Eliminación de exclusiones de Windows obsoletas de Cisco Secure Endpoint

Contenido

[Introducción](#)
[Descripción de problemas](#)
[Pasos adicionales](#)

Introducción

Este documento describe el proceso planeado para eliminar exclusiones mal formadas comunes del entorno de cliente de Windows Secure Endpoint.

Descripción de problemas

En un esfuerzo continuo por minimizar el impacto en el rendimiento y maximizar la funcionalidad de Cisco Secure Endpoint, nuestros ingenieros han identificado las exclusiones obsoletas más frecuentes presentes en nuestro entorno de cliente y las eliminarán durante el mes de octubre de 2022. Las iteraciones anteriores de Secure Endpoint (6.x y anteriores) dependían de la funcionalidad de comodines (*) para utilizar exclusiones de varias unidades. Los cambios y mejoras posteriores en la definición y la entrada de exclusión eliminaron la necesidad de un formato tan amplio y las exclusiones mantenidas por Cisco se ajustaron para abordar el impacto en el rendimiento que los comodines crearon. Con el lanzamiento de Windows Secure Endpoint 7.5.3, una nueva función permitía las exclusiones de procesos con caracteres comodín (*), lo que cambiaba la gestión de las exclusiones con asteriscos y causaba un aumento en el consumo de CPU para los clientes que aún tenían las siguientes exclusiones en su entorno:

```
*\Windows\Security\database\*.sdb
*\Windows\Security\database\*.edb
*\Windows\Security\database\*.chk
*\Windows\SoftwareDistribution\Datastore\Logs\*.log
*\Windows\Security\database\*.jrs
*\Windows\Security\database\*.log
*\Windows\Temp\content.zip.tmp\*.diff
*\Windows\Temp\content.zip.tmp\cur.scr
*\Windows\Temp\TMP*.tmp
*\Windows\Temp\musdmys_*
*\Windows\Temp\content.zip.tmp\SymDeltaDecompressOptions.xml
*.sas*
*\Windows\SoftwareDistribution\Datastore\Logs\edb*.log
*\System Volume Information\tracking.log
*\Program Files (x86)\SysTrack\LsiAgent\Condense\*\*\*.tmp
*\Program Files (x86)\SysTrack\LsiAgent\Condense\*\*.hld
*\Windows\Temp\AltirisScript*.cmd
*\Windows\System32\drivers\*-*.tmp
*\Users\*\AppData\Local\Temp\*-*.tmp
```

```
*\Users\*\AppData\Local\Temp\warsaw_*
*\Windows\Temp\warsaw_*
*Windows\SoftwareDistribution\Datastore\Logs\*.log
*\Windows\System32\Dns\*.dns
*\Windows\System32\DNS\*.scc
*\Windows\ntds\EDB*.log
*\Windows\ntds\Edbres*.jrs
*\Windows\ntds\*.pat
*\Windows\SoftwareDistribution\Datastore\Logs\edb.log
*Windows\Temp\mus*
*Windows\Temp\content.zip.tmp*
```

Pasos adicionales

La eliminación de estas exclusiones no tiene un impacto negativo en su entorno y puede aumentar el rendimiento en los hosts que utilizan Windows Secure Endpoint 7.5.3 y versiones posteriores. Revise las listas de exclusión personalizadas actuales para ver si hay exclusiones de Asterisk (*) y modifíquelas para usar la funcionalidad de "aplicar a todas las letras de unidad" disponible para comodines si necesita varias unidades, o proporcione una letra de unidad en la ruta si no la necesita. Si utiliza alguno de los siguientes software, asegúrese de agregar la lista de mantenimiento de Cisco a la política, ya que ya se han establecido las exclusiones correctas para su uso:

- Predeterminado de Microsoft Windows
- Altiris de Symantec
- Controlador de dominio
- Diebold Varsovia
- Software Lakeside - Systrack
- Aplicaciones SAS
- Symantec

> **Nota**: si su organización tiene dudas sobre la congelación de cambios, abra un caso TAC y consulte este artículo a **más tardar el 7 de octubre de 2022.**

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).