Cisco Secure Endpoint에서 오래된 Windows 제외 제거

목차

소개

이 문서에서는 Windows Secure Endpoint 고객 환경에서 형식이 잘못된 일반적인 제외 항목을 제거하기 위한 계획된 프로세스에 대해 설명합니다.

문제 설명

Cisco 엔지니어는 성능에 미치는 영향을 최소화하고 Cisco Secure Endpoint의 기능을 극대화하기 위한 지속적인 노력을 통해 고객 환경에 존재하는 가장 보편적인 오래된 제외 항목을 파악했으며 2022년 10월 중에 제거할 예정입니다. 보안 엔드포인트(6.x 이하)의 이전 이터레이션은 와일드카드 기능(*)에 의존하여 다중 드라이브 제외를 활용했습니다. 나중에 제외 정의 및 입력에 대한 변경 및 개선을 통해 이러한 광범위한 형식이 필요하지 않게 되었으며 Cisco Maintained Exclusions는 와일드카드가 생성한 성능 영향을 해결하기 위해 조정되었습니다. Windows Secure Endpoint 7.5.3 릴리스에서는 와일드카드(*) 프로세스 제외에 대한 새 기능이 허용되었습니다. 이 기능은 별표 선두 제외의 처리를 변경했으며 해당 환경에서 여전히 다음과 같은 제외가 있는 고객의 cpu 소비량을 증가시켰습니다.

```
*\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*
```

추가 단계

이러한 제외를 제거해도 환경에 부정적인 영향을 주지 않으며 Windows Secure Endpoint 7.5.3 이상을 사용하는 호스트의 성능이 향상될 수 있습니다. 현재 사용자 정의 제외 목록에서 별표 앞에 있는 제외(*) 제외 항목을 검토하고, 여러 개의 드라이브가 필요한 경우 와일드카드에 사용할 수 있는 "모든 드라이브 문자에 적용" 기능을 사용하도록 수정하거나, 그렇지 않은 경우 경로에 드라이브 문자를 제공하십시오. 다음 소프트웨어 중 하나를 사용하는 경우 정책에 Cisco Maintened List를 추가해야 합니다. 올바른 제외 항목이 이미 사용되고 있기 때문입니다.

- Microsoft Windows 기본값
- Symantec의 Altiris
- 도메인 컨트롤러
- 디볼드 바르샤바
- 레이크사이드 소프트웨어 - Systrak
- SAS 애플리케이션
- 시만텍

참고: 조직 내에서 변경 동결과 관련된 우려가 있는 경우 TAC 케이스를 열고 **2022년 10월 7일까지** 이 문서를 참조하십시오.

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.