

The background is a vibrant, abstract graphic. It features a central bright white light source from which numerous colorful rays emanate, creating a sunburst or starburst effect. The rays transition through a spectrum of colors including yellow, orange, red, and various shades of blue and green. Overlaid on this are several large, semi-transparent, wavy shapes in similar color tones, giving the overall image a sense of motion and energy.

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

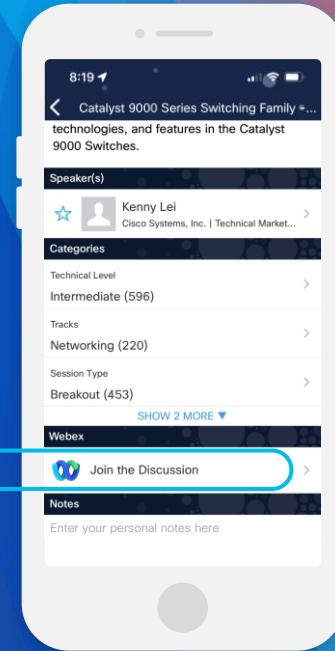
Questions?

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/ciscolivebot/#BRKSEC-2072>

Agenda

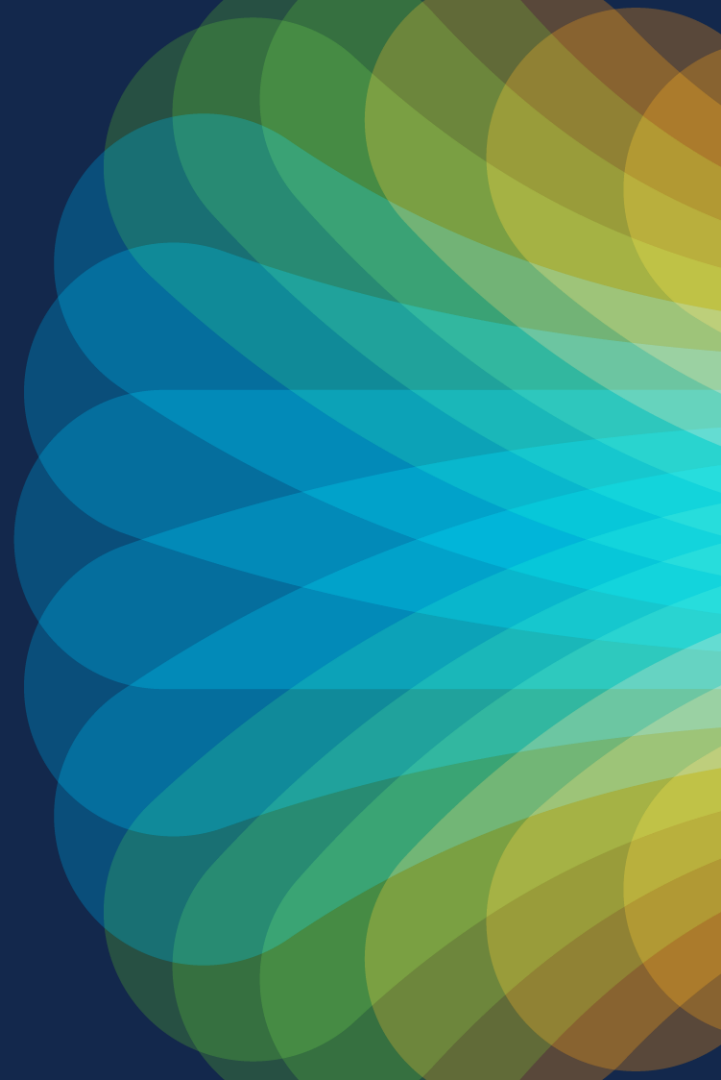
- Introduction
- Fundamentals
- Troubleshooting Methodology
- Self-Service Troubleshooting Tools
- Data to Collect
- Common Scenarios
- Conclusion

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

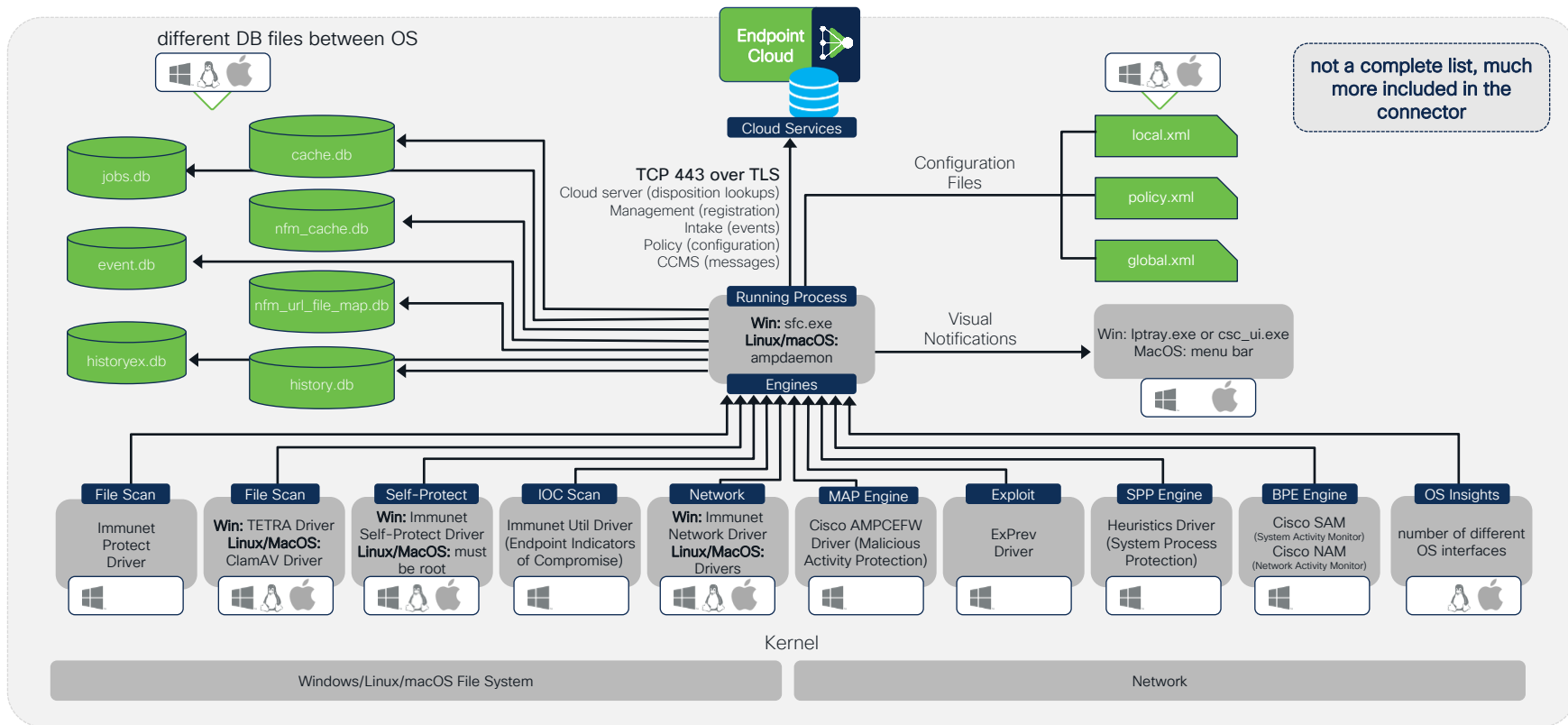
Why is Endpoint Performance Important?

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

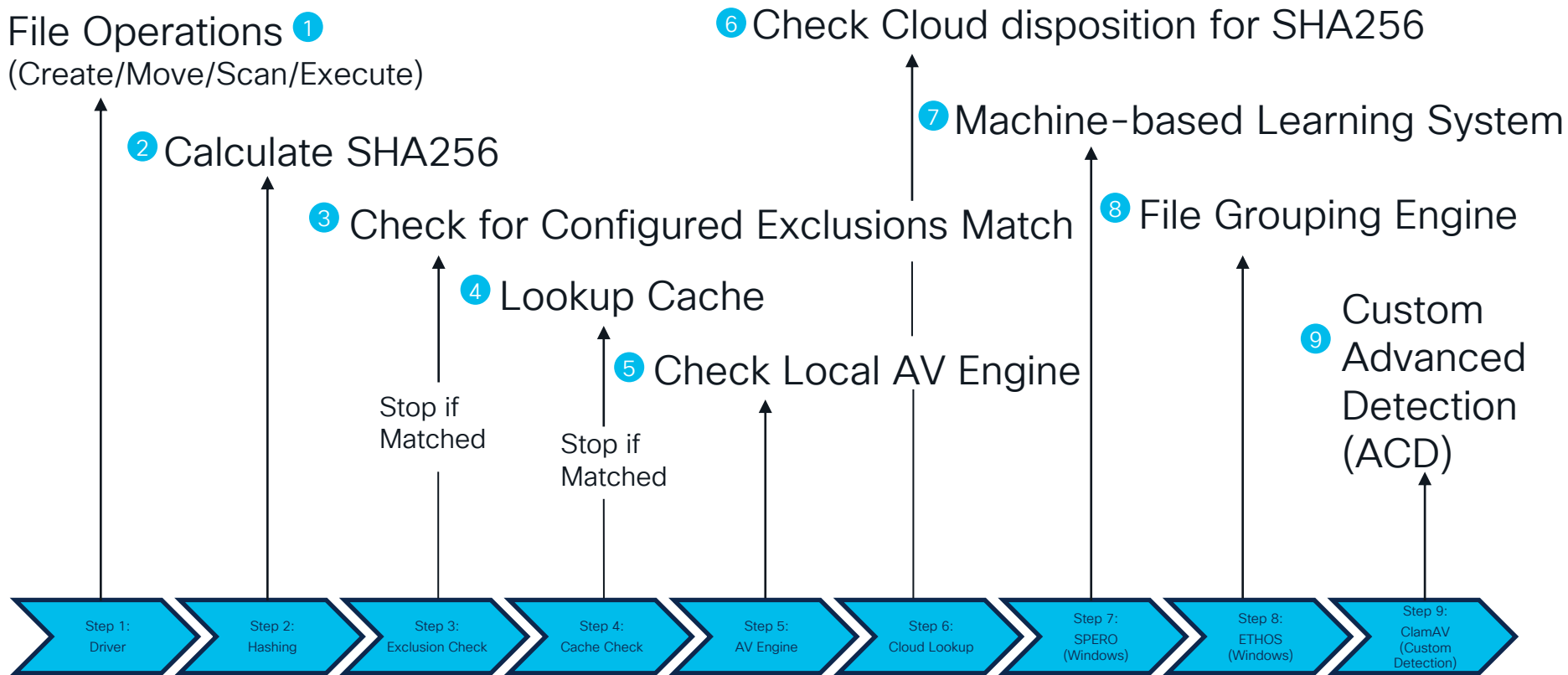
Secure Endpoint Architecture



Order of Operations

File Operations ①

(Create/Move/Scan/Execute)





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\immunetprotect.sys
ImmunetSelfProtectDriver	SPP/Self Protect	C:\Windows\System32\Drivers\immunetselfprotect.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

Linux/MAC

Modes and Engines

Advanced Settings -> ClamAV

MAC

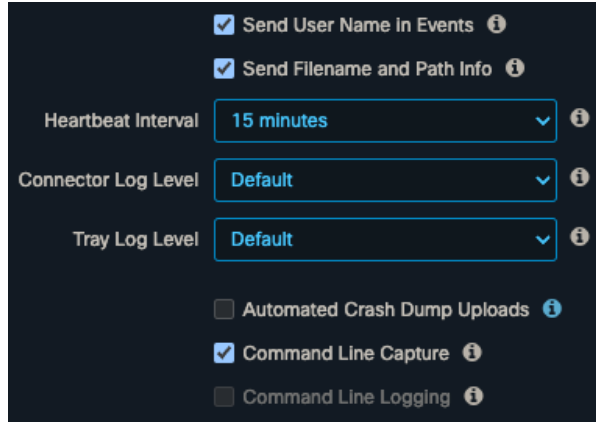
Linux

Windows

Modes and Engines

Advanced Policy Settings

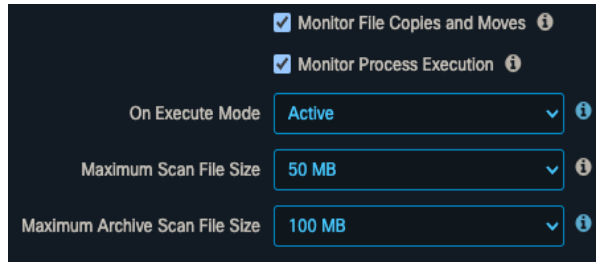
Linux/MAC



Advanced Policy Settings for Linux/MAC:

- ☒ Send User Name In Events ⓘ
- ☒ Send Filename and Path Info ⓘ
- Heartbeat Interval: ⓘ
- Connector Log Level: ⓘ
- Tray Log Level: ⓘ
- ☐ Automated Crash Dump Uploads ⓘ
- ☒ Command Line Capture ⓘ
- ☐ Command Line Logging ⓘ

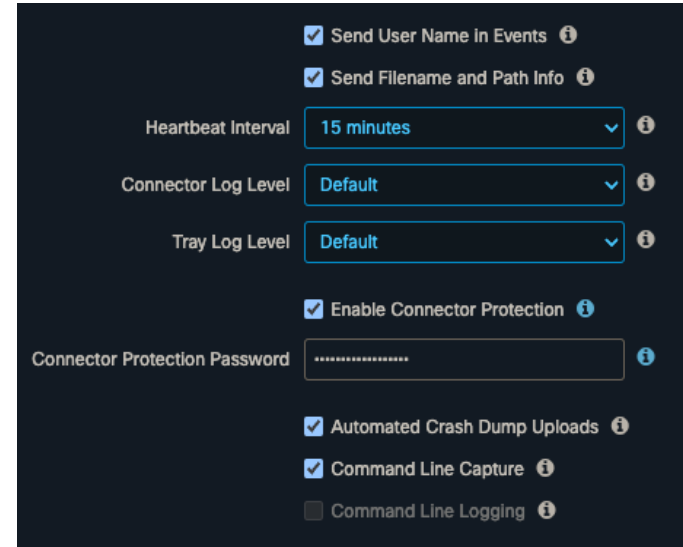
Advanced Settings ->
Administrative Features



Advanced Policy Settings for Linux/MAC - File and Process Scan:

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

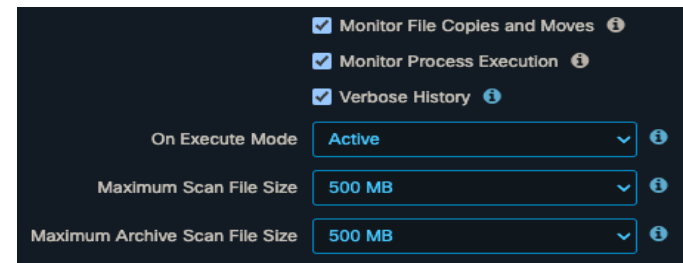
Windows



Advanced Policy Settings for Windows:

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

Advanced Settings -> File
and Process Scan

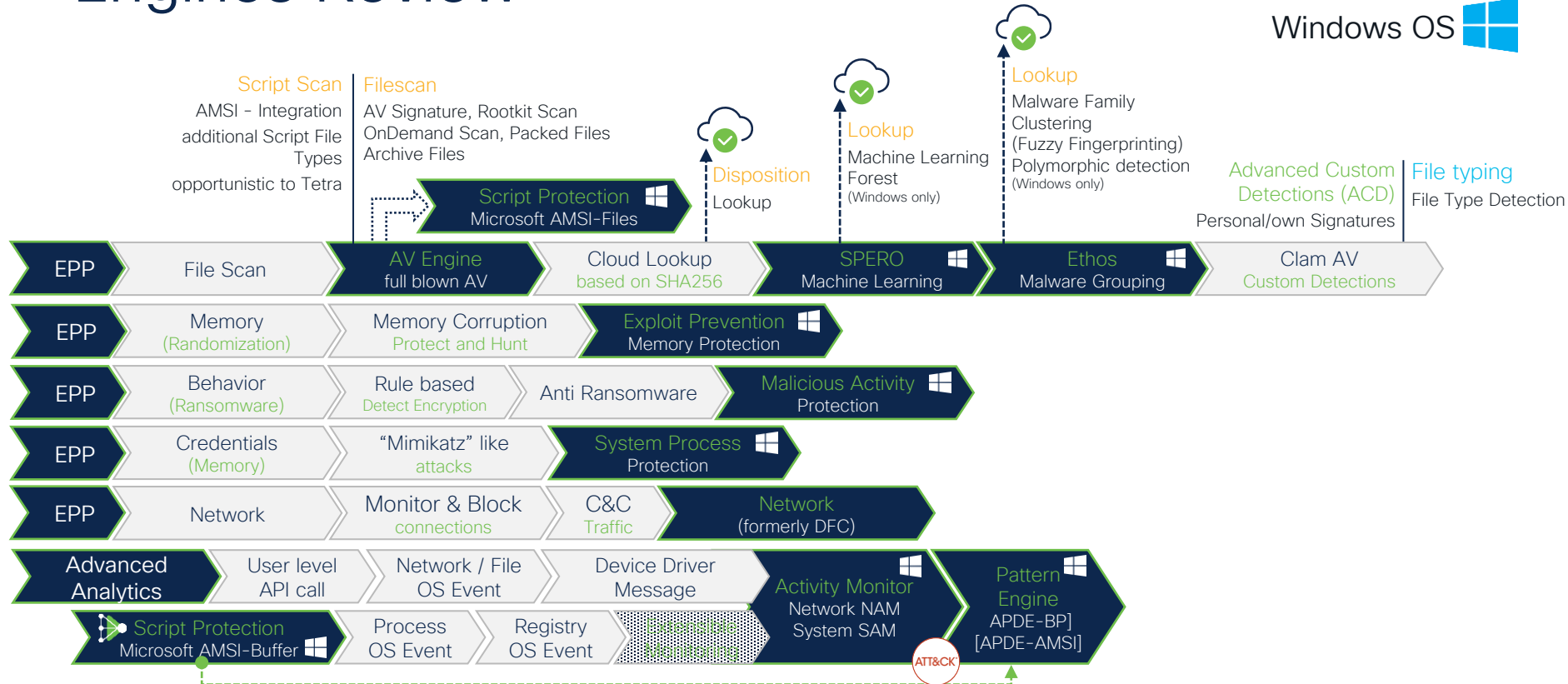


Advanced Policy Settings for Windows - File and Process Scan:

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

Engines Review

Windows OS 

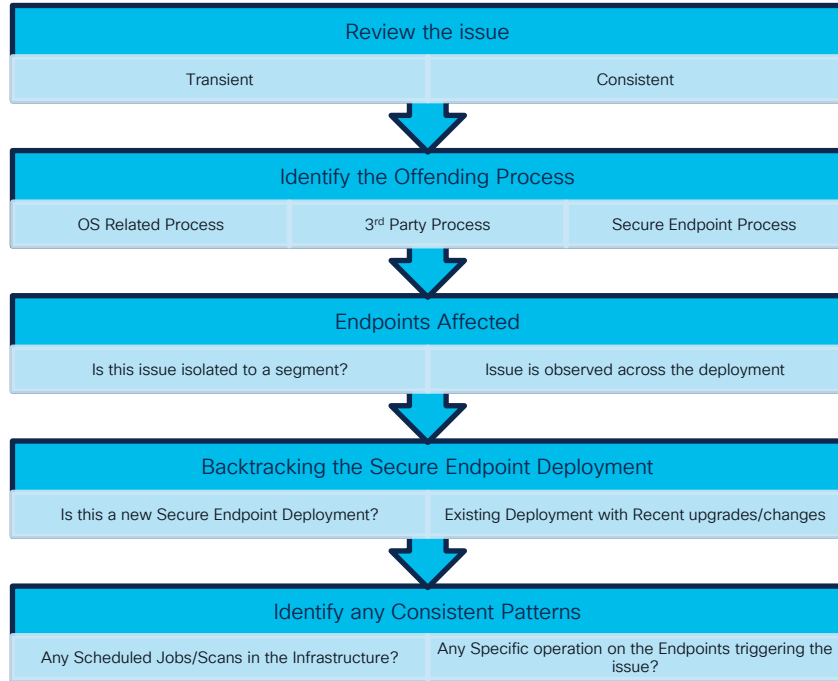


Troubleshooting Methodology

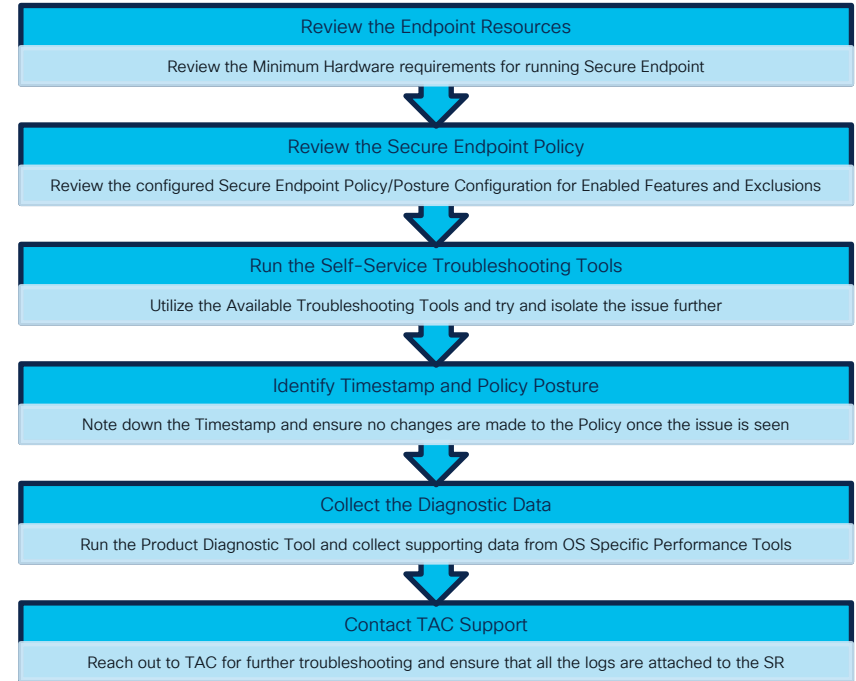


Isolating the Problem

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 screenshot shows the 'Details' view of an endpoint in the Secure Endpoint console. The interface includes a top navigation bar with 'Definitions Up To Date' and a search bar. Below the navigation bar is a table with endpoint details:

Hostname	Group
Windows 11, SP 0.0 (Build 22000.1696)	Policy: All Inclusive Policy - Windows
Connector Version: 8.1.7.21417	Internal IP: [Redacted]
Install Date: 2022-08-16 18:29:10 CDT	External IP: [Redacted]
Connector GUID: [Redacted]	Last Seen: 2023-04-25 18:24:22 CDT
Processor ID: 1f8bfbf000006f1	Definition Version: TETRA 64 bit (daily version: 90471)
Definitions Last Updated: 2023-04-25 13:23:16 CDT	Update Server: tetra-defs.amp.cisco.com
Cisco Secure Client ID: [Redacted]	Kenna Risk Score: [Redacted]

At the bottom of the details view, there are several buttons: 'Take Forensic Snapshot', 'View Snapshot', 'Orbital Query', 'Events', 'Device Trajectory', 'Diagnostics' (highlighted with a red box), 'View Changes', 'Start Isolation', 'Scan...', 'Diagnose...' (highlighted with a red box), 'Move to Group...', and 'Delete'.

The screenshot shows the 'New Connector Diagnostic' dialog box. It includes a 'Debug session' dropdown set to '5 minutes', and two checked options: 'Historical Data' and 'Kernel Log'. A warning message in a red box states: 'Diagnostic files are limited to 50MB in size and can take up to 24 hours to generate.' At the bottom right, there are 'Cancel' and 'Create' buttons.

D 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:

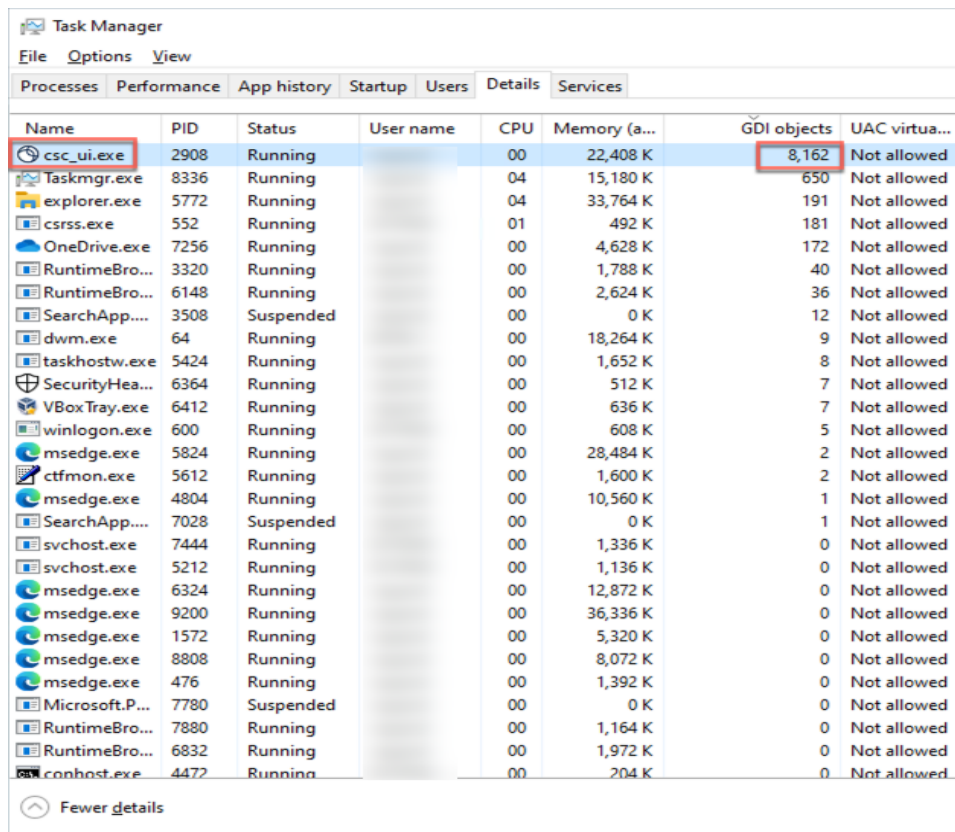
Windows Application Sluggishness

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

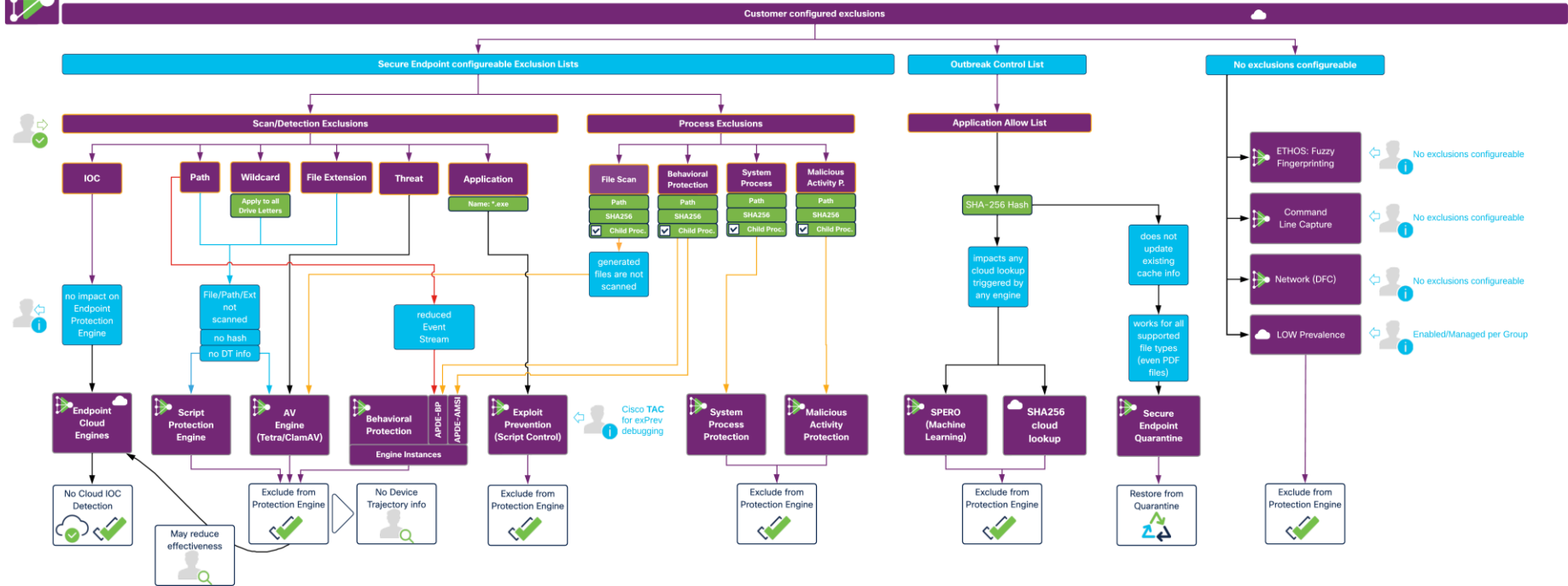


Name	PID	Status	User name	CPU	Memory (a...	GDI objects	UAC virtua...
csc_ui.exe	2908	Running		00	22,408 K	8,162	Not allowed
Taskmgr.exe	8336	Running		04	15,180 K	650	Not allowed
explorer.exe	5772	Running		04	33,764 K	191	Not allowed
csrss.exe	552	Running		01	492 K	181	Not allowed
OneDrive.exe	7256	Running		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



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

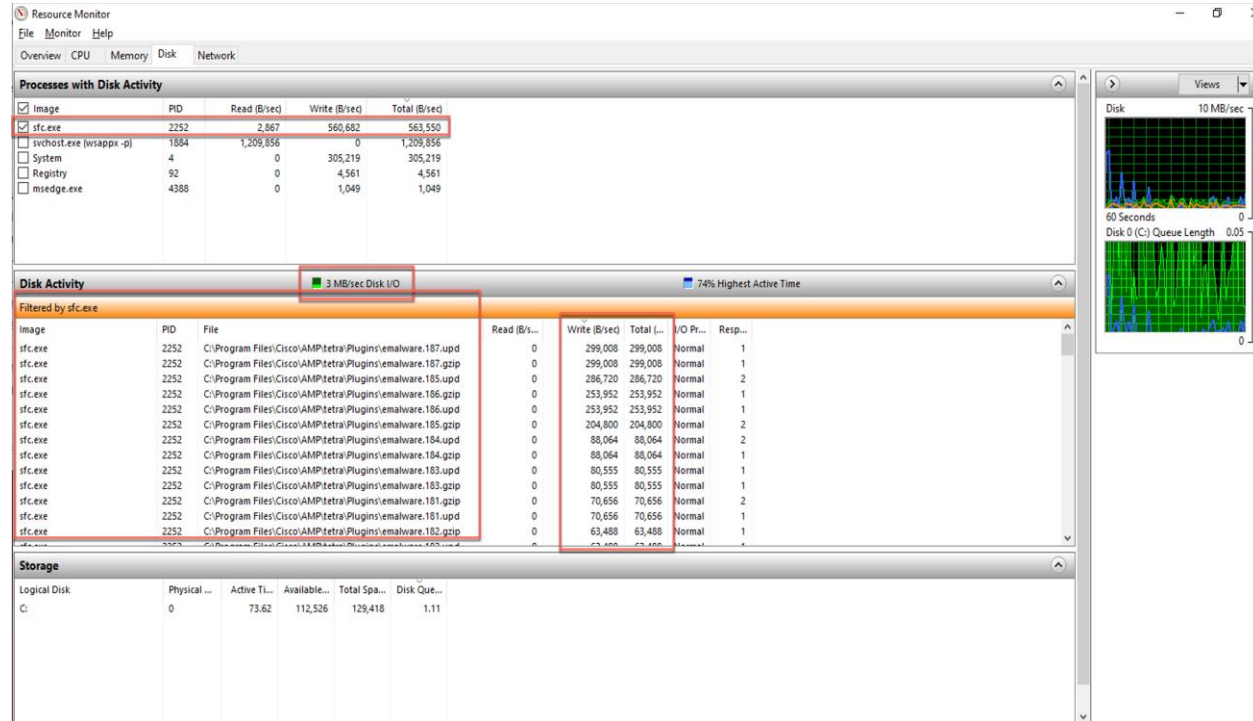
- Use Cisco Maintained Exclusions: <https://cs.co/9002OTQVp>
- **AVOID** using Exclusion for Possible Performance Gains
- Trim the Custom Exclusions as much as possible for increased Security and Visibility

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

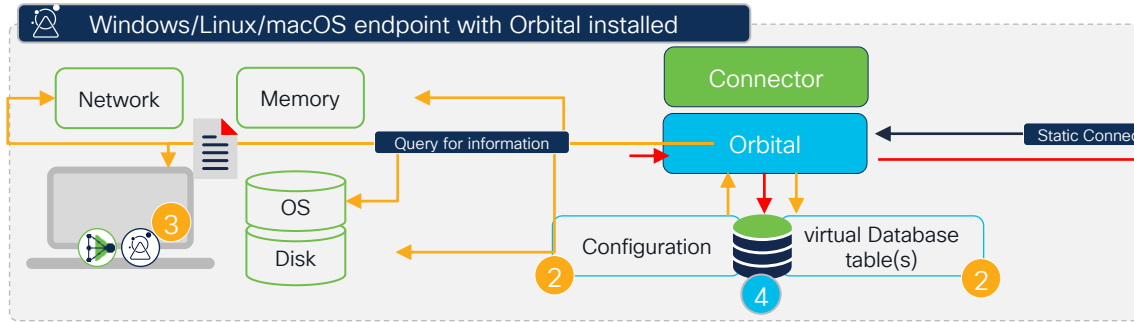


Secure Endpoint Orbital Queries

- ▶ installed programs
- ▶ running programs
- ▶ established network connections
- ▶ startup items
- ▶ file search
- ▶ firewall status

- ▶ Application Shims
- ▶ LLMNR Monitoring
- ▶ Low Privilege File Associations
- ▶ Malware Trickbot Mutex
- ▶ Parent Process not Explorer
- ▶ Log4j Monitoring

- ▶ Select column1, column2
from
Orbital_SQL_Table(s);



- 1 Analyst types a **SQL** statement (catalog). Or automated investigation triggered by the **Threat Hunting Service** or **Endpoint Pro Service**

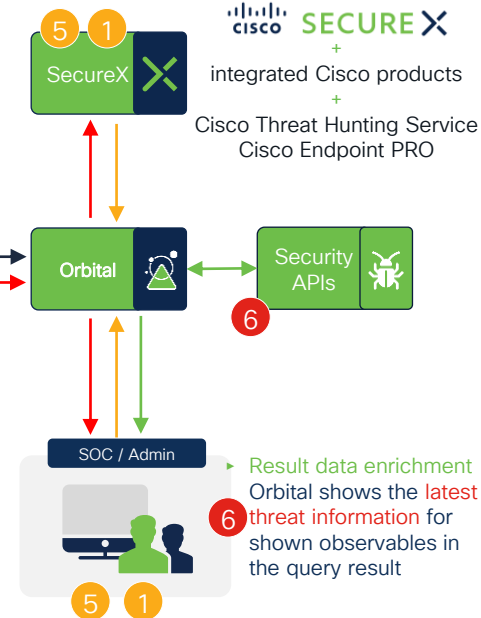
- 1 **Orbital Cloud** gets triggered by a **SecureX** integrated product or during an Orchestration Workflow

- 2 **Orbital Process** generates an empty virtual table and looks at the configuration behind

- 3 **Orbital Process** queries the right information from several sources from the endpoint

- 4 The **information** is written to the virtual Database(s) and the **SQL** statement gets executed. After the information is sent to the backend the virtual table is removed from memory

- 5 **Orbital Cloud** provides the query result to the analyst or to integrated products.



Processes/Services observed on Endpoints

Windows: osquervd.exe

Linux/Mac: osqueryd

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

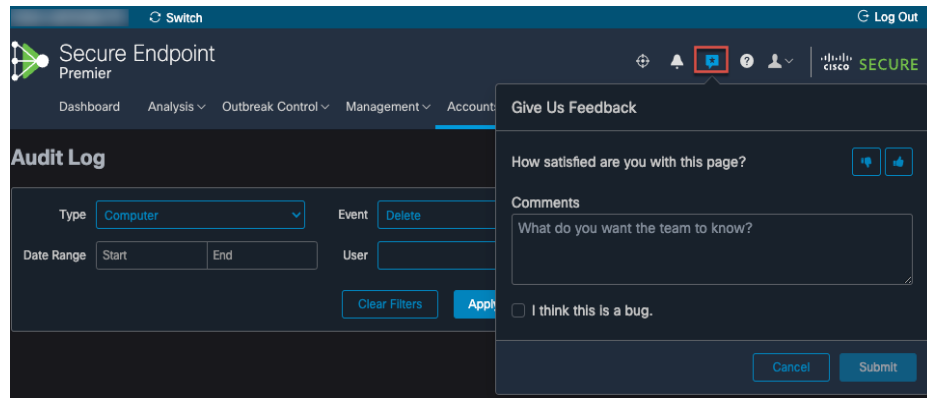
Final Words

- 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



- 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

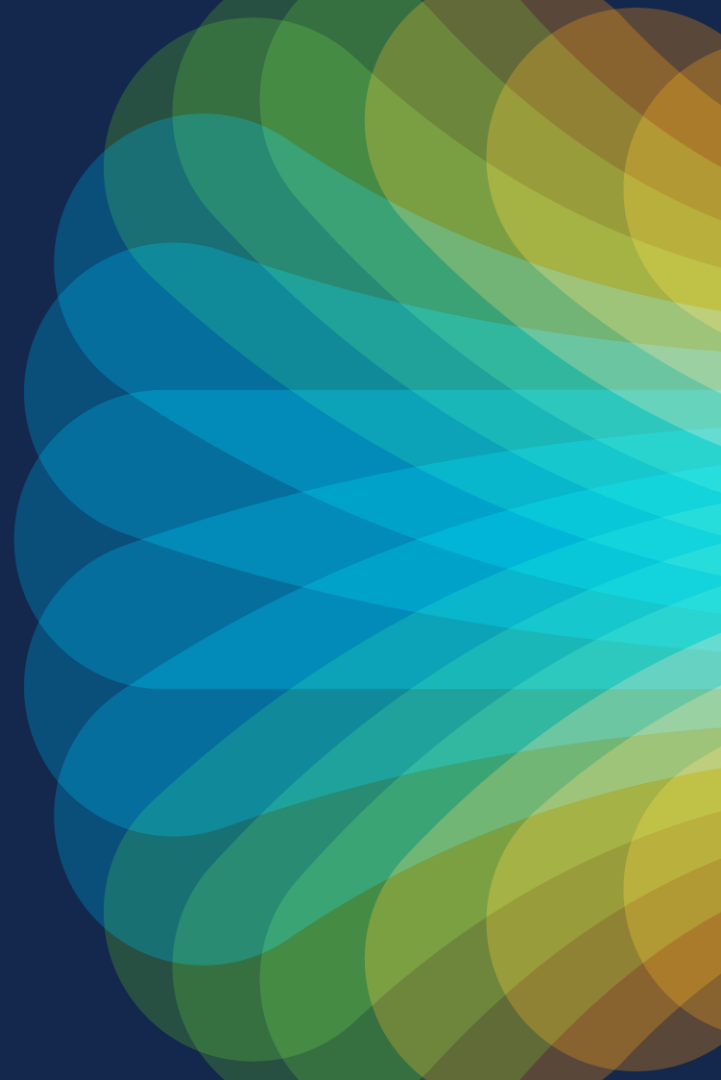


The bridge to possible

Thank you

CISCO *Live!*

#CiscoLive

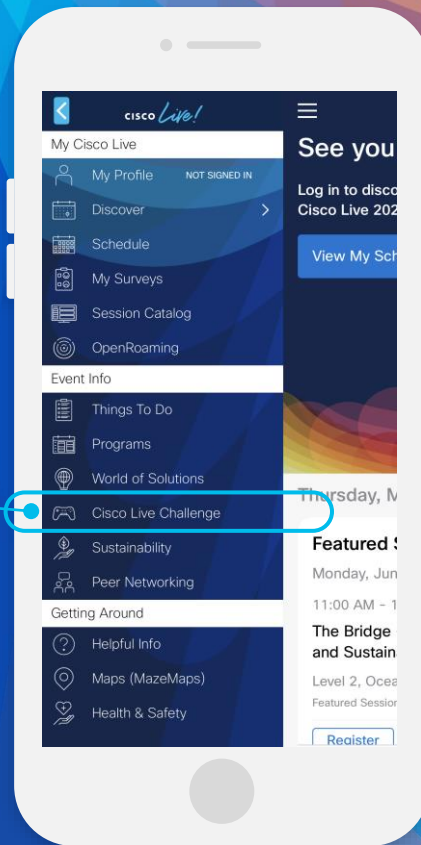
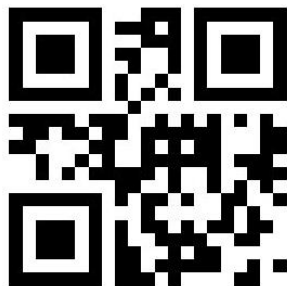


Cisco Live Challenge

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:



The background is a vibrant, abstract graphic. It features a central bright white light source from which numerous colorful rays emanate, creating a sunburst or starburst effect. The rays transition through a spectrum of colors including yellow, orange, red, and various shades of blue and green. Overlaid on this are large, flowing, wavy shapes in similar colors, giving the overall impression of energy, movement, and a digital or network theme.

cisco *Live!*

Let's go

#CiscoLive