드 디스크\

Microsoft Windows Defender - Windows

추가:

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

2022년 6월 29일

Microsoft Windows 기본값

추가:

- *.applocker

Cisco AnyConnect VPN

추가:

- CSIDL_PROGRAM_FILEESX86\Cisco\Cisco AnyConnect Secure Mobility Client\acwebhelper.exe

Cisco Webex

추가:

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

Microsoft OneDrive(이전 드라이브 1개)

추가:

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

Tanium - Windows

추가:

- C:\Program 파일 (x86)\Tanium\Tanium 최종 사용자 알림 도구\bin\end-user-notifications.exe

Citrix Provisioning 서버

추가:

- CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\MgmtDaemon.com

제거:

- CSIDL_PROGRAM_FILES\Citrix\Provisioning Services\MgmtDaemon.com

새로 만든 목록

X1 검색 - Windows

Microsoft Intune - Windows

2022년 9월 14일

Microsoft Windows 기본값

추가:

- CSIDL_PROGRAM_FILESX86\Cisco\Cisco Secure Client\
- CSIDL_PROGRAM_FILEESX86\Cisco\Cisco Secure Client\UI\acumbrellaagent.exe
- CSIDL_PROGRAM_FILESX86\Cisco\Cisco Secure Client\UI\acumbrellaagent.exencrypt-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_cmud.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

V. 2019를 포함하도록 확장됨

추가:

- 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

다음에 대한 추가:

- CSIDL_PROGRAM_FILESX86\Trend Micro\Security Agent\CCSF\TMCSF.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\Nttrtscan.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\ESServiceShell.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\TmsalInstance64.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

새로 만든 목록

Azure DevOps - Windows

2022년 10월 - 10월

10월 한 달 동안 제품이 이전에 반복될 때 Secure Endpoint 환경에 도입된 형식이 잘못된 제외는 사용자 지정 제외 목록에서 제거됩니다. 이 이니셔티브와 관련된 자세한 내용은 여기에서 확인할 수 [있습니다](#).

2022년 12월 14일

Microsoft Windows 기본값

추가:

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

백엔드 변경 사항 - Windows

- csc_ui.exe V5 및 스크립트 제어를 위한 Exploit Prevention Global Exclusions에 추가되었습니다.

제거: 성능에 [영향을 주는 제외](#)

새로 만든 목록

1비밀번호 - Windows, Mac, Linux

McAfee Trellix 솔리드 코어 - Windows

2023년 4월 12일

Microsoft Windows 기본값

추가:

- .pf
- CSIDL_PROGRAM_FILEESX86\Cisco\Cisco Secure Client\acumbrellaagent.exe

제거:

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

Microsoft Intune

추가:

- CSIDL_PROGRAM_FILESX86\Microsoft Intune 관리 확장
Microsoft.Management.Services.IntuneWindowsAgent.exe

McAfee Trellix 솔리드 코어

사소한 변경:

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

Cisco Webex

추가:

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

MacOS용 Microsoft Defender

추가:

- /Library/Application Support/Microsoft/Defender/

Linux용 Microsoft Defender

추가:

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

2023년 5월 31일 ~ 5월 31일

비암

추가:

- CSIDL_PROGRAM_FILES\Common Files\Veeam\Backup and Replication\Explorer 복구 서
비스\Veeam.StandBy.Service.exe
- CSIDL_PROGRAM_FILES\공통 파일\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.exe을 참조하십시오.
- .vbm.temp
- .flat

VMware

추가:

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

2023년 9월 27일

Cisco Webex

추가:

- CSIDL_LOCAL_APPDATA\Programs\Cisco Spark\CiscoCollabHost.exe

Microsoft OneNote

추가:

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

Microsoft SQL Server

추가:

- 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\클러스터\

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

제거:

- 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 팀

추가:

- CSIDL_LOCAL_APPDATA\Microsoft\Teams\current\squirrel.exe을 참조하십시오.
- CSIDL_LOCAL_APPDATA\Microsoft\TeamsMeetingAddin

Microsoft Windows 기본값

추가:

- CSIDL_WINDOWS\WinSxS*\TiWorker.exe

스플링크

추가:

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

Symantec 엔드포인트 보호

추가:

- 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

제거:

- 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\

새로 만든 목록

- Zscaler 클라이언트 커넥터
- ManageEngine Endpoint Central
- Symantec 데이터 손실 보호

2023년 11월 22일

Microsoft Windows 기본값

추가:

- CSIDL_PROGRAM_FILES\Cisco\Orbital\python\python.exe을 참조하십시오.

Citrix ICA 클라이언트

추가:

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

새로 만든 목록

- 이반티 랜드
- Atera 에이전트

2024년 1월 24일

Microsoft SQL Server 및 Azure DevOps는 Windows Endpoint 8.2.1+에 대한 제외 처리 변경과 관련된 약간의 조정이 필요했습니다. 제외가 추가되지 않았습니다.

새 목록 생성됨

- 복극 늑대

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.