

cisco *Live!*

Let's go

#CiscoLive



The bridge to possible

Troubleshoot and Isolate Performance Issues on Secure Endpoints (Windows, Linux and MAC)

Vibhor Amrodia
Customer Delivery Engineering Technical Leader

BRKSEC-2072

cisco *Live!*

#CiscoLive

Cisco Webex App

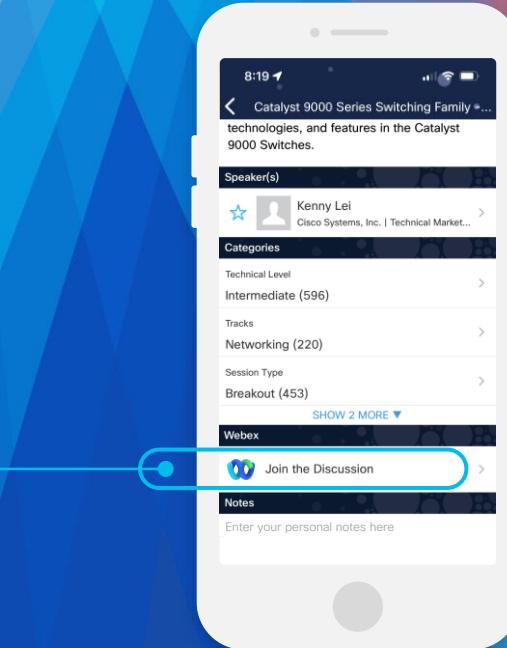
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 9, 2023.



<https://ciscolive.ciscoevents.com/ciscoevents/ciscoeventsbot/#BRKSEC-2072>

Agenda

- Introduction
- Fundamentals
- Troubleshooting Methodology
- Self-Service Troubleshooting Tools
- Data to Collect
- Common Scenarios
- Conclusion

Who Am I ???



- 11+ Years of Support Experience
- Security Technical Leader
- Firewall/Email/Endpoint Technology Expertise
- Leading Secure Endpoint Global TAC Teams
- “Customer Focused” Attitude

Introduction

“Before you marry a person, you should first make them use a computer with slow Internet to see who they really are.”

Will Ferrell

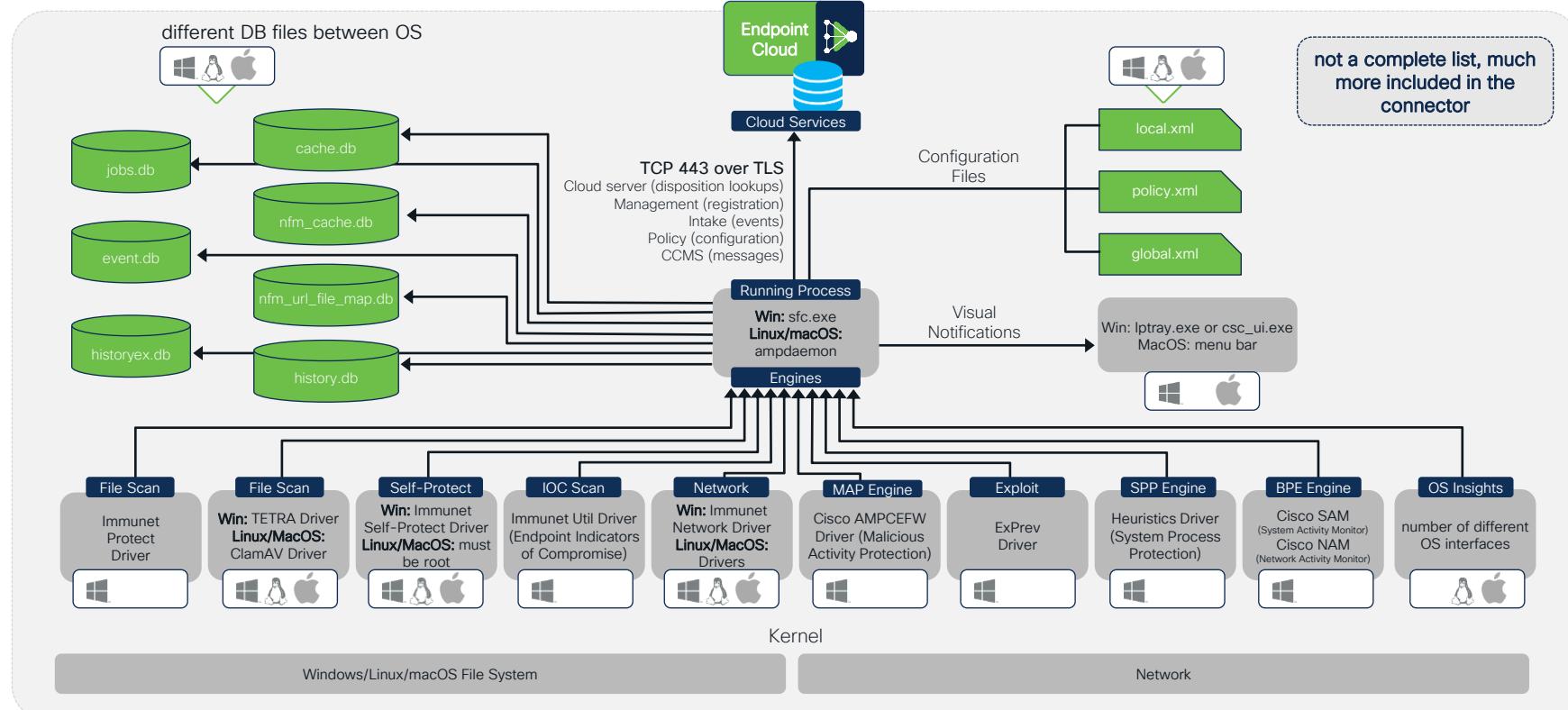
Why is Endpoint Performance Important?

Possible Impact:

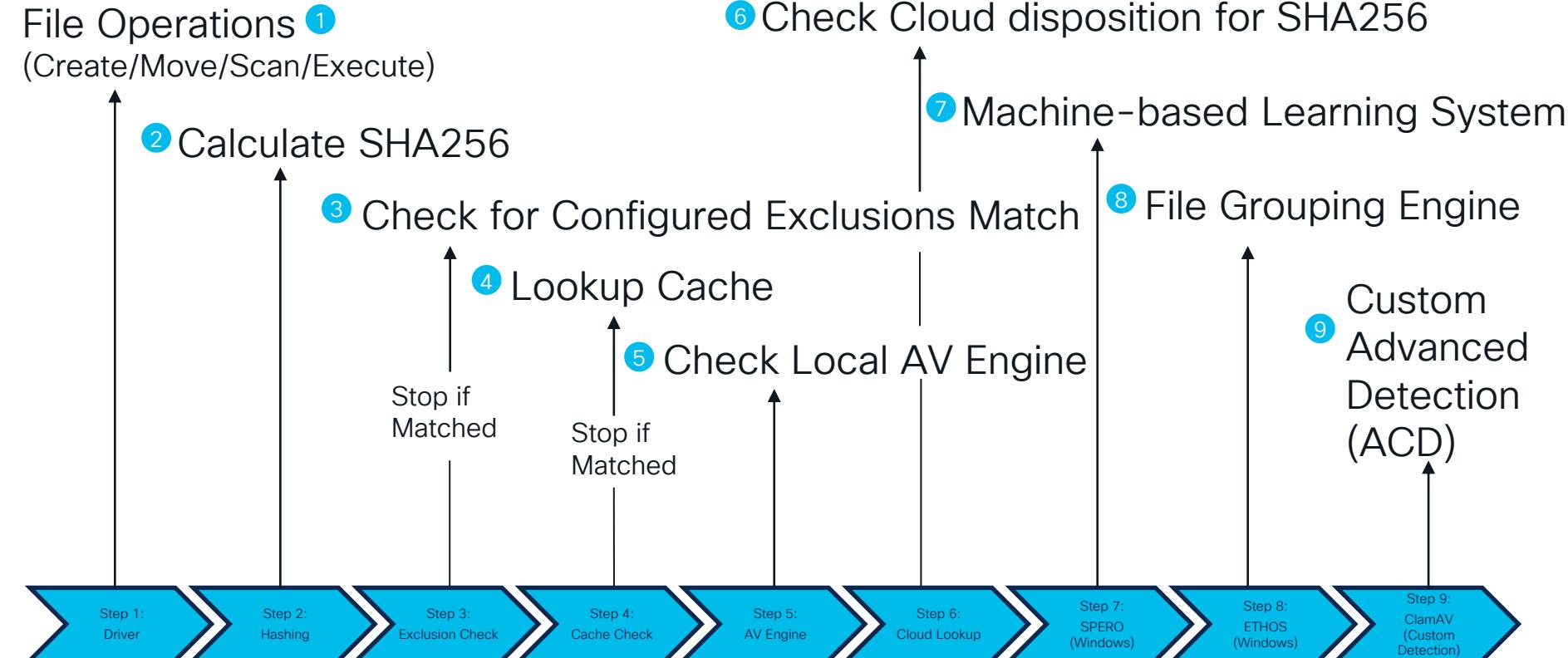
- End User Usability of Assets
- End User Productivity
- Critical Infrastructure Services
- Database Services
- Application/Web Servers
- Email Servers
- Virtual Infrastructure
- and many more.....

Fundamentals

Secure Endpoint Architecture



Order of Operations





Secure Endpoint Windows Drivers

Driver Name	Required For	Filename
ancrl	Endpoint Isolation	C:\Program Files\Cisco\AMP\endpointisolation\ancrl64.sys
CiscoAMPCEFWDriver	MAP	C:\Windows\System32\Drivers\CiscoAMPCEFWDriver.sys
CiscoAMPELAMDriver	WSC/CSCMS	C:\Windows\system32\Drivers\CiscoAMPELAMDriver.sys
CiscoAMPHeurDriver	MAP/ETHOS/SPERO	C:\Windows\System32\Drivers\CiscoAMPHeurDriver.sys
CiscoSAM	BP	C:\Windows\system32\Drivers\CiscoSAM.sys
csadc	Device Control	C:\Windows\system32\DRIVERS\csadc.sys
ImmunetNetworkMonitorDriver	Network	C:\Windows\System32\Drivers\ImmunetNetworkMonitor.sys
ImmunetProtectDriver	Scan	C:\Windows\System32\Drivers\immutnetprotect.sys
ImmunetSelfProtectDriver	SPP/Self Protect	C:\Windows\System32\Drivers\immutnetselfprotect.sys



Secure Endpoint Windows Services

Service Name	Display Name
CiscoAMP	Cisco Secure Endpoint 8.1.7
CiscoOrbital	Cisco AMP Orbital
CiscoSCMS	Cisco Security Connector Monitoring Service 8.1.7
iptray	Cisco Secure Endpoint Tray Client (Only with Connector Version 7.x and below)
csc_ui	Cisco Secure Client User Interface (Only with Connector Version above 8.x)

Command Line CLI: `sc queryex type=service state=all | find /i "cisco"`

Note: *The names will vary with the respective version of Connector*



Secure Endpoint Linux Processes

Process Name	Description	Location
ampcli	Interactive Shell	/opt/cisco/amp/bin/
ampcreport	Internal Use Only	/opt/cisco/amp/bin/
ampdaemon	Main Connector Process	/opt/cisco/amp/bin/
ampmon	Internal Use Only	/opt/cisco/amp/bin/
ampscansvc	Scanning Process	/opt/cisco/amp/bin/
orbital	Orbital Process	/opt/cisco/amp/bin/
ampupdater	Connector Updates	/opt/cisco/amp/bin/



Secure Endpoint MAC Processes

Process Name	Description	Location
ampcli	Interactive Shell	/Applications/Cisco Secure Endpoint/Secure Endpoint Service.app/Contents/MacOS/ampcli
ampcreport	Internal Use Only	/Applications/Cisco Secure Endpoint/Secure Endpoint Service.app/Contents/MacOS/ampcli
ampdaemon	Main Connector Process	/Applications/Cisco Secure Endpoint/Secure Endpoint Service.app/Contents/MacOS/ampcli
ampmon	Internal Use Only	/Applications/Cisco Secure Endpoint/Secure Endpoint Service.app/Contents/MacOS/ampcli
ampscansvc	Scanning Process	/Applications/Cisco Secure Endpoint/Secure Endpoint Service.app/Contents/MacOS/ampcli
orbital	Orbital Process	/Applications/Cisco Secure Endpoint/Secure Endpoint Service.app/Contents/MacOS/ampcli
ampupdater	Connector Updates	/Applications/Cisco Secure Endpoint/Secure Endpoint Service.app/Contents/MacOS/ampcli

Policy Options

Modes and Engines

Conviction Modes

These settings control how Secure Endpoint responds to suspicious files and network activity.

Files

Quarantine Audit

Remove and report malicious files.

Network

Block Audit Disabled

Block and report malicious network connections.

Detection Engines

ClamAV 

Linux/MAC

Recommended Settings

Workstation

- Files: Quarantine
- Network: Block

Apply Workstation Settings

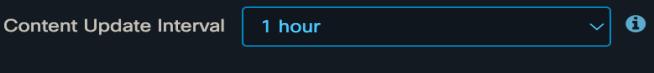
Server

- Files: Quarantine
- Network: Disabled

Apply Server Settings

Advanced Settings -> ClamAV

MAC



Linux



Windows

Modes and Engines

Conviction Modes

These settings control how Secure Endpoint responds to suspicious files and network activity.

Files

Quarantine Audit

Remove and report malicious files.

Network

Block Audit Disabled

Block and report malicious network connections.

Malicious Activity Protection

Quarantine Block Audit Disabled

End ransomware-like processes, remove their executable, and report them.

System Process Protection

Protect Audit Disabled

Block possible malicious tampering of critical operating system processes and report the activity.

Script Protection

Quarantine Audit Disabled

Stop, remove, and report malicious scripts when they execute.

Exploit Prevention

Block Audit Disabled

Detect binary code injection attacks against some processes, end the process, and report it.

Exploit Prevention - Script Control

Block Audit Disabled

Block applications from loading certain DLLs.

Behavioral Protection

Protect Audit Disabled

Detect malicious activity, take remedial actions as needed, and report it.

Enable Event Tracing for Windows

TETRA 

Detection Engines

Recommended Settings

Workstation

- Files: Quarantine
- Network: Block
- Malicious Activity Protection: Quarantine
- System Process Protection: Protect
- Script Protection: Quarantine
- Exploit Prevention: Block
- Exploit Prevention - Script Control: Audit
- Behavioral Protection: Protect

Apply Workstation Settings

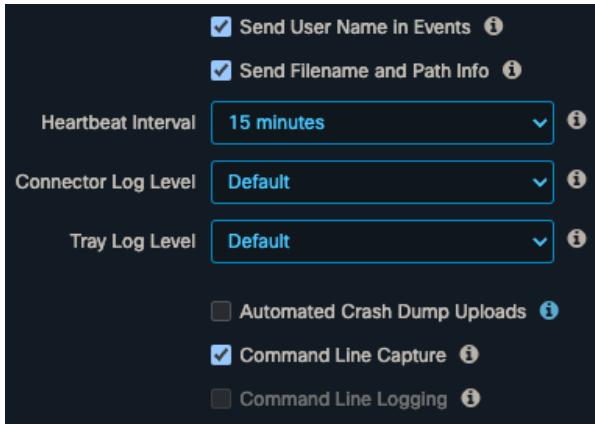
Server

- Files: Quarantine
- Network: Disabled
- Malicious Activity Protection: Disabled
- System Process Protection: Disabled
- Script Protection: Quarantine
- Exploit Prevention: Audit
- Exploit Prevention - Script Control: Audit
- Behavioral Protection: Protect

Apply Server Settings

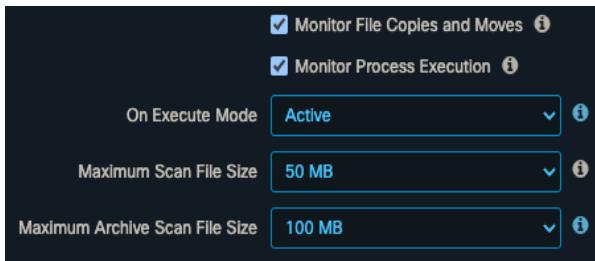
Advanced Policy Settings

Linux/MAC



Send User Name in Events i
Send Filename and Path Info i
Heartbeat Interval i
Connector Log Level i
Tray Log Level i
Automated Crash Dump Uploads i
Command Line Capture i
Command Line Logging i

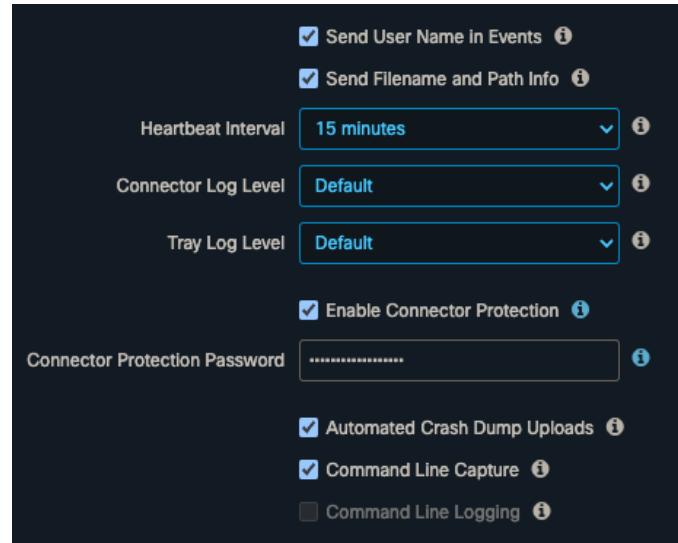
Advanced Settings ->
Administrative Features



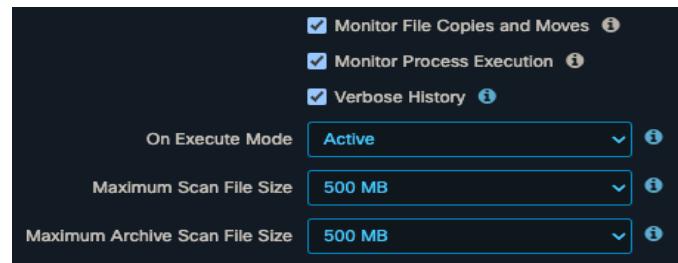
Monitor File Copies and Moves i
Monitor Process Execution i
On Execute Mode i
Maximum Scan File Size i
Maximum Archive Scan File Size i

Advanced Settings -> File
and Process Scan

Windows

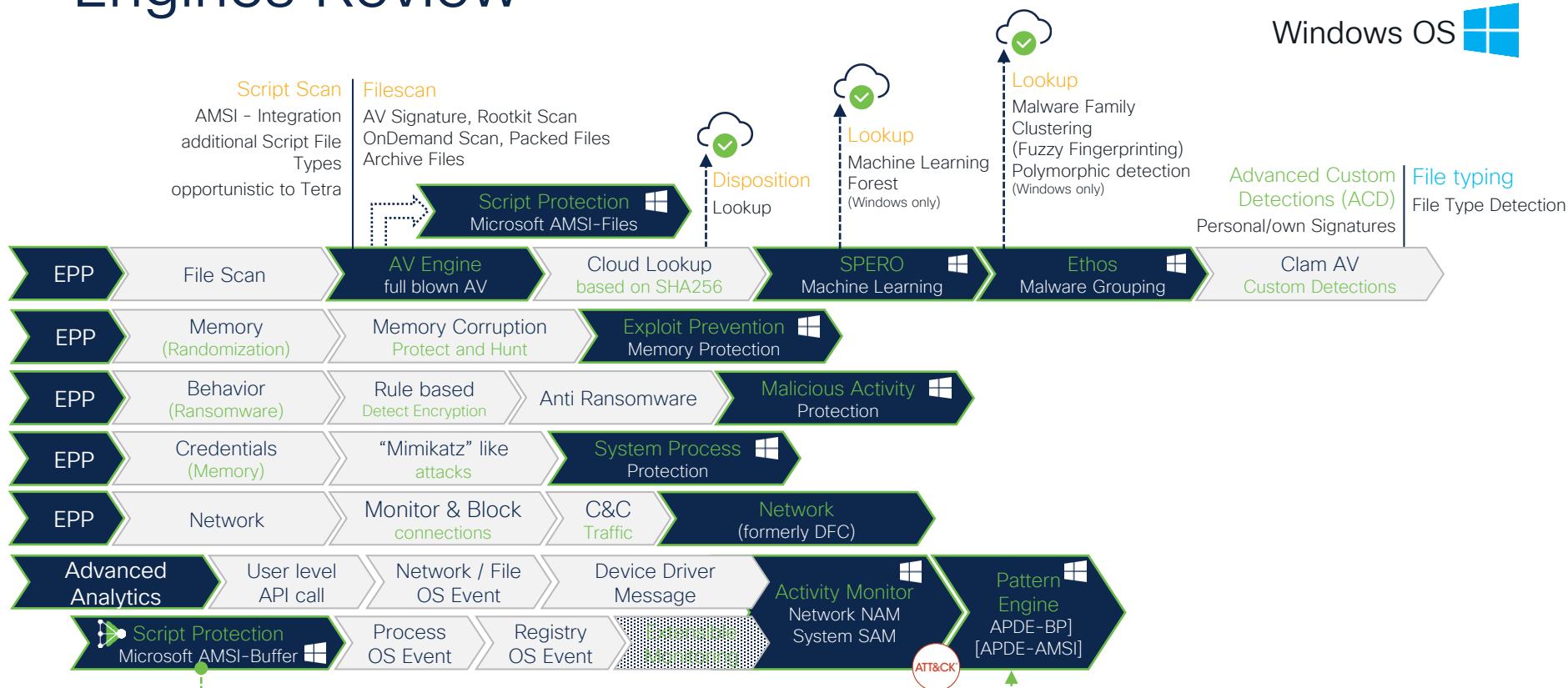


Send User Name in Events i
Send Filename and Path Info i
Heartbeat Interval i
Connector Log Level i
Tray Log Level i
Enable Connector Protection i
Connector Protection Password i
Automated Crash Dump Uploads i
Command Line Capture i
Command Line Logging i



Monitor File Copies and Moves i
Monitor Process Execution i
Verbose History i
On Execute Mode i
Maximum Scan File Size i
Maximum Archive Scan File Size i

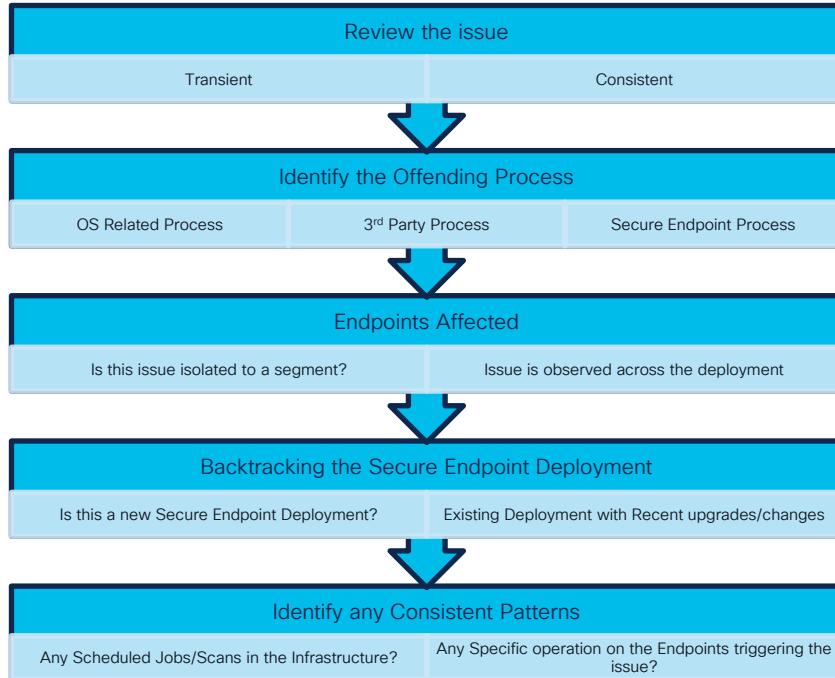
Engines Review



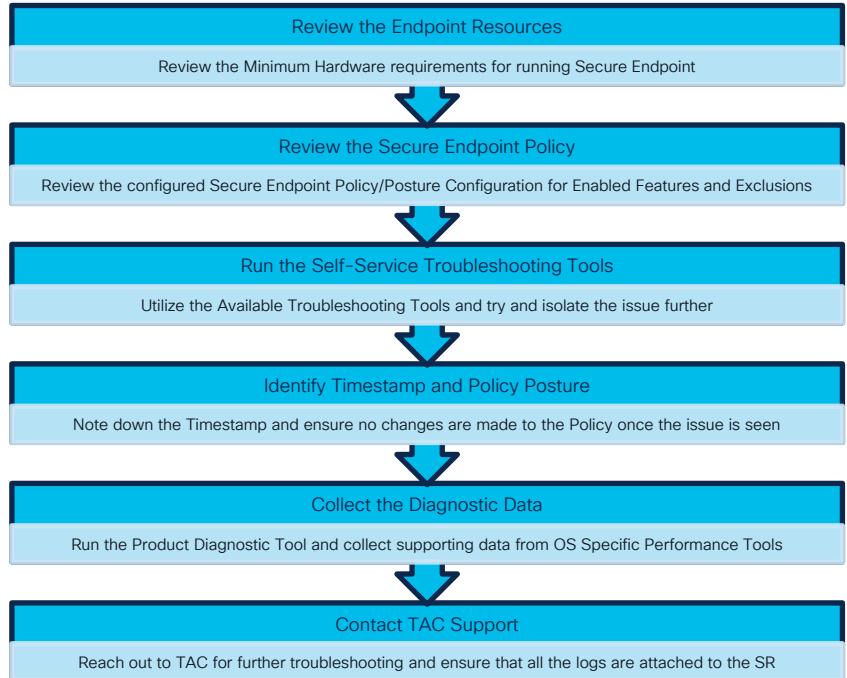
Troubleshooting Methodology

Isolating the Problem

Initial Review



Secure Endpoint Process



Self-Service Troubleshooting Tools

Cisco Self-Service Tools

- Product Support Diagnostics Tools
- Cisco Orbital
- SecureX Orchestration
- Cisco RADKit
- AMP Health Checker (Windows Only)

Data To Collect

Collecting Diagnostic Data

Windows

- Support Diagnostic Bundle
- Windows Health Checker
- 3rd Party Tools (Microsoft)
 - Task Manager
 - Resource Monitor
 - Performance Monitor
 - Logman
 - Perfview
 - Process Monitor

and many more..

Mac/Linux

- Support Diagnostic Bundle
 - Activity Monitor (Mac)
- and many more CLI Utilities..

Collecting Support Diagnostics

Generating Support Diagnostics Locally: <https://cs.co/9000OTZmr>

Note: Use Timed Diagnostic Tool option for ease of collection of data

Generating Remotely

Login to Secure Endpoint Console -> Management -> Computers -> Expand the Specific Endpoint -> Diagnose

The image shows two screenshots of the Cisco Secure Endpoint Console. The left screenshot displays a list of endpoint details for a specific device, including Hostname, Operating System, Connector Version, Install Date, Connector GUID, Processor ID, Definitions Last Updated, and Cisco Secure Client ID. The right screenshot shows a 'New Connector Diagnostic' dialog box with options for a 'Debug session' (set to 5 minutes), 'Historical Data' (checked), and 'Kernel Log' (checked). A warning message in an orange box states: 'Diagnostic files are limited to 50MB in size and can take up to 24 hours to generate.' At the bottom right of the dialog are 'Cancel' and 'Create' buttons.

Diagnostic file would be available under Analysis -> File Repository -> Available

Common Scenarios

Secure Endpoint Windows UI Slowness

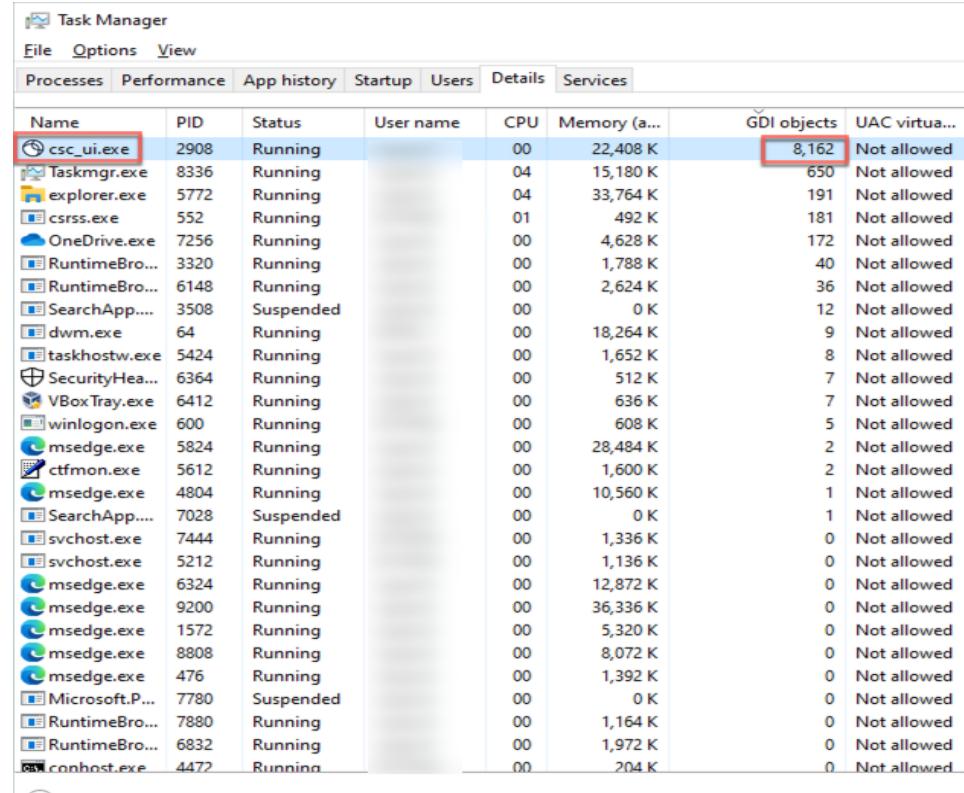
CSCwe72861: csc_ui.exe causing performance issues on Windows connectors
<https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwe72861>

Problem:
Minor GDI Leak in *csc_ui.exe*

Symptoms:
Windows Application Sluggishness

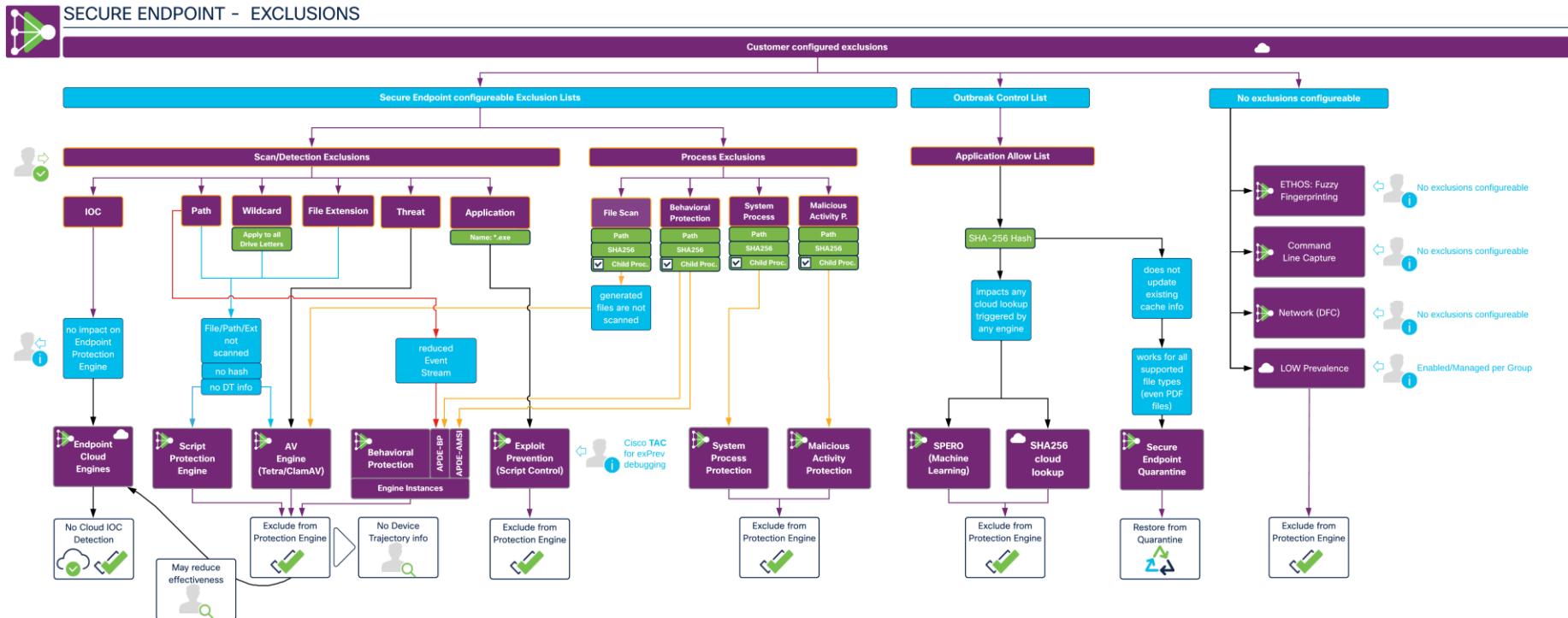
Affected Versions:
Every 8.x Release before 8.1.7.x
7.X version are NOT affected

Fixed Release:
8.1.7.x and above



Name	PID	Status	User name	CPU	Memory (a...)	GDI objects	UAC virtua...
csc_ui.exe	2908	Running		00	22,408 K	8,162	Not allowed
Taskmgr.exe	8336	Running		04	15,180 K	650	Not allowed
explorer.exe	5772	Running		04	33,764 K	191	Not allowed
csrss.exe	552	Running		01	492 K	181	Not allowed
OneDrive.exe	7256	Running		00	4,628 K	172	Not allowed
RuntimeBro...	3320	Running		00	1,788 K	40	Not allowed
RuntimeBro...	6148	Running		00	2,624 K	36	Not allowed
SearchApp....	3508	Suspended		00	0 K	12	Not allowed
dwm.exe	64	Running		00	18,264 K	9	Not allowed
taskhostw.exe	5424	Running		00	1,652 K	8	Not allowed
SecurityHea...	6364	Running		00	512 K	7	Not allowed
VBoxTray.exe	6412	Running		00	636 K	7	Not allowed
winlogon.exe	600	Running		00	608 K	5	Not allowed
msedge.exe	5824	Running		00	28,484 K	2	Not allowed
ctfmon.exe	5612	Running		00	1,600 K	2	Not allowed
msedge.exe	4804	Running		00	10,560 K	1	Not allowed
SearchApp....	7028	Suspended		00	0 K	1	Not allowed
svchost.exe	7444	Running		00	1,336 K	0	Not allowed
svchost.exe	5212	Running		00	1,136 K	0	Not allowed
msedge.exe	6324	Running		00	12,872 K	0	Not allowed
msedge.exe	9200	Running		00	36,336 K	0	Not allowed
msedge.exe	1572	Running		00	5,320 K	0	Not allowed
msedge.exe	8808	Running		00	8,072 K	0	Not allowed
msedge.exe	476	Running		00	1,392 K	0	Not allowed
Microsoft.P...	7780	Suspended		00	0 K	0	Not allowed
RuntimeBro...	7880	Running		00	1,164 K	0	Not allowed
RuntimeBro...	6832	Running		00	1,972 K	0	Not allowed
conhost.exe	4472	Running		00	204 K	0	Not allowed

Secure Endpoint Exclusions



Secure Endpoint Exclusions (contd.)

File Scan Exclusion impact on exclusion hit

- **Stops** full File Scanning Sequence -> Raised Performance -> **Reduced** Protection
- **Stops** hashing the file -> Raised Performance
- **Stops** sending Telemetry data to backend for processing -> **Reduced** Detection



Suggestions

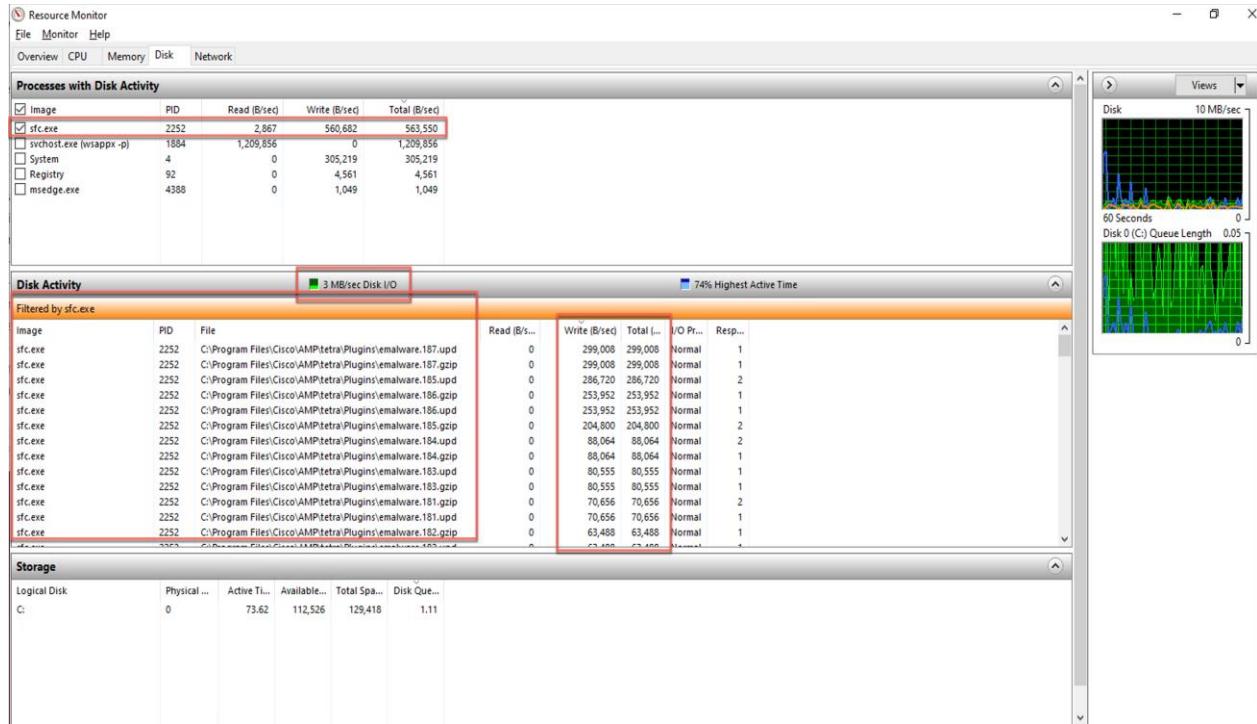
- Use Cisco Maintained Exclusions: <https://cs.co/9002OTQVp>
- AVOID using Exclusion for Possible Performance Gains
- Trim the Custom Exclusions as much as possible for increased Security and Visibility

Best Practices: <https://cs.co/9003OTaxf>

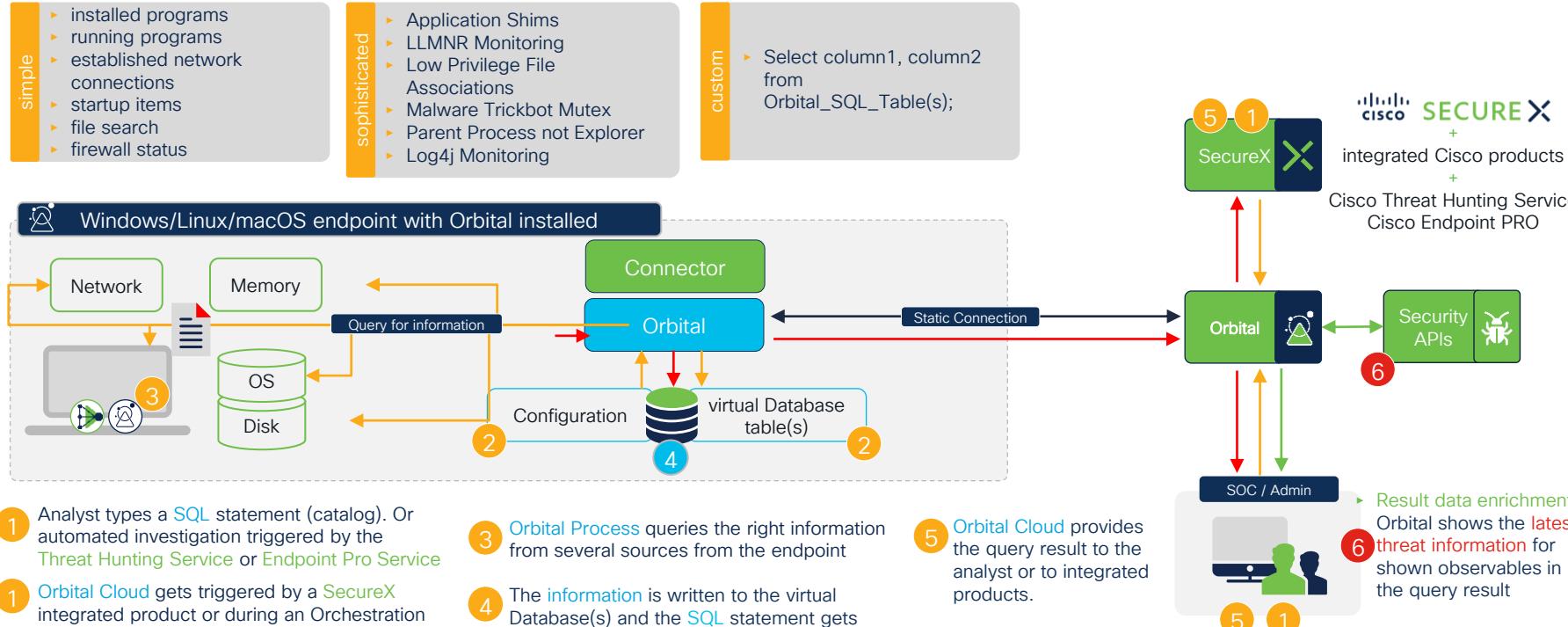
Secure Endpoint TETRA Updates

Summary

- Around ~300 MB for initial Signature Download
- Incremental Signature updates around ~8MB with frequency of 4-8 Times a day (Depends on configured *Content Update Interval*)
- **ONLY** during the Initial TETRA Enablement, we would see an increase in the Disk Writes to load the signatures on the Endpoints



Secure Endpoint Orbital Queries



Secure Endpoint Debug Logging

Details

- Max of 10 Files retained of ~50 MB

Suggestions

- Enable **Debug** only for Investigation/TAC
- Utilize **Timed Diagnostic Tool** for ease of collecting data
- Enabling it locally on the Endpoint is **preferred** vs in the Policy
- If needed for Policy, create a separate Policy
- **AVOID** deploying new connector with Policy configured with Debug Logging

Note: These are as per the best practice suggestion and there might be instances where some of might be needed for Investigation/troubleshooting purposes

Secure Endpoint Full Scan

Details

- Full Scan = Flash Scan + ALL Files on all local Drives
- Flash Scan all running processes/services, system registry and loaded modules (.DLL's) with cloud lookups and/or local signatures (if applicable)
- On Windows , we would observe **sfc.exe** service
- On Mac/Linux, we would observe **ampscansvc** process/service

Suggestions

- **Best** to run/schedule Full Scan outside of production hours
- Run **Flash Scan** daily
- Schedule **Full Scan** over the weekends
- Run a Full Scan after the **initial install**

Conclusion

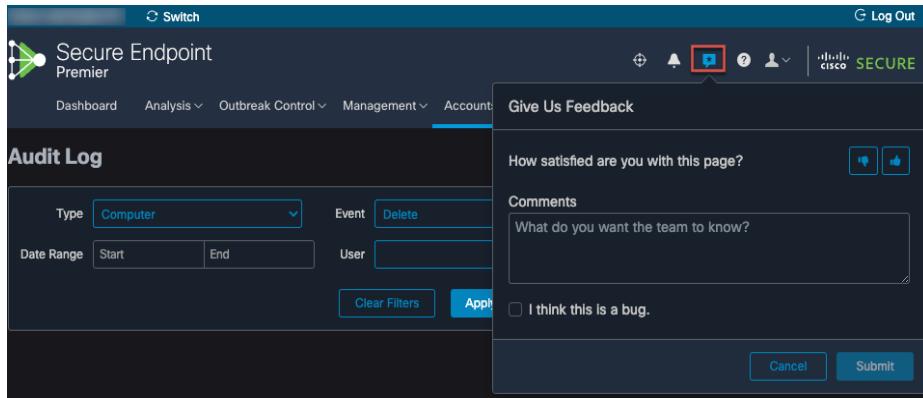
Final Words

- Use **Cisco Maintained Exclusions**
- Trim down the **Custom Exclusion**
- Exclusions **IS NOT** a utility to improve performance
- Review the Secure Endpoint **minimum resource** requirements
- **DO NOT** use Debug Logging as default in **Production**. Only for Investigations/TAC
- Test **Extensive Custom Orbital Queries**
- Update **Connector Versions** frequently
- **Best** to run/schedule Full Scan outside of production hours
- Initial **TETRA installs** would cause High Disk I/O Writes
- Utilize **other Cisco Products/Services**

Your Feedback Matters

How?

Top Right Corner, Click on  icon to open the feedback widget



Next Steps

Feedback gets into our Internal System for the requests to be reviewed and prioritized

Fill out your session surveys!



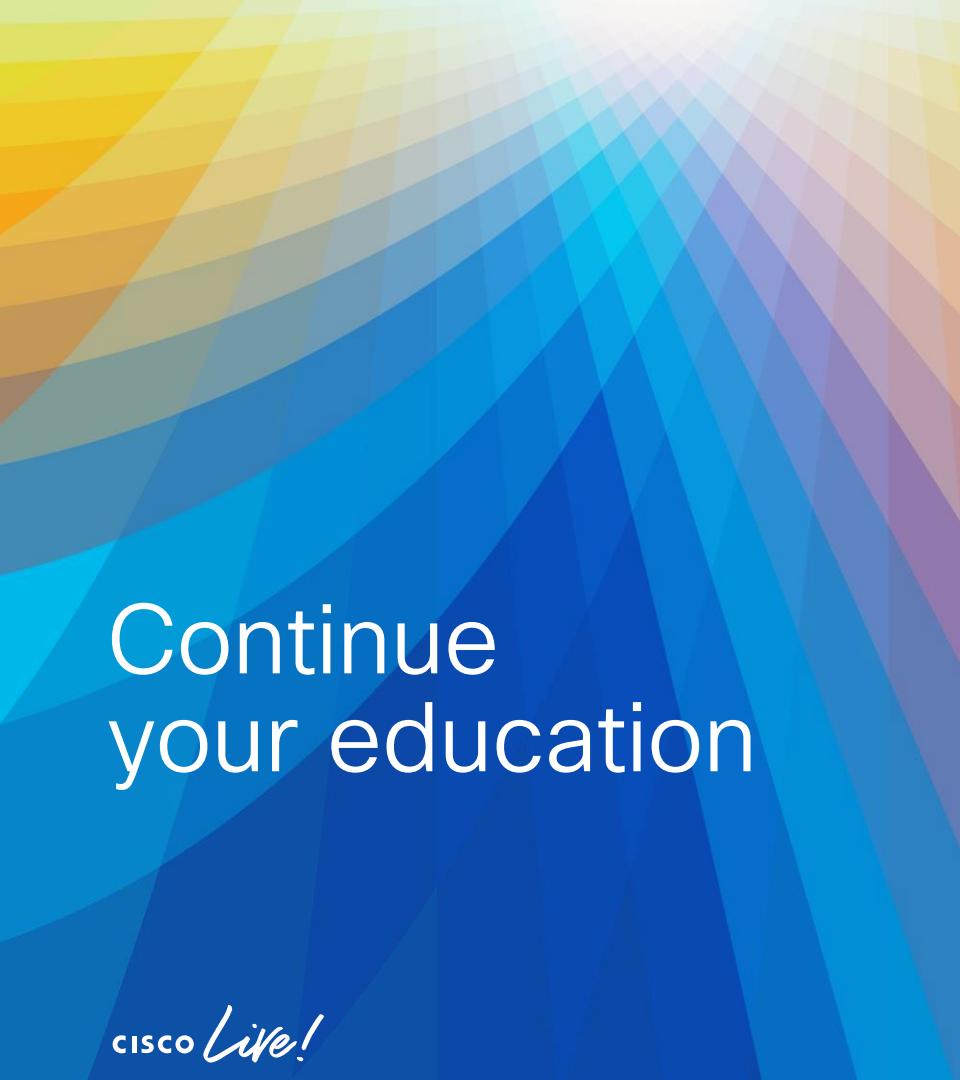
Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!



Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.



These points help you get on the leaderboard and increase your chances of winning daily and grand prizes



Continue your education

CISCO *Live!*

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



The bridge to possible

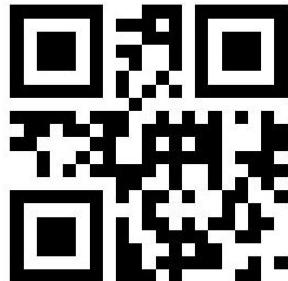
Thank you

Cisco Live Challenge

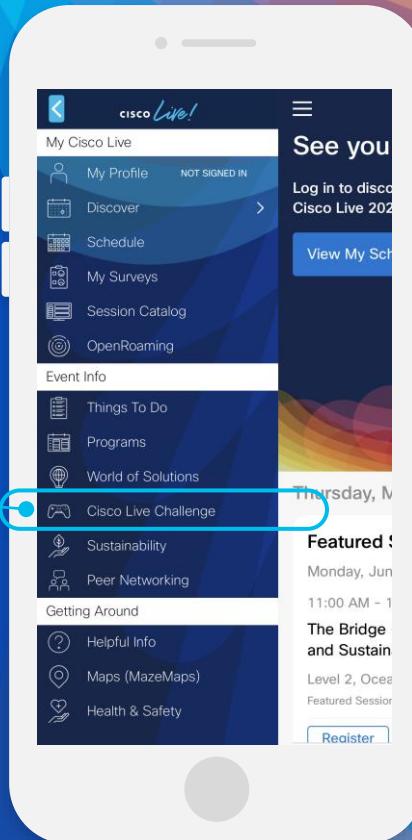
Gamify your Cisco Live experience!
Get points for attending this session!

How:

- 1 Open the Cisco Events App.
- 2 Click on 'Cisco Live Challenge' in the side menu.
- 3 Click on View Your Badges at the top.
- 4 Click the + at the bottom of the screen and scan the QR code:



CISCO *Live!*



cisco *Live!*

Let's go

#CiscoLive