Configurar e identificar exclusões do Cisco Secure Endpoint

Contents

Introduction

Este documento descreve as práticas recomendadas para localizar e criar exclusões no Secure Endpoint.

Contribuição dos engenheiros da Cisco.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso ao console do Secure Endpoint
- Conta com privilégios de Administrador
- Um conhecimento prático do ambiente do cliente.

Componentes Utilizados

As informações neste documento são baseadas nos sistemas operacionais Windows, Linux e MacOS.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Como entender as exclusões

Um conjunto de exclusões é uma lista de diretórios, extensões de arquivos ou nomes de ameaças que você não deseja que o Conector de Ponto de Extremidade Seguro examine ou condene. As exclusões são uma necessidade para garantir o equilíbrio entre desempenho e segurança em uma máquina quando a proteção de endpoint, como o Secure Endpoint, está habilitada. Este artigo descreve exclusões para Secure Endpoint Cloud, TETRA, SPP e MAP.

Cada ambiente é único, bem como a entidade que o controla, variando de políticas rigorosas a abertas, onde estas últimas seriam classificadas como um pote de mel. Como tais exclusões são definidas deve ser exclusivamente adaptado a cada situação.

Diferentes exclusões podem ser categorizadas de duas maneiras, **exclusões óbvias** e **exclusões indistintas**.

Exclusões óbvias

Exclusões óbvias são exclusões que foram criadas com base em pesquisa e teste para sistemas operacionais, programas e outros softwares de segurança usados com frequência. Essas exclusões podem ser encontradas na Lista de exclusões mantida pela Cisco em seu console.

> **Observação**: é recomendável entrar em contato com outros fornecedores de antivírus (AV) e solicitar que suas exclusões recomendadas sejam adicionadas. Isso garante que o Secure Endpoint e o AV funcionem em conjunto e também minimizem o impacto no desempenho.

Exclusões Indistintas

É recomendável criar uma política duplicada para evitar preocupações e interrupções de segurança da empresa para identificar Computadores com indicadores de problemas de desempenho e separá-los em um grupo para usar essa política duplicada.

> **Cuidado**: as alterações de configuração no painel exigem tempo para permitir que os conectores sincronizem a política. Permita uma atualização de pulsação ou sincronize manualmente as políticas nos conectores.

Criação de política

1. **Secure Endpoint Console > Guia Management > Policies**
2. Clique em **+ Nova política...**

3. **Selecione** no menu suspenso do sistema operacional.
4. Forneça um nome significativo para permitir que você diferencie essa política e descrição (*opcional*).
5. Selecione as ações de política de acordo com seus requisitos e use as exclusões padrão por enquanto.
6. Importante: Em **Advanced Settings > Administrative Features,** defina o Connector log level como **Debug**.
7. Clique em **Salvar** para concluir a criação da diretiva.

Criação de grupo

1. **Secure Endpoint Console > guia Management > Groups (Gerenciamento > Grupos)**
2. Clique em **Criar grupo**
3. Forneça um nome significativo para permitir que você diferencie esse grupo e a descrição (*opcional*).
4. **Selecione** a política duplicada criada.
5. Clique em **Salvar** para concluir a criação do grupo.

Como identificar exclusões

Após a criação de políticas e grupos duplicados, com o **nível de log de depuração nos conectores** execute os *Computadores* de acordo com as operações comerciais normais. Aguarde um tempo para obter dados suficientes de log do conector enquanto os programas e processos são acessados, gere um pacote de diagnóstico de suporte para revisar e identificar exclusões.

Guia para criar pacotes de diagnóstico para diferentes sistemas operacionais disponíveis:

- Windows
- Linux
- MAC

MacOS ou Linux

Extraia o pacote de diagnóstico de depuração compactado. O arquivo **fileops.txt** A lista os caminhos onde os arquivos criam, modificam e renomeam atividades acionadas pelo Secure Endpoint para executar varreduras de arquivos. Cada caminho tem uma contagem associada que indica quantas vezes ele foi examinado e a lista é classificada em ordem decrescente. Embora uma contagem alta não signifique necessariamente que o caminho deve ser excluído (por exemplo, um diretório que armazena e-mails pode ser varrido com frequência, mas não deve ser excluído), a lista fornece um ponto de partida para identificar candidatos à exclusão.

```
31 /Users/eugene/Library/Cookies/Cookies.binarycookies
24 /Users/eugene/.zhistory
9 /Users/eugene/.vim/.temp/viminfo
9 /Library/Application Support/Apple/ParentalControls/Users/eugene/2018/05/10-usage.data
5 /Users/eugene/Library/Cookies/HSTS.plist
5 /Users/eugene/.vim/.temp/viminfo.tmp
4 /Users/eugene/Library/Metadata/CoreSpotlight/index.spotlightV3/tmp.spotlight.state
3 /Users/eugene/Library/WebKit/com.apple.Safari/WebsiteData/ResourceLoadStatistics/full_browsir
3 /Library/Logs/Cisco/supporttool.log
2 /private/var/db/locationd/clients.plist
2 /Users/eugene/Desktop/.DS_Store
2 /Users/eugene/.dropbox/instance1/config.dbx
2 /Users/eugene/.DS_Store
2 /Library/Catacomb/DD94912/biolockout.cat
2 /.fseventsd/000000000029d66b
```

```
1 /private/var/db/locationd/.dat.nosync0063.arg4tq
```

Windows

O sistema operacional Windows é mais complicado, mais opções de exclusão estão disponíveis devido aos processos pai e filho. Isso indica que uma análise mais profunda é necessária para identificar os arquivos que foram acessados, mas também os programas que os geraram. Consulte esta Ferramenta de Ajuste do Windows na página GitHub da Cisco Security para obter mais detalhes sobre como analisar e otimizar o desempenho do Windows com o Secure Endpoint.

Como criar exclusões

Esta seção aborda as práticas recomendadas para criar exclusões para o seu ambiente.

> **Cuidado**: sempre entenda os arquivos e processos antes de gravar uma exclusão para evitar vulnerabilidades de segurança no computador.

> **Observação**: detalhes adicionais disponíveis no Guia do usuário, consulte o Capítulo 3 Aqui. Este capítulo abrange os tipos de exclusões, implementação e navegação do portal Secure Endpoint.

Caminho e processo do CSIDL

A CSIDL é uma forma aceita e incentivada de escrever exclusões. O CSIDL permite exclusões de processos que podem ser confirmadas em ambientes que usam letras de drive alternativas e podem ignorar a necessidade de caracteres curinga quando esse caminho for específico ao usuário (já que as exclusões de processos não permitem caracteres curinga). Mais informações sobre o CSIDL . No entanto, há limitações que precisam ser consideradas quando o CSIDL é usado. Se o ambiente instalar programas em mais de uma letra de drive, o caminho do CSIDL se refere apenas ao drive marcado como o local de instalação padrão, por exemplo, se o SO estiver instalado em C:\, mas o caminho de instalação do Microsoft SQL tiver sido alterado manualmente para D:\, a exclusão baseada em CSIDL na lista de exclusão mantida não se aplica a esse caminho. Para exclusões de processos, isso significa que uma exclusão deve ser inserida para cada processo não localizado no drive C:\, pois o uso do CSIDL não o mapeia.

Exclusões de Caminho

Essas exclusões são as mais frequentemente usadas, conflitos de aplicativos geralmente envolvem a exclusão de um diretório. Crie uma exclusão de caminho usando um caminho absoluto ou o CSIDL.

Por exemplo, para excluir um aplicativo antivírus no diretório Arquivos de programas, o caminho de exclusão seria:

```
C:\Program Files\MyAntivirusAppDirectory
CSIDL_PROGRAM_FILES\MyAntivirusAppDirectory
```

Sem uma barra à direita, o **conector do Windows** faz uma correspondência parcial nos caminhos, enquanto o **Mac e o Linux não.**

Por exemplo, se você aplicar as seguintes exclusões de caminho"**C:\Program Files"** e como **"C:\test":**

C:\Program Arquivos e **C:\Program Arquivos (x86)** estão excluídos:

<#root>

```
C:\Program Files
```

```
C:\Program Files (x86)
```

C:\test está excluído, como **C:\test123**:

<#root>

```
C:\test
```

```
C:\test123
```

Você pode alterar a exclusão de "**C:\test"** para "**C:\test\"**, isso impede que "**C:\test123"** seja excluído.

Observação: as exclusões de caminho são recursivas e excluem todos os subdiretórios também.

Extensão de arquivo

Essas exclusões permitem a exclusão de todos os arquivos com uma determinada extensão.

Pontos principais:

- A entrada esperada no lado do conector é **.extension**
- O Painel anexa automaticamente um ponto à extensão do arquivo se nenhuma tiver sido adicionada.
- As extensões ***não*** diferenciam maiúsculas de minúsculas.

Por exemplo, para excluir todos os arquivos de banco de dados do Microsoft Access, você pode criar a seguinte exclusão:

```
.MDB
```

Observação: as exclusões padrão estão disponíveis na lista padrão. **Não é** recomendável excluir essas exclusões, pois isso pode causar alterações de desempenho nos seus **computadores.**

Curinga

Essas exclusões são as mesmas que as exclusões de caminho ou extensão, exceto pelo uso de um asterisco (*) de gatilhos de caracteres como curinga.

> **Cuidado**: a exclusão de curinga não pára nos separadores de caminho; isso pode levar a exclusões não intencionais. Exemplo: **C:*\test** exclui **C:\sample\test**, bem como **C:\1\test** ou **C:\sample\test123 .**

> **Aviso**: iniciar uma exclusão com um asterisco (*) pode causar problemas graves de desempenho. Com **7.5.3+**, a adição de Exclusões de Processos Curinga causou problemas adicionais de desempenho com exclusões de asterisco. Remova ou altere todas as exclusões neste formato para reduzir o impacto na cpu.

Por exemplo, para excluir máquinas virtuais em um MAC de serem examinadas, insira esta exclusão de caminho:

```
/Users/johndoe/Documents/Virtual Machines/
```

Essa exclusão só funciona para *johndoe*, para permitir várias correspondências de usuário, substitua o nome de usuário no caminho por um asterisco(*) para uma exclusão de curinga:

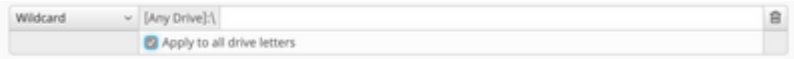
```
/Users/*/Documents/Virtual Machines/
```

Grave uma exclusão para caminhos que existam em unidades separadas.

Exemplo: **C:\testpath** e **D:\testpath** são:

```
^[A-Za-z]\testpath
```

O sistema gera automaticamente o ^[A-Za-z] quando a caixa de seleção "Aplicar a todas as letras de unidade" é marcada depois que o curinga é selecionado no menu suspenso Tipo de exclusão, como mostrado na imagem:



Processo

As Exclusões de Processos permitem que os administradores excluam processos em execução de Verificações de Arquivos normais (Secure Endpoint Windows Connector versão 5.1.1 e posterior), Proteção de Processos do Sistema (Connector versão 6.0.5 e posterior) ou Proteção contra Atividades Mal-Intencionadas (Connector versão 6.1.5 e posterior).

A exclusão do processo é feita especificando o caminho completo para o executável do processo, o valor SHA-256 do executável do processo ou o caminho e o SHA-256. Os caminhos permitem caminhos diretos ou usam um valor CSIDL.

> **Cuidado**: os processos filho criados por um processo excluído **não** são incluídos na exclusão por padrão. Exemplo: a exclusão de processo para o MS Word não excluiria por padrão nenhum processo adicional criado pelo Word.exe e seria examinado. Para incluir processos adicionais, clique na caixa

de seleção **Aplicar para processos filho**. Além disso, excluir Word.exe não é sugerido como malware regularmente se esconde em arquivos .docx modernos.

Observação: é necessário especificar Path e SHA-256 para que ambas as condições sejam atendidas para excluir o processo.

Limitações:

- Se o tamanho do arquivo do processo for maior do que o tamanho máximo de arquivo de varredura definido na política, o SHA-256 do processo não será calculado e a exclusão **não funcionará**. Usar uma exclusão de processo baseada em caminho para arquivos maiores do que o tamanho máximo de arquivo de digitalização
- Conector versões 5.x.x a 6.0.3 - um limite de 25 exclusões de processos em todos os tipos de exclusão de processos
- Conector versões 6.0.5+ - limite de 100 exclusões de processos em todos os tipos de exclusão de processos.
- Connector versões 7.x.+ - limite de 500 exclusões de processos em todos os tipos de exclusão de processos.
- O conector só aceita as exclusões de processo até o limite, na parte superior da lista de exclusões de processo em policy.xml
- Toda política tem uma exclusão de processo para sfc.exe, que conta contra o limite

```
3|0||CSIDL_Secure Endpoint_VERSION\sfc.exe|48|
```

Ameaça

Essas exclusões permitem que um nome de ameaça específico seja excluído dos eventos de acionamento. A exclusão de ameaças só deve ser usada quando o resultado da varredura aciona a detecção de falsos positivos e confirma que eles não são uma ameaça real.

A caixa de texto para adicionar uma exclusão de ameaça ***não*** diferencia maiúsculas de minúsculas. Exemplo: W32.Zombies.NotAVirus ou w32.zombies.notavirus correspondem ao mesmo nome de ameaça.

Aviso: não exclua ameaças, a menos que a investigação e a confirmação do nome da ameaça seja considerada como falso-positiva. As ameaças excluídas não são mais preenchidas na guia Eventos para revisão e auditoria.

Processar Curinga

Windows

O endpoint 7.5.3+ permite exclusões adicionais usando a funcionalidade Curinga nas exclusões de processo. Isso permite uma cobertura mais ampla com menos exclusões, mas também pode ser perigoso se muito for deixado indefinido. **Use apenas o curinga para cobrir o número mínimo de caracteres necessários para fornecer a exclusão necessária.**

Uso de (*) no Curinga do Processo para Windows:

- (*) Pode ser usado no lugar de um único caractere ou de um diretório completo. Ele não pode ser colocado no início do caminho, ele será considerado inválido. O curinga funcionará entre dois caracteres definidos, barras ou alfanuméricos. Colocá-lo no final de um caminho excluirá os processos nesse diretório, mas não os subdiretórios.
- (**) Pode ser usado no final de um caminho para excluir todos os processos nesse diretório e os processos nos subdiretórios. Isso permite um conjunto de exclusão muito maior com entrada mínima, mas também deixa uma brecha de segurança muito grande para a visibilidade. **Use esse recurso com extremo cuidado**.

Examples:

```
C:\Windows\*\Tiworker.exe - Excludes all Tiworker.exe found in the subfolders of 'Windows'
C:\Windows\P*t.exe - Excludes Pot.exe, Pat.exe, P1t.exe Etc.
C:\Windows\*chickens.exe - Excludes all Processes in 'Windows' folder ending in chickens.exe
C:\* - Excludes all Processes in the C: drive in the top layer of folders but not the subfolders
C:\** - Excludes every Process on the C: drive.
```

MacOS e Linux

O endpoint 1.15.2+ permite exclusões adicionais usando a funcionalidade Curinga nas exclusões de processo. Isso permite uma cobertura mais ampla com menos exclusões, mas também pode ser perigoso se muito for deixado indefinido. **Use apenas o curinga para cobrir o número mínimo de caracteres necessários para fornecer a exclusão necessária.**

Uso de (*) no Curinga do Processo para Mac:

- (*) Pode ser usado no lugar de um único caractere ou de um diretório completo. Ele não pode ser colocado no início do caminho, ele será considerado inválido. O curinga funcionará entre dois caracteres definidos, barras ou alfanuméricos.

Examples:

```
/Library/Java/JavaVirtualMachines/*/java - Excludes Java within all subfolders of JavaVirtualMac
/Library/Jibber/j*bber - Excludes the Process for jabber, jibber, jobber, etc.
```

Exclusões de prevenção de exploração (aplicativo)

Windows

O Secure Endpoint 7.5.1+ usa o V5 do Mecanismo de Prevenção de Exploração e o console agora permite que as exclusões de aplicativos sejam configuradas na funcionalidade de lista de exclusões atual. **No momento, isso está restrito apenas a aplicativos e quaisquer exclusões relacionadas a DLLs ainda devem ser feitas através da abertura de um caso com suporte.**

Encontrar as exclusões corretas para a prevenção de exploração é um processo muito mais intensivo do que qualquer outro tipo de exclusão e exige testes extensivos para minimizar quaisquer brechas de segurança prejudiciais.

Erros comuns a serem evitados

Tenha cuidado ao criar exclusões, pois isso reduz o nível de proteção fornecido pelo Cisco Secure Endpoint. Os arquivos excluídos não são submetidos a hash, verificados ou estão disponíveis no cache ou na nuvem, a atividade não é monitorada e as informações estão ausentes nos mecanismos de back-end, na trajetória do dispositivo e na análise avançada.

As exclusões *só* devem ser usadas com moderação em casos específicos, como problemas de compatibilidade com aplicativos específicos ou problemas de desempenho que não podem ser melhorados de outra forma.

Abaixo estão alguns erros comuns a serem evitados ao trabalhar com exclusões.

- **Exclusões proativas**
  - Não presuma que uma exclusão é necessária, a menos que tenha sido provado que ela é um problema que não pode ser resolvido de outra forma. Problemas de desempenho, falsos positivos ou problemas de compatibilidade de aplicativos devem ser completamente investigados e mitigados antes da aplicação de uma exclusão

- **Uma exclusão que é muito ampla**
  - Excluindo grandes partes do endpoint, como toda a unidade C
  - Usando uma exclusão de caractere curinga quando uma exclusão mais específica é possível
  - Usando apenas o nome do arquivo em vez de um caminho totalmente qualificado para o arquivo
  - Use a Trajetória do dispositivo ou o Pacote de diagnósticos de endpoint seguro e a Ferramenta de ajuste de desempenho para investigar e determinar a exclusão específica necessária

- **Uso excessivo de exclusões de caracteres curinga**
  - As exclusões de curinga não apenas criam mais brechas de segurança, mas também exigem mais recursos do sistema do que qualquer outro tipo de exclusão
  - Certifique-se de usar a quantidade mínima de curingas em uma exclusão; somente as pastas que são realmente variáveis devem se tornar variáveis com um curinga. Por exemplo:
    - Arquivos de programas\Software* excluirão tudo o que estiver na pasta, mas não as subpastas
    - Arquivos de Programas\Software** excluirão tudo o que estiver na pasta, incluindo subpastas

- **Excluindo itens que são usados em ataques**
  - Tipos de arquivos, como .cmd, .zip, .jpg etc.
  - Processos como svchost.exe, bash.exe, powershell.exe, etc.
  - Locais de pastas, como C:\Users\, C:\Windows\Temp\, C:\Program Files\Java etc.

- **Duplicar exclusões**
  - Antes de criar uma exclusão, verifique se a exclusão já existe nas Exclusões personalizadas criadas pelo usuário ou nas Exclusões mantidas pela Cisco.
  - A remoção de exclusões duplicadas não só melhora o desempenho, como também reduz o

gerenciamento operacional de exclusões

- **Exclusões obsoletas**
  - Exclusões criadas há muito tempo e podem não ser necessárias.
  - Revise e audite regularmente sua lista de exclusão e não deixe de manter um registro do motivo pelo qual uma determinada exclusão foi adicionada.

- **Não removendo exclusões pós-infecção**
  - As exclusões devem ser removidas assim que uma infecção for identificada, a fim de recuperar a segurança e a visibilidade ideais
  - Usar a função Ações automatizadas "Mover computador para grupo" antecipadamente permitirá que você aplique rapidamente uma política mais segura após a infecção, incluindo a configuração de uma política sem nenhuma exclusão

- **Falta de táticas de mitigação**
  - Quando as exclusões forem absolutamente necessárias, considere quais táticas atenuantes podem ser tomadas, como ativar a proteção contra gravação para adicionar algumas camadas de proteção para os itens excluídos.

Para obter mais práticas recomendadas sobre exclusões ou endpoints seguros, consulte o Guia de práticas recomendadas

Exclusões Não Recomendadas

Para efeitos de boa postura de segurança e visibilidade, não são recomendadas as seguintes exclusões:

AcroRd32.exe
addinprocess.exe
addinprocess32.exe
addinutil.exe
bash.exe
bginfo.exe
bitsadmin.exe
cdb.exe
csi.exe

dbghost.exe
dbgsvc.exe
dnx.exe
dotnet.exe
excel.exe
fsi.exe
fsiAnyCpu.exe
iexplore.exe
java.exe
kd. exe
lxssmanager.dll
msbuild.exe
mshta.exe
ntkd.exe
ntsd.exe
outlook.exe
psexec.exe
powerpnt.exe

powershell.exe
rcsi.exe
svchost.exe
schtasks.exe
system.management.automation.dll
windbg.exe
winword.exe
wmic.exe
wuauclt.exe
.7z
.bat
.bin
.cab
.cmd
.com
.cpl
.dll
.exe

.fla
.gif
.gz
.hta
.inf
.java
.jar
.trabalho
.jpeg
.jpg
.js
.ko
.ko.gz
.msi
.ocx
.png
.ps1
.py

.rar
.reg
.scr
.sys
.tar
.tmp
.url
.vbe
.vbs
.wsf
.zip
bash
java
python
Python3
sh
zsh
/

/bin
/sbin
/usr/lib
C :
C:\
C:*
D:\
D:*
C:\Program Files\Java
C:\Temp\
C:\Temp*
C:\Users\
C:\Users*
C:\Windows\Prefetch
C:\Windows\Prefetch\
C:\Windows\Prefetch*
C:\Windows\System32\Spool

C:\Windows\System32\CatRoot2
C:\Windows\Temp
C:\Windows\Temp\
C:\Windows\Temp*
C:\Program Arquivos\<nome da empresa>\
C:\Program Arquivos (x86)\<nome da empresa>\
C:\Users\<UserProfileName>\AppData\Local\Temp\
C:\Users\<UserProfileName>\AppData\LocalLow\Temp\

Informações Relacionadas

- **Suporte Técnico e Documentação - Cisco Systems**
- **Endpoint seguro da Cisco - Notas técnicas**
- **Endpoint Cisco Secure - Guia do usuário**
- **Ponto de extremidade seguro: exclusões de processos no macOS e no Linux**

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.