



The bridge to possible

Malware Defense Cloud & Secure Malware Analytics Integrations

Bill Yazji – Technical Security Architect

byazji@cisco.com |  @BillYazji |  billyazji

BRKSEC-1105

CISCO *Live!*

#CiscoLive

Abstract

The artists known as "AMP Cloud and Threat Grid", are now called Malware Defense Cloud and Secure Malware Analytics. This session will review and take a dive deep into the Malware Defense Cloud and Malware Analytics offerings while covering their integrations with Cisco security architectures, including Secure Email, Secure Web, Secure Firewall, Secure Endpoint, Umbrella and Meraki. These products work together, and we will be covering the Malware Defense Architecture and demonstrate how all of the pieces fit together to provide the industry leading Advanced Threat Architecture. This session is perfect for those who are newer to the Cisco Security Suite, as well as those customers who own one or more products and want to learn how to connect them all to achieve operational efficiency.

#me :: “the work”

- Technical ~~Security~~ Solutions Architect
- Over 14 years with Cisco and nearly 25 years of security, cloud and networking experience
- Global lead for Secure Client Technical Advisory Group
- Life before Cisco...
 - Cisco competitor in Web Security space
 - Network and Security Consultant on the customer side
 - Large design, deployment, integration and troubleshooting focus



The “not” work...



Cisco Webex App

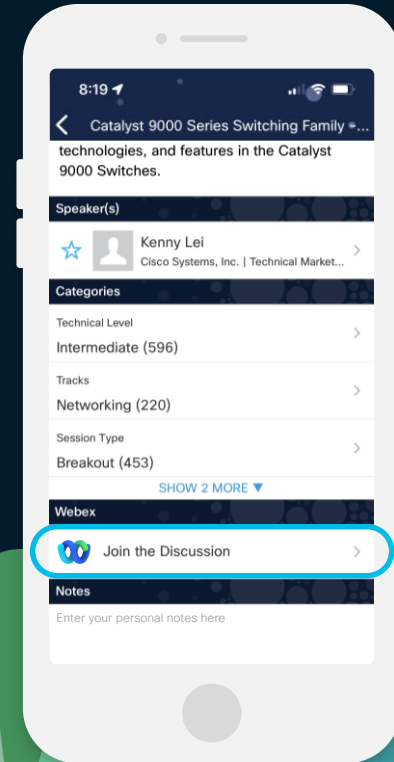
Questions?

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 7, 2024.



Please fill out the survey



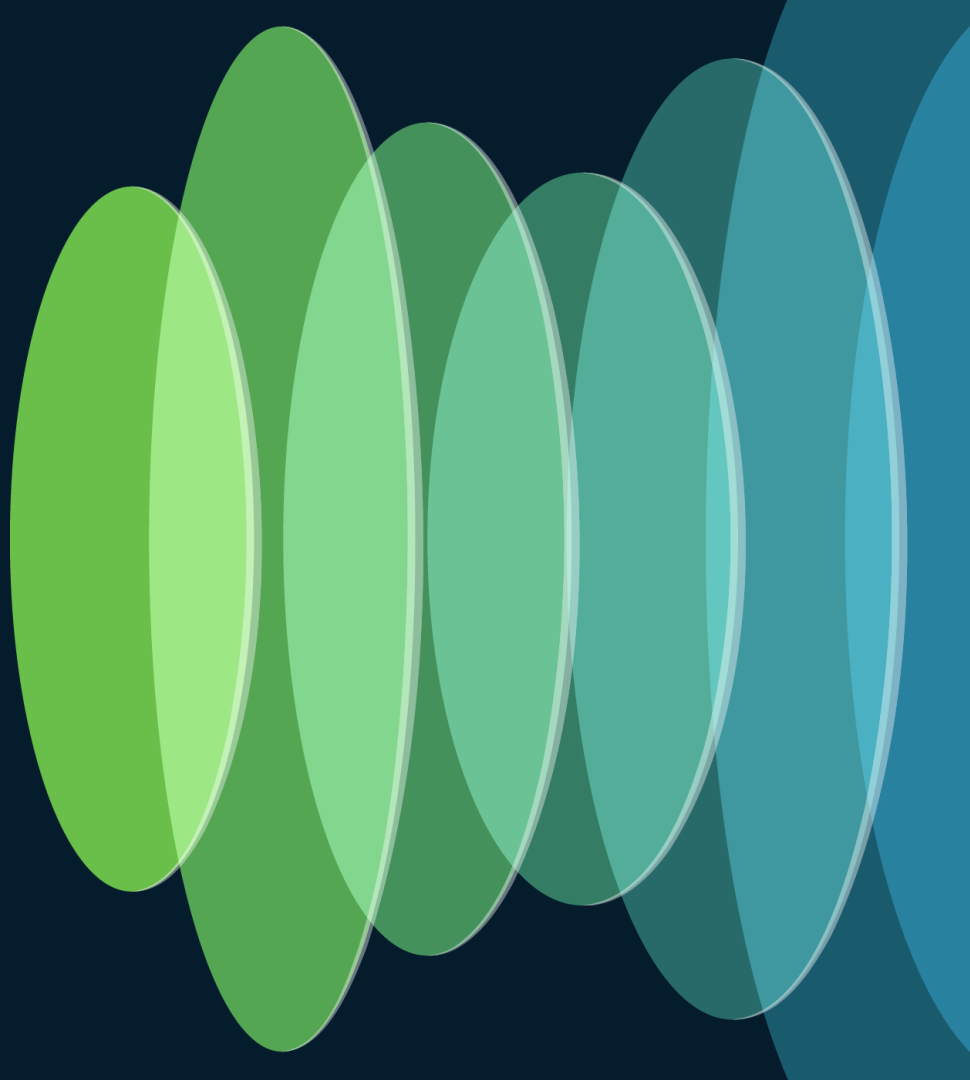
Drop your email in the comments – I WILL respond!



Agenda

- Architecture Review
- Secure Malware Analytics product tier deep dive
- APIs & Integrations with Secure Malware Analytics
- See once, block many
- Secure Malware Analytics demo dive

Architecture Review



Questions you'll be able to answer after this section:

- What is Malware Defense?
- What is Secure Malware Analytics?
- How do they create an ecosystem?
- Cloud vs. On-Prem?
- What CAN go where?
- What things should you not do?

Ecosystem Components



- **Malware Defense (AMP)** – A large database that drives **File Reputation** and **File Retrospection**
 - Cloud SaaS & Appliance
- **Secure Malware Analytics (Threat Grid)** – File Analysis and much, much more...
 - Cloud SaaS & Appliance
- **Malware Defense-Enabled Integration** – A Cisco device, 3rd party or service that queries data from Malware Defense, and submits files to Malware Analytics
- **Secure Endpoint (AMP for Endpoints)** – Cisco's EDR tool

Cisco Secure Client

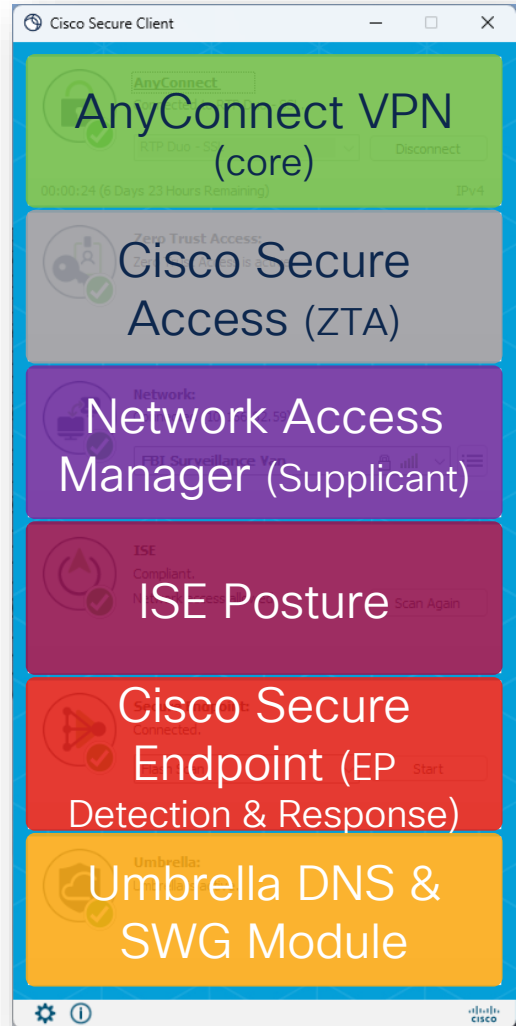
- Security Modules with UI
- Security Modules with no UI:
 - Cloud Management Module
 - Secure Firewall Posture (aka: HostScan)
 - Network Visibility Module (NVM)
 - Thousand Eyes
 - Diagnostics and Reporting Tool (DART)



Bill Yazji
Technical Architect

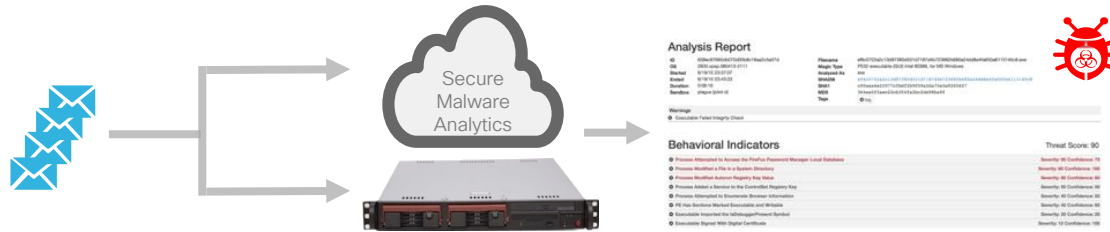
Cisco Secure Client: Technical
Deep Dive

BRKSEC-2834
Thursday, June 6



Secure Malware Analytics

- Secure Malware Analytics is Cisco's unified malware analysis and threat intelligence platform.



- Flexible Deployments: Cloud SaaS or On-Premise Appliance
- Submissions through Web Portal, Malware Defense-Enabled Device or API
- API automates sample analysis, enrichment and reporting
- Full Integration with Cisco and 3rd Party SIEM and Threat Solutions

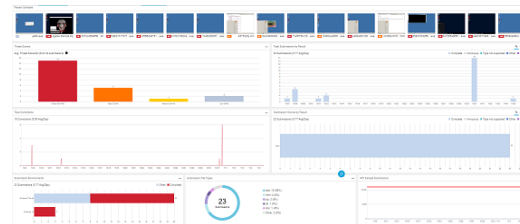
Integration Use Cases

- Submit Samples for Analysis
- Query Malware Intelligence
- Retrieve Curated Intelligence Feeds
- Usage Statistics and Data



Malware Analytics API

Malware Analysis & Threat Intelligence



Secure Malware Analytics Integrations

Submit Samples & Receive Analysis Results



SOAR



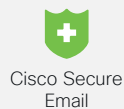
Network



Endpoint



Email



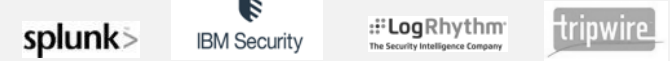
Deception



Visualization of Submitted Samples



SIEM



Threat Visualization/ Response



Threat Intelligence Feeds



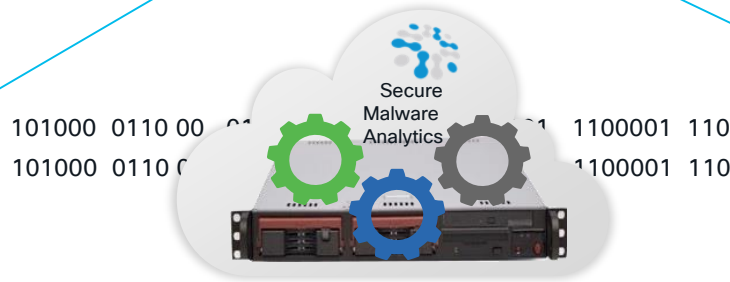
Unsupported Python Integrations



Secure Malware Analytics

- ...performs automated static and dynamic analysis ...

What it is..
What it **contains**...
File on disk – header
details/AV engines



An automated engine observes, deconstructs,
and analyzes using multiple techniques

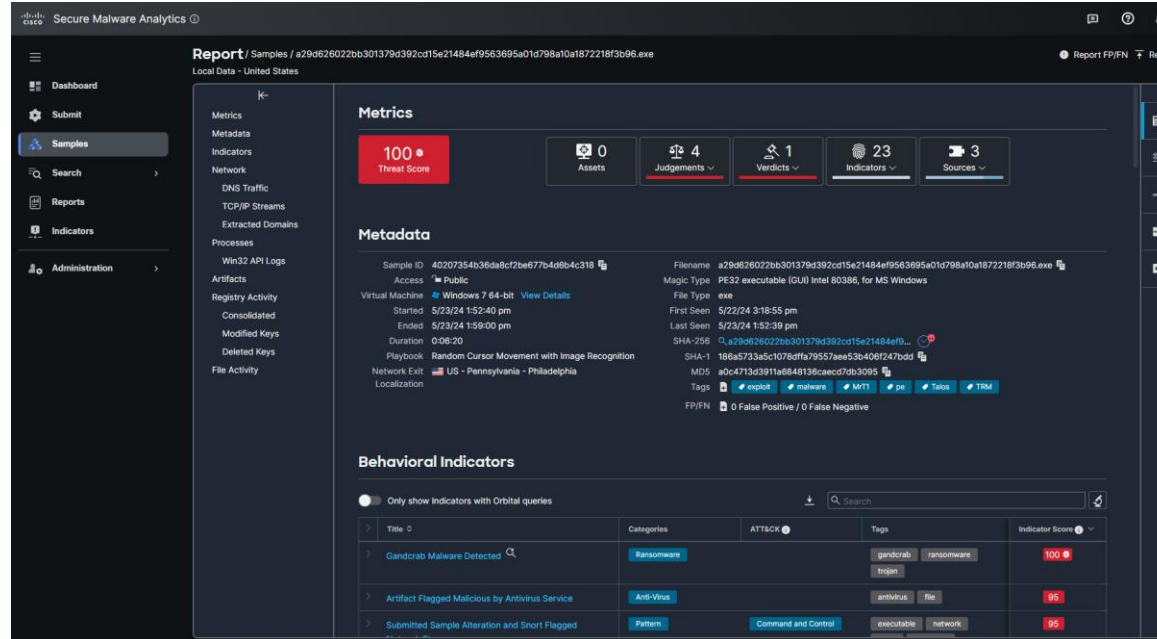
What it **does**..
Execution/Detonation
File/System changes
Function/Library calls

- “Outside looking in” approach / No presence in the virtual machine
- Observes & records all activity
- Wide range of supported file types
- Network Exit Localization, Playbooks and Evasion Behavior Indicators
- Fully interactive sample submission experience (Glovebox)

Secure Malware Analytics

...produces human readable report for submissions.

- 2500+ behavioral indicators
- Malware families, malicious behaviors, and more (not just signatures)
- Detailed description and actionable information
- MITRE ATT&CK data inputs
- Integration with Secure Endpoint Orbital queries

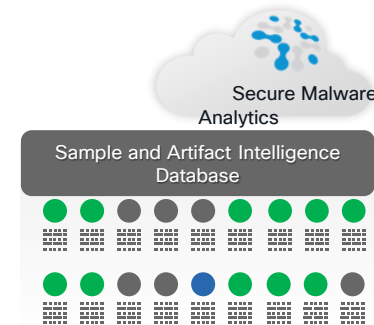


Secure Malware Analytics

- Secure Malware Analytics' global scalability drives context rich information that can be consumed directly by analysts and researchers or via content rich threat intelligence feeds.

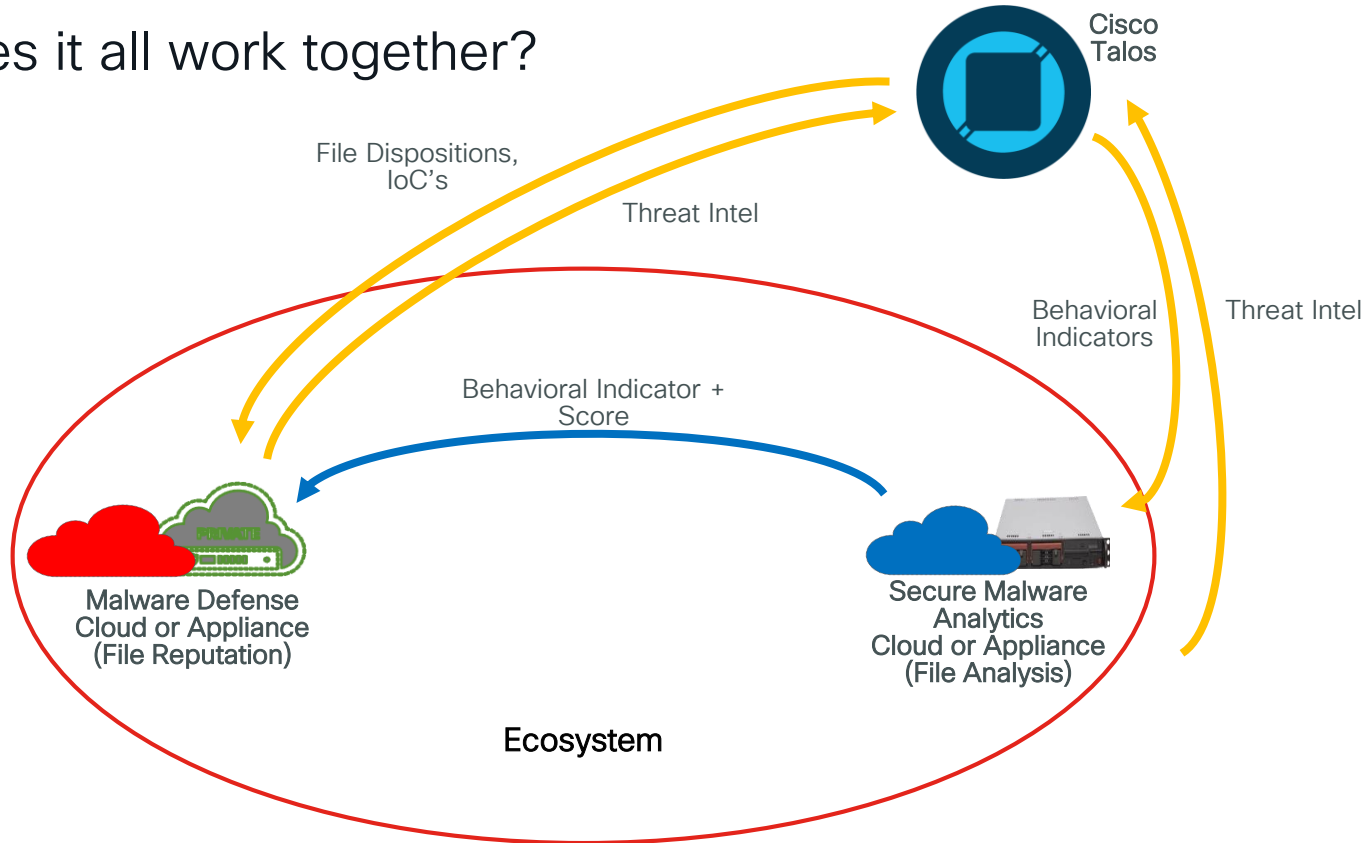
- Samples correlated with billions of malware artifacts
- Global / historical context on threat landscape
- Create custom feeds with context/metadata
- Download curated feeds
- Various formats (JSON, CyBOX, STIX, CSV, or Snort rules)

Automation saves time for the analyst



Malware Defense and Malware Analytics Integration

How does it all work together?

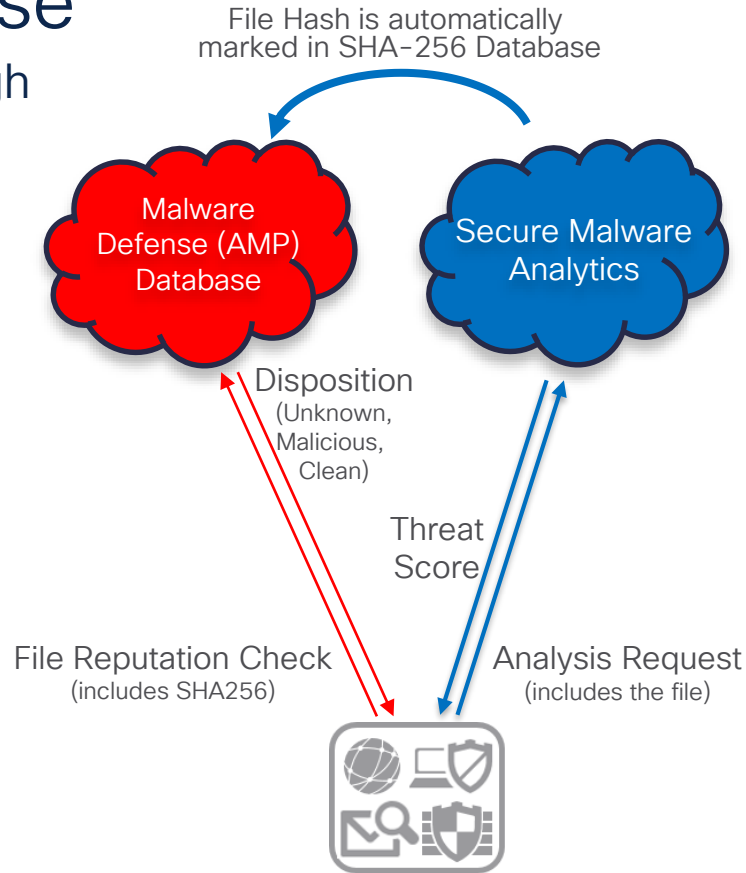


Integrations & Capabilities

Service	 File Reputation	 File Analysis	 File Retrospection
Secure Firewall	✓ Active Blocking during Transport	✓ Informative, Manual Remediation	✓ Informative, Manual Remediation
Secure Email	✓ Active Blocking during Transport	✓ Active Blocking with Quarantine	✓ Manual Or Automatic Remediation with O365, and Exchange
Secure Web	✓ Active Blocking during Transport	✓ Informative, Manual Remediation	✓ Informative, Manual Remediation
Meraki MX	✓ Active Blocking during Transport	✓ Informative, Manual Remediation	✓ Informative, Manual Remediation
Umbrella / SSE	✓ Active Blocking during Transport	✓ Informative, Manual Remediation *SWG Only*	✓ Informative, Manual Remediation *SWG Only*
Secure Endpoint	✓ Active Blocking at Create, Copy, Move, Execute	✓ Low Prevalence Exe + Manual Submissions	✓ Automatic Remediation

Malware Defense

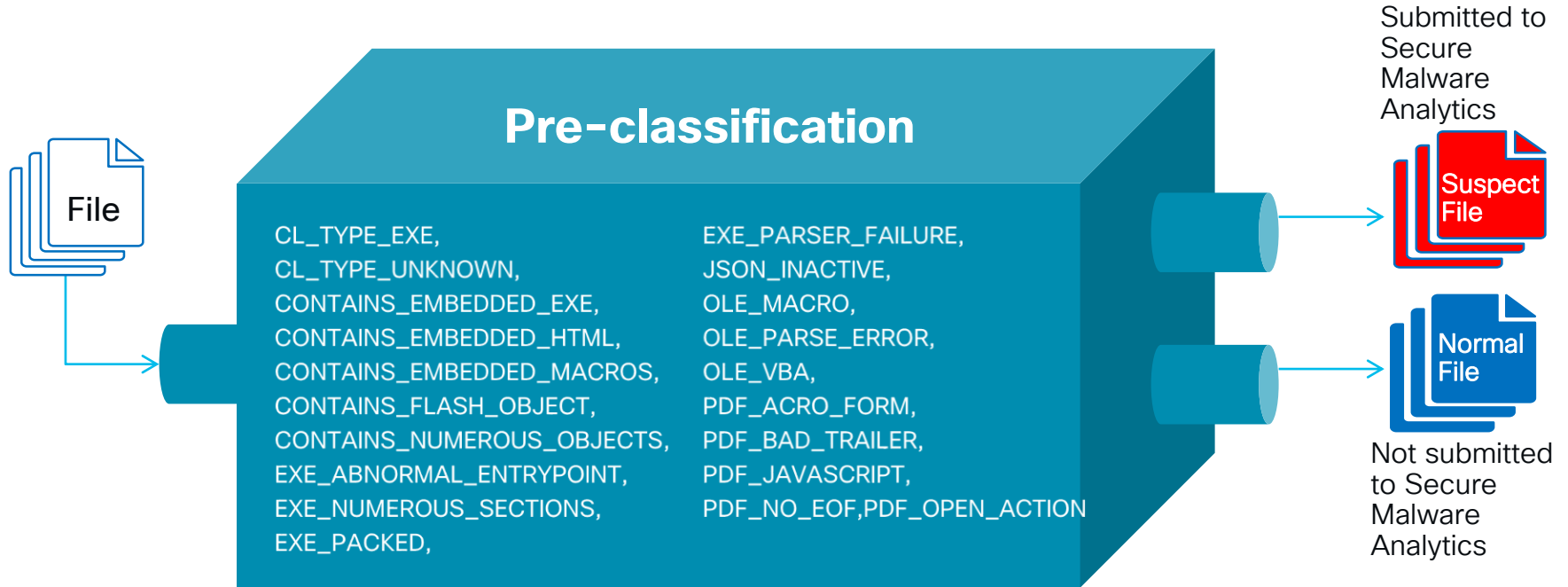
Integration Walk Through



← File Analysis
← File Reputation

Malware Defense-Enabled Integration

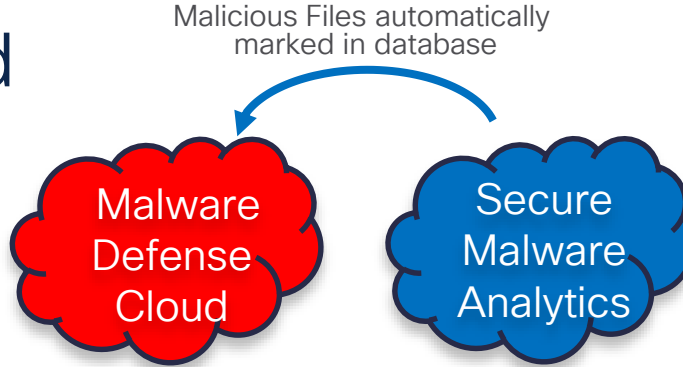
File Pre-Classification



Full Public Cloud

Information stored:

- Hashes
- Device GUID



Information stored:

- Files and Device GUID
- Analysis Results and Reports

Organization's Perimeter

- ← File Analysis
- ← File Reputation

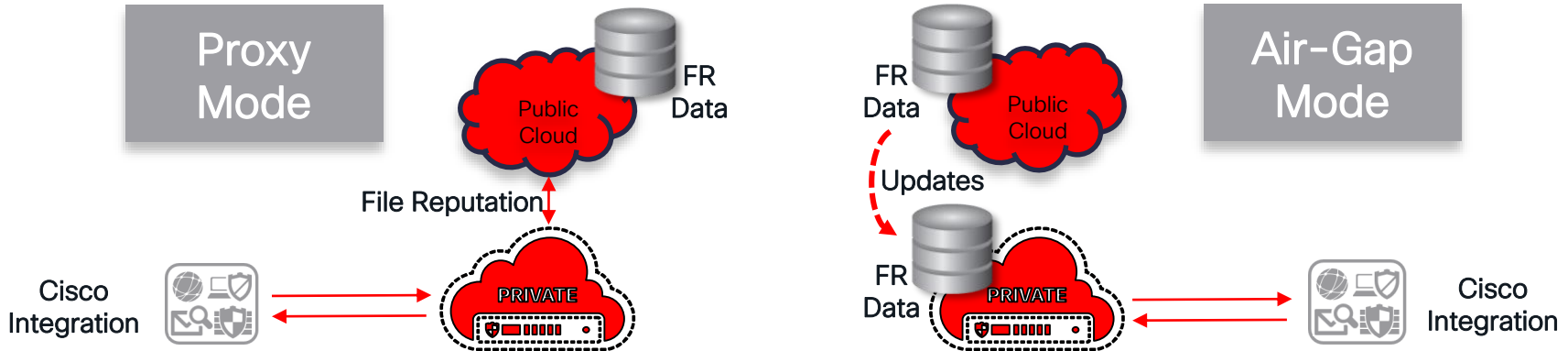


Malware Defense Enabled Integration

Secure Endpoint Private Cloud

Two Deployment Options

- The File Reputation (FR) database provides the foundation for the solution
- Available as a standalone appliance or virtual appliance
- Delivers many of the cloud features with a dedicated instance on premise
- Great for environments with very high data privacy requirements (Air Gap)
- Private Cloud Appliance can be deployed in two ways:



Secure Malware Analytics Appliance

- Appliance and Cloud user experience parity
- Aggressive compute to permit concurrent sample analysis
- License scaling from 500 to 10,000 submissions per day, per appliance.

- TG-M6



- Appliances can be clustered for redundancy and increased capacity with cluster licensing for up to 70,000 samples per day

Cisco Secure Malware Analytics

Appliance vs. Cloud

Secure Malware Analytics **Appliance**

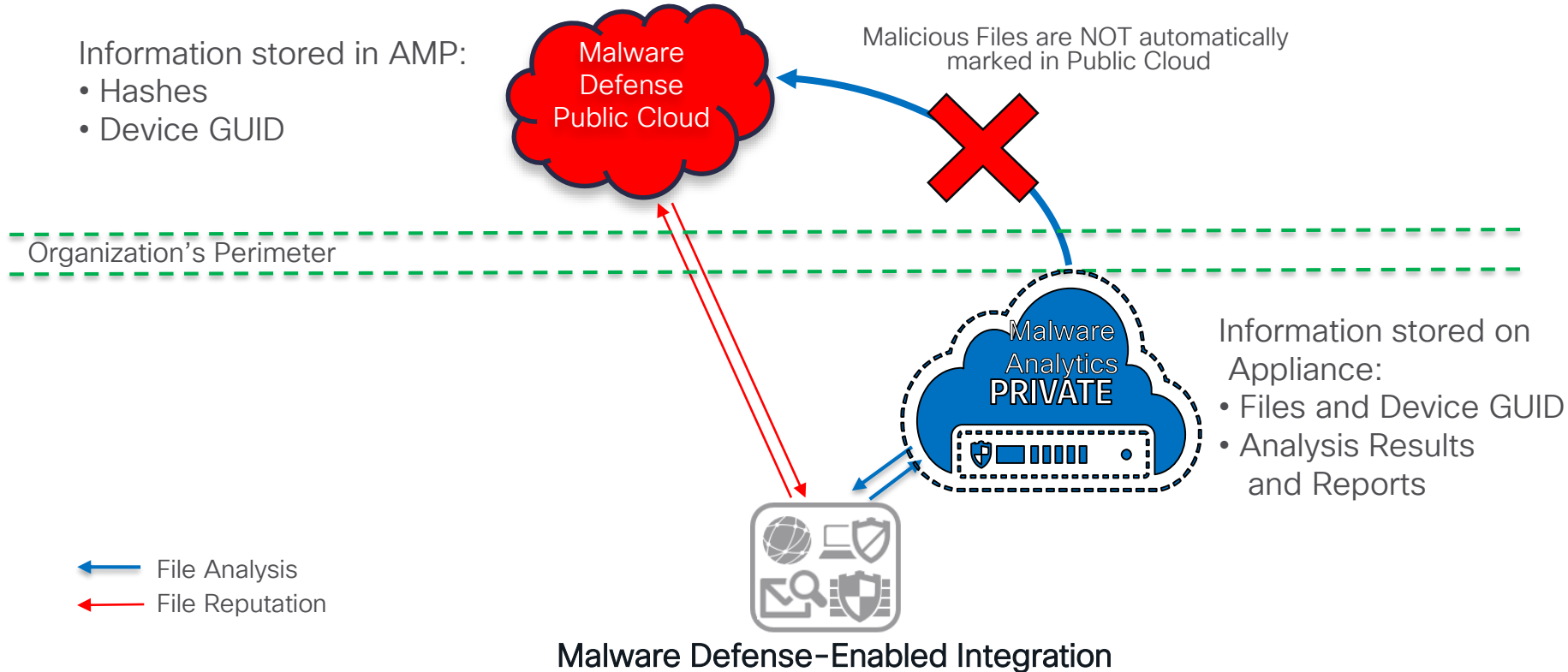
- All samples & artifacts are local - **no data is sent to the cloud**
- Pivoting on samples and artifacts is only based on local data
- Malicious marking can only be achieved with Private Cloud and has only local relevance
- Submission Limits based on appliance platform and license purchase

Secure Malware Analytics **Cloud**

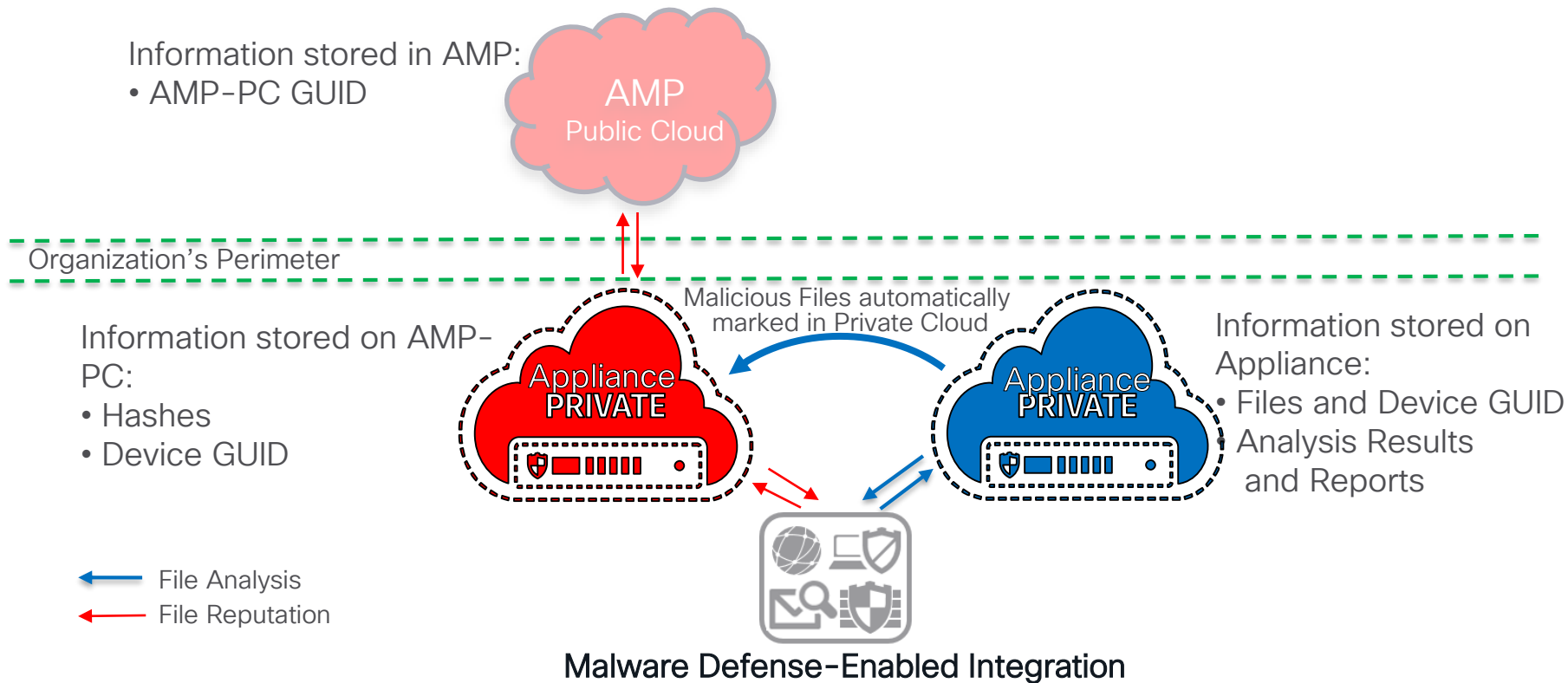
- Manual and API Samples are submitted either as Private or Public (depending on Tagging)
- Malware Defense-Enabled Integrations (Secure Email/Web/Firewall/Endpoint) are **ALWAYS** marked private
- Public data can be pivoted on, but is still anonymous on who submitted the sample
- Curated Feeds
- Submission Limits based on purchased amount, easily scalable as needs grow

Hybrid Deployments

(Except Secure Endpoint)

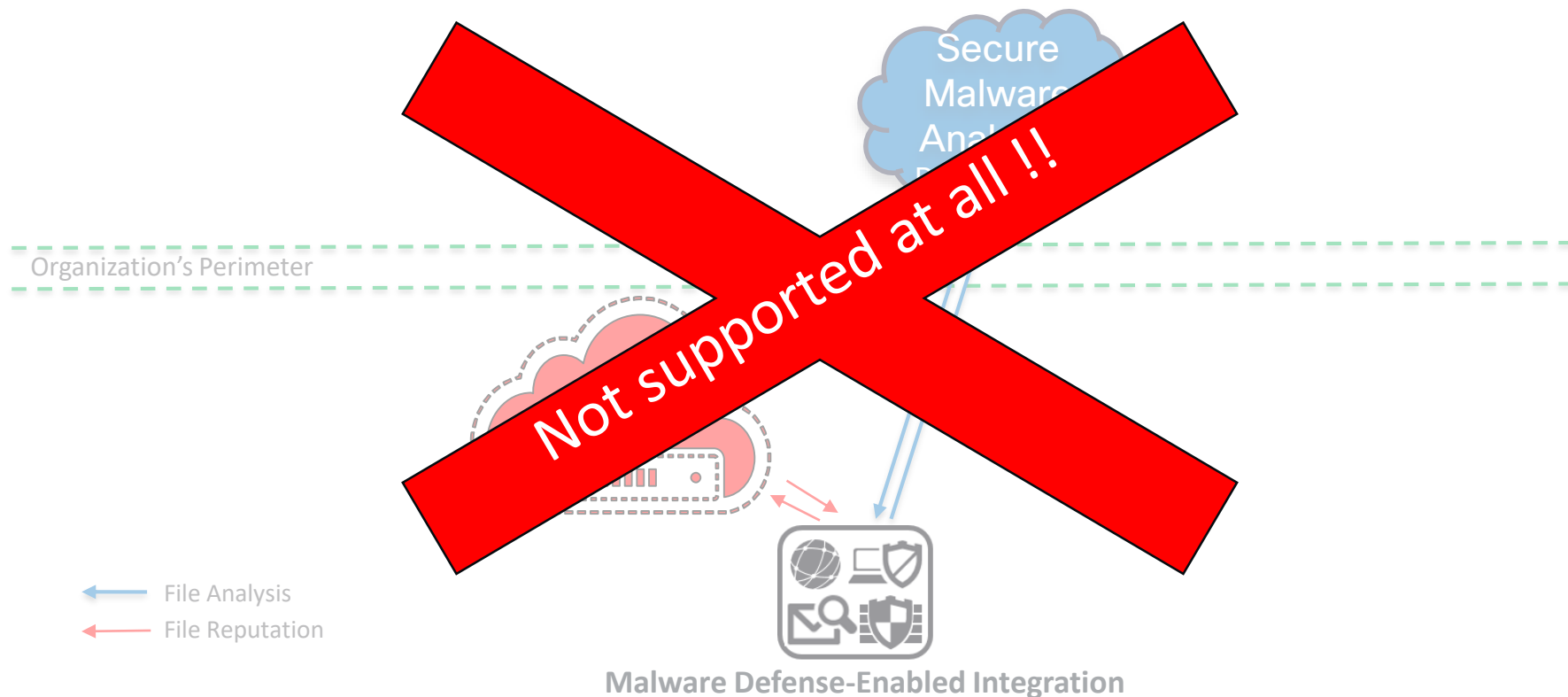


Full Private Cloud for Integrations



AMP Deployments

Hybrid for Integrations



Deployment Options

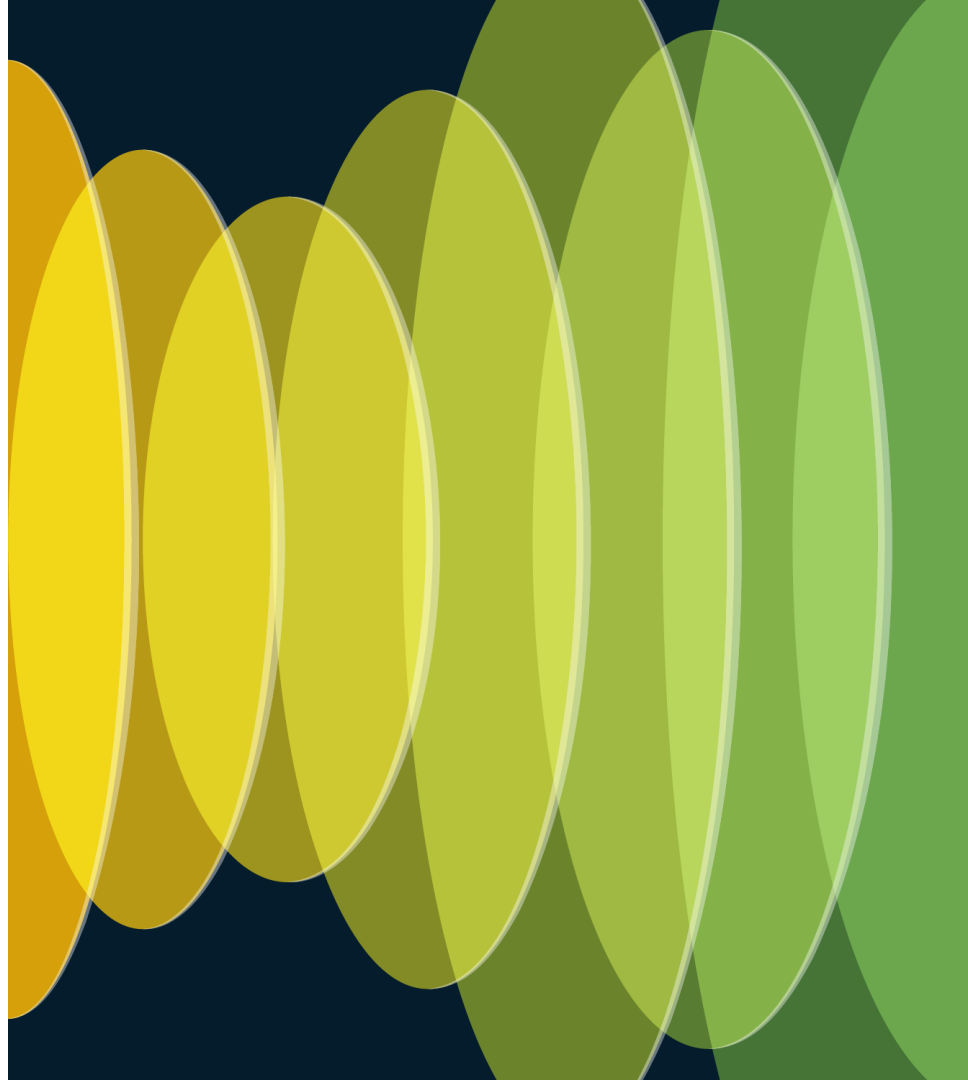
Deployment Option	Full Public MD Cloud + MA Cloud	Full Private MD PC + MA Appliance	Hybrid MD Cloud + MA Appliance	Hybrid MD PC + MA Cloud
Secure Endpoint	✓	✓	✗	✗
Secure Firewall	✓	✓	✓	✗
Secure Email	✓	✓ *ESA Only	✓	✗
Secure Web	✓	✓	✓	✗
Meraki MX	✓	✗	✗	✗
Umbrella / SSE	✓	✗	✗	✗

✓ – recommended deployment option, Full Private for customers with high privacy requirements
✓ – supported, but has drawbacks, Malware Analytics Appliance does not talk to the Public Cloud (does not share analysis results)
✗ – not supported

Caution!
Breaks the architecture!

Doesn't really make sense...

Secure Malware Analytics Product Tiers

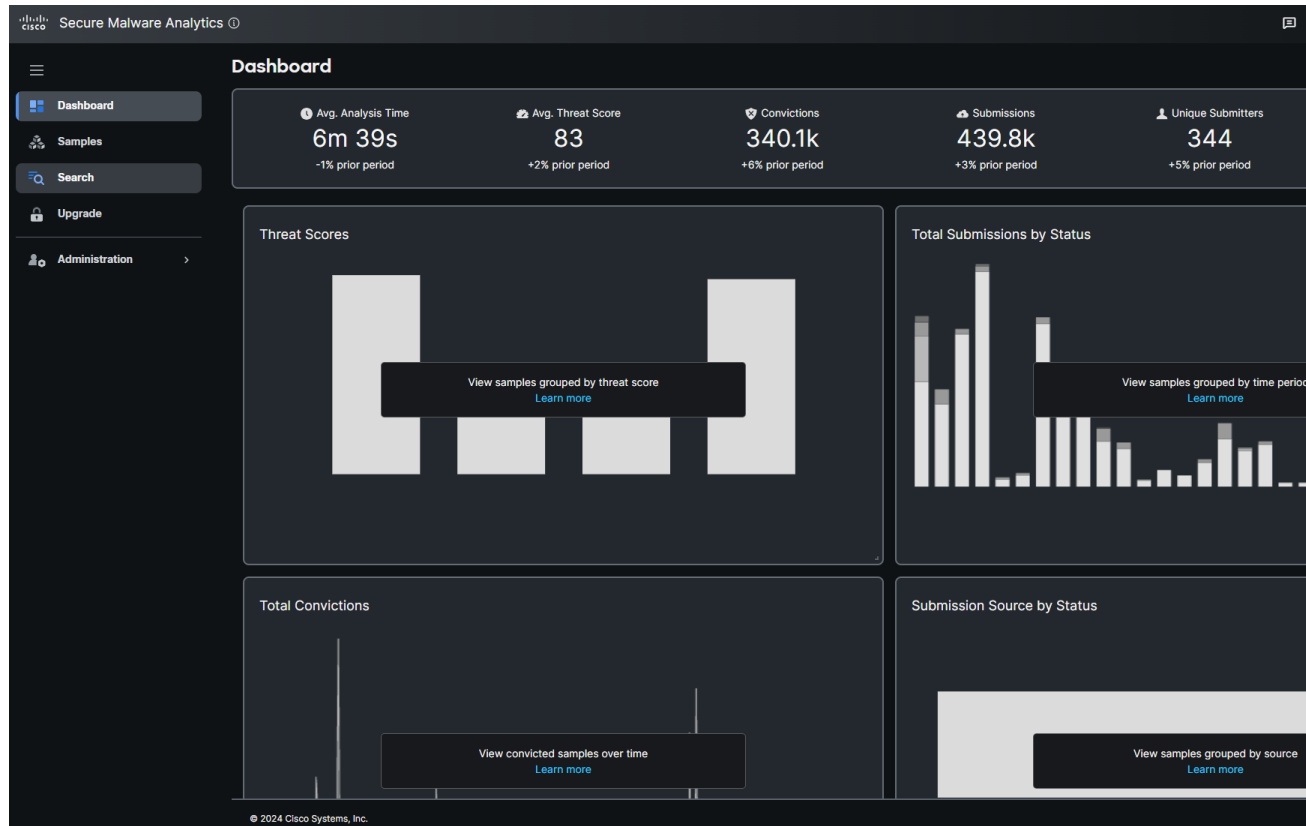


Questions you'll be able to answer after this section:

- What Secure Malware Analytics is 'included' with a Malware Defense-Enabled integration?
- Secure Malware Analytics Cloud full portal vs. Malware Defense-Enabled integration?
- Can I integrate with 3rd party products? How?
- Secure Malware Analytics offers different types of portal views?!?
- How do I integrate my Malware Defense-Enabled devices to Secure Malware Analytics Cloud?

Secure Malware Analytics Entitlement Portal

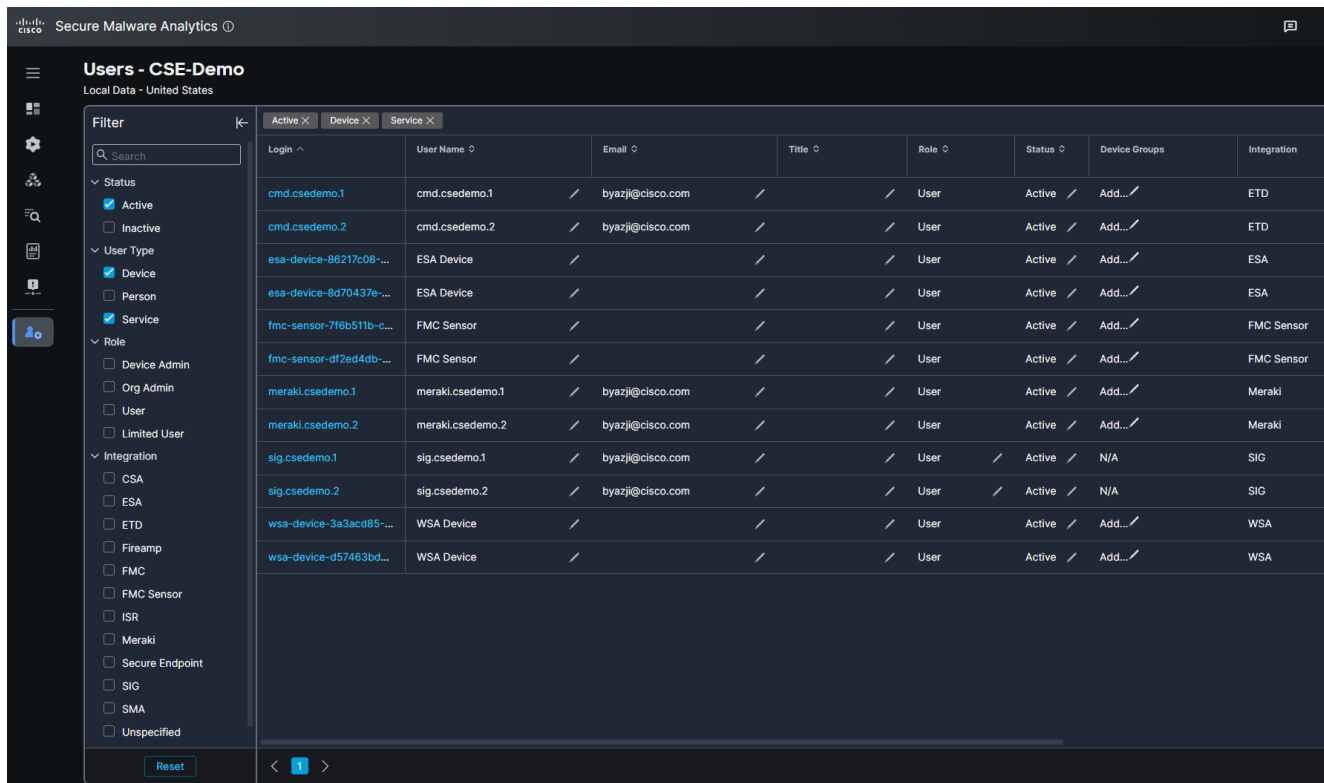
- No-cost access for all Malware Defense-Enabled customers who do not have Secure Malware Analytics Cloud
- 'Device_Admin' account that provides a *limited view* of the Secure Malware Analytics Cloud portal
 - Sample Consumption per 24 hours
 - Basic Dashboard – Avg. Analysis Time, Avg. Threat Score, Convictions, etc.



Secure Malware Analytics Entitlement Portal

“Device & Service” View

- View all devices and cloud services in an organization
 - Device detail
 - API Limits
 - Amount Consumed
 - Remaining
- Ability to self-configure device limits from organizational total



Secure Malware Analytics

Users - CSE-Demo

Local Data - United States

Filter

Search

Active ☒ Inactive ☐

User Type ☒ Device ☐ Person ☐ Service ☒

Role ☐ Device Admin ☐ Org Admin ☐ User ☐ Limited User

Integration ☐ CSA ☐ ESA ☐ ETD ☐ Fireamp ☐ FMC ☐ FMC Sensor ☐ ISR ☐ Meraki ☐ Secure Endpoint ☐ SIG ☐ SMA ☐ Unspecified

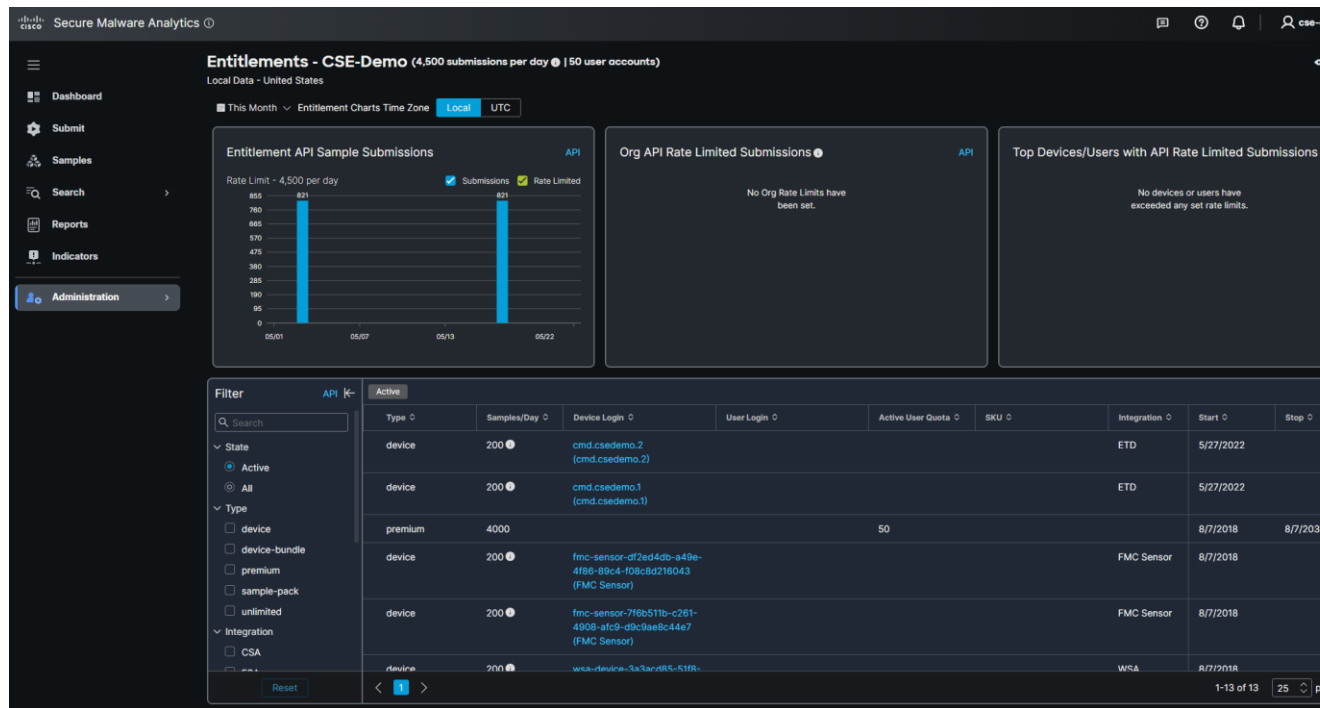
Reset

Login	User Name	Email	Title	Role	Status	Device Groups	Integration
cmd.csedemo.1	cmd.csedemo.1	byazji@cisco.com		User	Active	Add...	ETD
cmd.csedemo.2	cmd.csedemo.2	byazji@cisco.com		User	Active	Add...	ETD
esa-device-86217c08-...	ESA Device			User	Active	Add...	ESA
esa-device-8d70437e-...	ESA Device			User	Active	Add...	ESA
fmc-sensor-7f6b511b-c...	FMC Sensor			User	Active	Add...	FMC Sensor
fmc-sensor-df2ed4db-...	FMC Sensor			User	Active	Add...	FMC Sensor
meraki.csedemo.1	meraki.csedemo.1	byazji@cisco.com		User	Active	Add...	Meraki
meraki.csedemo.2	meraki.csedemo.2	byazji@cisco.com		User	Active	Add...	Meraki
sig.csedemo.1	sig.csedemo.1	byazji@cisco.com		User	Active	N/A	SIG
sig.csedemo.2	sig.csedemo.2	byazji@cisco.com		User	Active	N/A	SIG
wsa-device-3a3acd85-...	WSA Device			User	Active	Add...	WSA
wsa-device-d57463bd...	WSA Device			User	Active	Add...	WSA

Secure Malware Analytics Entitlementment Portal

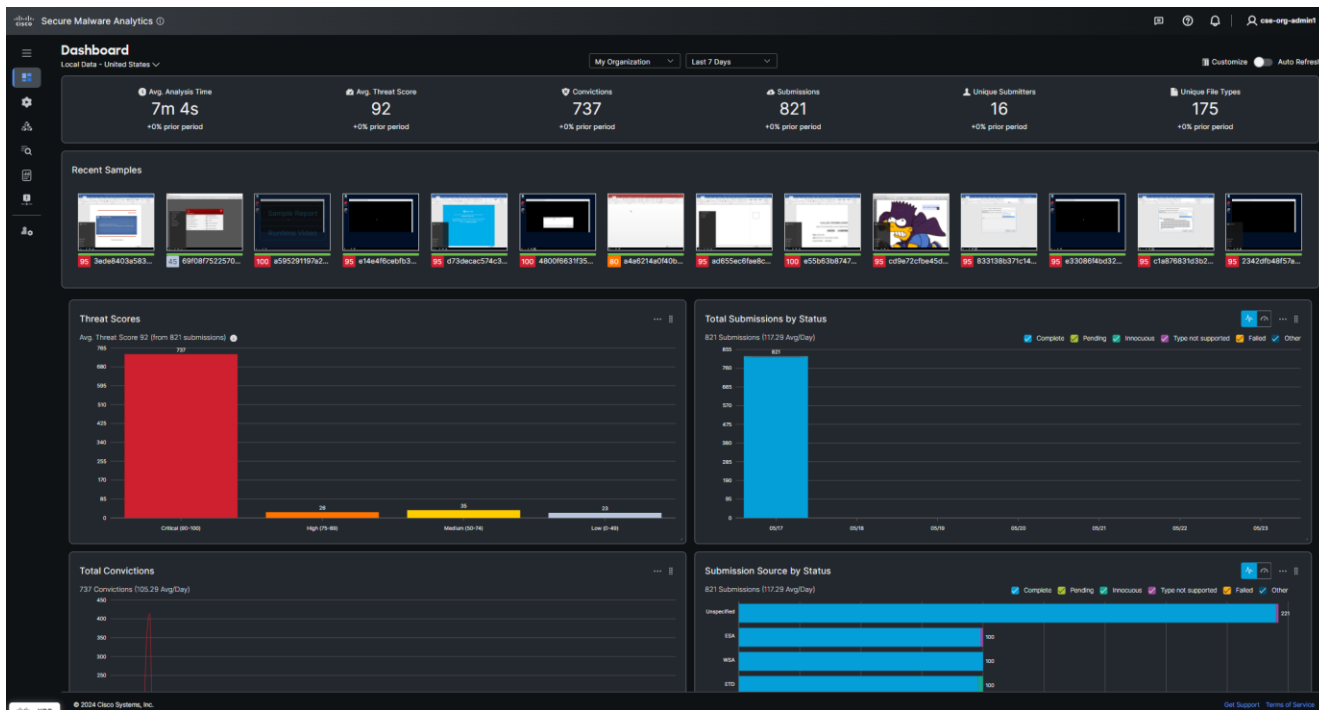
“Entitlements” View

- View all Entitlements in an organization
 - Type Samples/Day
 - Login
 - Users (if applicable)
 - Start/End date - subscription



Secure Malware Analytics Cloud

Full access portal



- Full Visibility into global views
- Submission Types
- Threat Scores
- Environmentals
- Behavioral Indicators and IP's

Secure Malware Analytics Sample Manager

Samples
Create Tags Delete Samples Downloads

Local Data - United States

Filter API

Freeform

Search

- Scope
 - All
 - My Organization
 - My Samples
- Date Range
 - Last 24 Hours
 - Last 7 Days
 - Last 30 Days
 - Last 90 Days
 - Custom Range
- Threat Score
 - Critical
 - High
 - Medium
 - Low
- Integration
 - CSA

Filename	SHA-256	Type	Tags	VM	Playbook	Threat Score	In	Access	Status	Actions
> 3ede8403a583eec1a0706c588eb0f6fe.pdf	Q2e686c0...	doc		Windows 10	Random Cursor Movem...	95				
> 69f08f752257032a5d42a3d456d5a5cc.pdf	Q2dfff05b5...	pdf		Windows 10	Random Cursor Movem...	45				
> a595291197a297989291bf604cc25456	Q2df8d6c1...	exe		Windows 10	Random Cursor Movem...	100				
> e14e4f6cebfb3ae45f4f117034c779b	Q2dbbb4d...	gz		Windows 10	Random Cursor Movem...	95				
> d73decac574c322d4f723627b3bab255	Q2db80767...	docx		Windows 10	Random Cursor Movem...	95				
> 480f6631f35b769dec24e3ffd048447	Q2da048b...	exe		Windows 10	Random Cursor Movem...	100				
> a4a8214a0f40b13f1fd5b23c0e05d1c0.exe	Q2d6ebec9...	zip		Windows 10	Random Cursor Movem...	80				
> ad655ec6fae8ccf70eb9088a2758682b.doc	Q2d440c5...	rtf		Windows 10	Random Cursor Movem...	95				
> e55b63b8747bd94a0d4867ec73eaaf6	Q2cc922f7...	doc		Windows 10	Random Cursor Movem...	100				
> cd9e72cfbe45dd237a07e5989ef9f441	Q2cda8c1d...	pdf		Windows 10	Random Cursor Movem...	95				
> 833138b371c14f407affe32b6a8c2574	Q2cb3935...	cdf		Windows 10	Random Cursor Movem...	95				
> e33086f4bd32ad44fb13e06a3a54439	Q2c95a60...	dll		Windows 10	Random Cursor Movem...	95				

Secure Malware Analytics Sample Report

- Report Data:
 - Meta Data
 - Behavioral Indicators
 - Network Activity
 - Processes
 - Artifacts
 - Registry Activities
 - File Activities
 - Cisco XDR Bar
- Deep view of sample run
 - Video of the VM session
 - PCAP from all network activities
 - Export the report in various formats
 - Download the sample and Artifacts
 - Ability to interact with sample
 - Global sample search

The screenshot displays the 'Secure Malware Analytics' web interface. The top navigation bar includes a search icon, a settings icon, and a user profile icon. The main header shows the report title 'Report / Samples / 3ede8403a583eec1a0706c588eb0f6e.pdf' and the location 'Local Data - United States'. The interface is divided into several sections:

- Metrics:** A red box displays a 'Threat Score' of 95. To the right, there are four summary cards: 'Assets' (1), 'Judgements' (1), 'Verdicts' (1), and 'Indicators' (0).
- Metadata:** This section provides detailed information about the sample, including its ID, filename, magic type, file type, first/last seen timestamps, SHA-256/SHA-1 hashes, MD5, and tags. It also includes a 'Virtual Machine' section with details about the OS (Windows 10), start/end times, duration, and the type of activity (Random Cursor Movement with Image Recognition).
- Behavioral Indicators:** This section shows a table of indicators. The table has columns for 'Title', 'Categories', 'ATT&CK', 'Tags', 'Hits', and 'Indicator Score'. Two indicators are listed: 'A Suspicious Document Containing Randomized Variable Names Detected' (1 hit, score 95) and 'Artifact Flagged Malicious by Antivirus Service' (2 hits, score 95).

Endpoint Submission

Secure Endpoint > Cloud Analytics

The screenshot shows the 'File Repository' section of the Secure Endpoint Premier interface. It includes a search bar, filters for file type and group, and a table of files. A file named 'pad_config.exe' is selected, and a context menu is open, showing options like 'Copy', 'Search', 'File Analysis', and 'Investigate in Cisco Threat Response'.

Secure Endpoint Premier

Dashboard Analysis Outbreak Control Management Accounts

File Repository

Search by SHA-256 or file name

Type All Group All Groups

Clear Filters Apply Filters

All Available Requested Being Processed Failed Rejected

File	Status	Requested By	Date	Actions
notification_helper.exe	Available	Timothy Snow	2022-12-03 14:56:18 +07	
pad_config.exe	Available	Timothy Snow	2022-12-03 14:56:09 +07	

Original File Name: pad_config.exe
Fingerprint (SHA-256): ed684b0e...235458ad

Disposition: Malicious
Filename: pad_config.exe

Copy
Search
VirusTotal: (36/71)
Riskware: Hides Windows
Full Report
File Fetch
File Analysis
File Trajectory
Outbreak Control
Investigate in Cisco Threat Response

The screenshot shows the 'File Analysis' section of the Secure Endpoint Premier interface. It displays a list of files with their SHA-256 hashes, types, and VMs. A file named 'pad_config.exe' is selected, and its details are shown, including behavioral indicators and a list of actions.

Secure Endpoint Premier

Dashboard Analysis Outbreak Control Management Accounts

File Analysis

Submit Sample Dashboard Samples Search Reports Indicators

Samples

Local Data - United States

Filter

SHA-256

Search

Scope

- All
- My Organization
- My Samples

Date Range

- Last 24 Hours
- Last 7 Days
- Last 30 Days
- Last 90 Days
- Custom Range

Filename	SHA-256	Type	Tags	VM	Access	Status	Actions
notification_helper.exe	1dc5cc50...			Windows 7 64-bit			
pad_config.exe	ed684b0...			Windows 7 64-bit			

Details

Sample ID: 14408915ce423b0b4cb3684863a32ca6

SHA-256: ed684b0e03a34f13a086c49d9d5191c7460a80...

SHA-1: 95acc1fe601496c0039f27c28c3e63007d7c8af7

MD5: 31649d901f32412f20f81eb2c3332d

Tags

Sightings

First: 12/3/2022 2:56 PM
Last: 12/3/2022 2:56 PM
Times: 1

Network

Streams: 6

Registry

Actions: 6

Artifacts

Disk: 7
Memory: 3

Environment

VM: Windows 7 64-bit
Runtime: 5 minutes

Behavioral Indicators

Artifact Flagged as Known Trojan by Antivirus: 95

Artifact Flagged Malicious by Antivirus Service: 95

Artifact Flagged by Antivirus: 72

Process Modified an Executable File: 60

Process Modified File in a User Directory: 56

Static Analysis Flagged Artifact As Anomalous: 48

Command Exe File Execution Detected: 40

Process Modified INI File: 35

Memory Block Allocation with Read/Write/Execute Permissions: 25

Sample Created A Batch File: 25

Sample Used A Temporary Batch File: 25

PE Contains TLS Callback Entries: 24

PE Has Sections Marked Executable and Writable: 24

Process Read INI File: 15

Executable Packed with UPX: 9

Executable with Encrypted Sections: 9

Executable Imported the IsDebuggerPresent Symbol: 4

PE COFF Header Timestamp is Set to Date Prior to 1999: 3

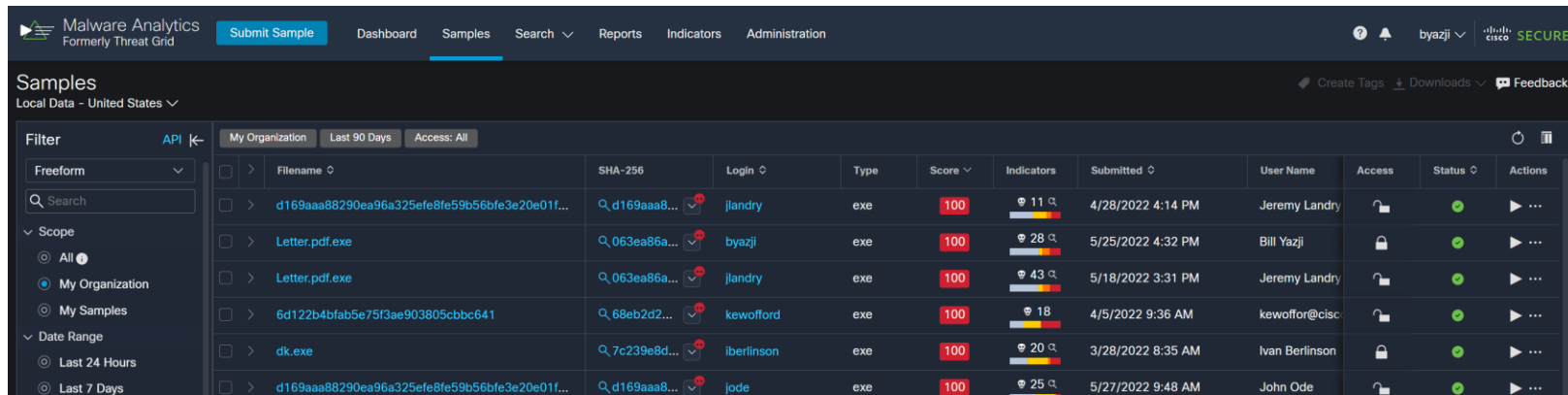
DNS Traffic

cisco Live!

You control the privacy...

'Public' and 'Private' Access

- Sample tagging controls privacy
 - Private – Full sample detail is only visible to the submitting Organization
 - Public – Sample will be visible globally (all users can access all the details of the report)



The screenshot displays the Cisco Malware Analytics interface. The top navigation bar includes 'Submit Sample', 'Dashboard', 'Samples', 'Search', 'Reports', 'Indicators', and 'Administration'. The 'Samples' section is active, showing a table of samples. The table has columns for Filename, SHA-256, Login, Type, Score, Indicators, Submitted, User Name, Access, Status, and Actions. The samples listed are:

Filename	SHA-256	Login	Type	Score	Indicators	Submitted	User Name	Access	Status	Actions
d169aaa88290ea96a325efe8fe59b56bfe3e20e01f...	Q_d169aaa8...	jlandry	exe	100	11	4/28/2022 4:14 PM	Jeremy Landry	🔒	🟢	▶ ...
Letter.pdf.exe	Q_063ea86a...	byazji	exe	100	28	5/25/2022 4:32 PM	Bill Yazji	🔒	🟢	▶ ...
Letter.pdf.exe	Q_063ea86a...	jlandry	exe	100	43	5/18/2022 3:31 PM	Jeremy Landry	🔒	🟢	▶ ...
6d122b4bfab5e75f3ae903805cbbc641	Q_68eb2d2...	kewofford	exe	100	18	4/5/2022 9:36 AM	kewoffor@cisc	🔒	🟢	▶ ...
dk.exe	Q_7c239e8d...	iberlinson	exe	100	20	3/28/2022 8:35 AM	Ivan Berlinson	🔒	🟢	▶ ...
d169aaa88290ea96a325efe8fe59b56bfe3e20e01f...	Q_d169aaa8...	jode	exe	100	25	5/27/2022 9:48 AM	John Ode	🔒	🟢	▶ ...

Orbital and MITRE ATT&CK Integrations

Samples
Local Data - United States ▾

Filter API ←

Freeform ▾
Search

Scope

- All 1
- My Organization
- My Samples

Date Range

- Last 24 Hours
- Last 7 Days
- Last 30 Days
- Last 90 Days
- Custom Range

Threat Score

- Critical
- High
- Medium
- Low

Integration

- CMD
- CSA
- ESA
- Fireamp
- FMC
- FMC Sensor
- ISR

Scope: All **Last 90 Days** **Access: All**

Filename	SHA-256	Login	Type	Score	Indicators		Status	Actions
80057b2586179d8328a7c4b1d87f5e8b735f2cbce...	Q.80057b2...	✓	exe	100	28	5/4/2022 6:15 AM	🔒	🟢 ▶
c45caf9fc817277f573dec9da10c6eab	Q.4abe13b...	✓	exe	100	38	4/24/2022 10:15 AM	🔒	🟢 ▶
67f3567f0776be96f9d7a8868204e95069d6abcf...	Q.67f3567f...	✓	exe	100	15	4/22/2022 3:17 PM	🔒	🟢 ▶
a5ef80c3eb402e8e2aa8ac4bdb2d48b0523053bf...	Q.a5ef80c3...	✓	exe	100	22	4/28/2022 7:04 AM	🔒	🟢 ▶
9aadee4b56e6fab0e7ff3c9dea015eb14527d4c89...	Q.9aadee4b...	✓	exe	100	16	4/25/2022 8:25 AM	🔒	🟢 ▶
220b1c087dddaca54781b785874e4db24df87b43...	Q.220b1c0...	✓	exe	100	21	3/14/2022 1:34 AM	🔒	🟢 ▶
7e038a9a8a39c1834f14ce61002c0ce4671ae0004...	Q.7e038a9a...	✓	exe	100	17	3/12/2022 12:18 AM	🔒	🟢 ▶
778395fc43d29915ec301d65f0652a5e5b7384113...	Q.778395fc...	✓	exe	100	20	4/17/2022 3:01 AM	🔒	🟢 ▶
422733273eedc69ba2a98b0836345d32984ba5b8...	Q.4227332...	✓	exe	100	16	4/16/2022 7:50 AM	🔒	🟢 ▶
8b4edb435225e5126db577bd394d77bfe42db1ea...	Q.8b4edb4...	✓	exe	100	11	4/15/2022 3:26 AM	🔒	🟢 ▶
8ecfb9684759b2bae43b20674e05c5d6f82acba9...	Q.8ecfb968...	✓	exe	100	6	4/16/2022 8:54 PM	🔒	🟢 ▶
192e52f0373721ca3dd66eac844ab42732332036...	Q.192e52f0...	✓	exe	100	31	4/18/2022 4:36 AM	🔒	🟢 ▶
23d2a81e1694f474769355aeb0abb8e8ca153cc308...	Q.23d2a81e...	✓	exe	100	22	3/15/2022 5:59 PM	🔒	🟢 ▶
9901aca51fd71f6b4552922a4d7da1f8	Q.c385e18e...	✓	exe	100	40	3/7/2022 8:33 AM	🔒	🟢 ▶
1f2efce3fcd7ef8760a338f81a6a56f8da1178d265...	Q.1f2efce3f...	✓	exe	100	19	4/22/2022 6:08 PM	🔒	🟢 ▶
6f7b5143a9582d36791f8fc12ec13b150ac80ff132...	Q.6f7b5143...	✓	exe	100	14	5/22/2022 2:54 PM	🔒	🟢 ▶
8bd7127ef3fb2a12127ea60018b0ca61e805ec410...	Q.8bd7127...	✓	exe	100	21	5/26/2022 8:57 PM	🔒	🟢 ▶

Indicators

- 5 90-100 **Orbital Queries**
- 1 75-89
- 6 50-74
- 9 0-49

Orbital

Orbital and MITRE ATT&CK Integrations

Report / Samples / c45caf9fc817277f573dec9da10c6eab
Local Data - United States

Report FP/FN ↑ Results

Metrics
Metadata
Indicators
Network
DNS Traffic
TCP/IP Streams
Extracted Domains
Processes
Artifacts
Registry Activity
Consolidated
Created Keys
Modified Keys
File Activity

Behavioral Indicators

☐ Only show Indicators with Orbital queries

Search

Title	Orbital Queries	Categories	ATT&CK	Tags	Score
Mabezat File Path Detected	Orbital Queries	Worm	Initial Access Lateral Movement	mabezat usb worm	100
USB Autorun Enabled through the Creation of autorun.inf		Spreading	Initial Access Lateral Movement	autorun file process	100
Artifact Flagged as Known Trojan by Antivirus		Anti-Virus		RAT trojan	95
Artifact Flagged Malicious by Antivirus Service		Anti-Virus		antivirus file	95
Executable File Created On the USB Drive		Spreading	Initial Access Lateral Movement	executable file PE process spreading usb	90
Process Created a File in a Recycle Bin Folder	Orbital Queries	Evasion	Defense Evasion	file process recycler	90
Process Created an Executable in a Recycle Bin Folder		Evasion	Defense Evasion	executable file process recycler	90
Process Modified the Windows System Startup File		Persistence	Persistence Privilege Escalation	file process system modification	90
Process Modified a File in a System Directory		Dynamic Anomaly		executable file process	85
A PE Artifact has an Invalid Certificate Signature		Static Anomaly	Defense Evasion	attributes certificate PE	80
An Executable Found in Recycle Bin Folder		Pattern	Defense Evasion	executable file process recycler	80

Orbital and MITRE ATT&CK Integrations

Report / Samples / c45caf9fc817277f573dec9da10c6eab
Local Data - United States

Report FP/FN Resubmit Downloads Feedback

Metrics
Metadata
Indicators
Network
DNS Traffic
TCP/IP Streams
Extracted Domains
Processes
Artifacts
Registry Activity
Consolidated
Created Keys
Modified Keys
File Activity

Behavioral Indicators

☐ Only show Indicators with Orbital queries

Search

Title	Orbital Queries	Categories	ATT&CK	Tags	Score
Mabezat File Path Detected	Orbital Queries	Worm	Initial Access Lateral Movement	mabezat usb worm	100

Mabezat File Path Detected

Score: 100 Hits: 1

Description

A file path associated with Mabezat has been detected. Mabezat is a worm that infects Windows executable files and can be spread through email attachments, network shared drives, USB drives and CD burning. In addition to capabilities typical of worms, it can download and execute additional payloads from a command and control server.

Trigger

This indicator is triggered when a file path associated with mabezat has been detected.

Process	Process Name	Path	Actions
Process 17	tazebama_dl_	\\zPharaoh.exe	Orbital Query

USB Autorun Enabled through the Creation of autorun.inf

Spreading Initial Access

autorun file process 100

MITRE ATT&CK attack.mitre.org

Tactic: Initial Access

Technique: Replication Through Removable Media

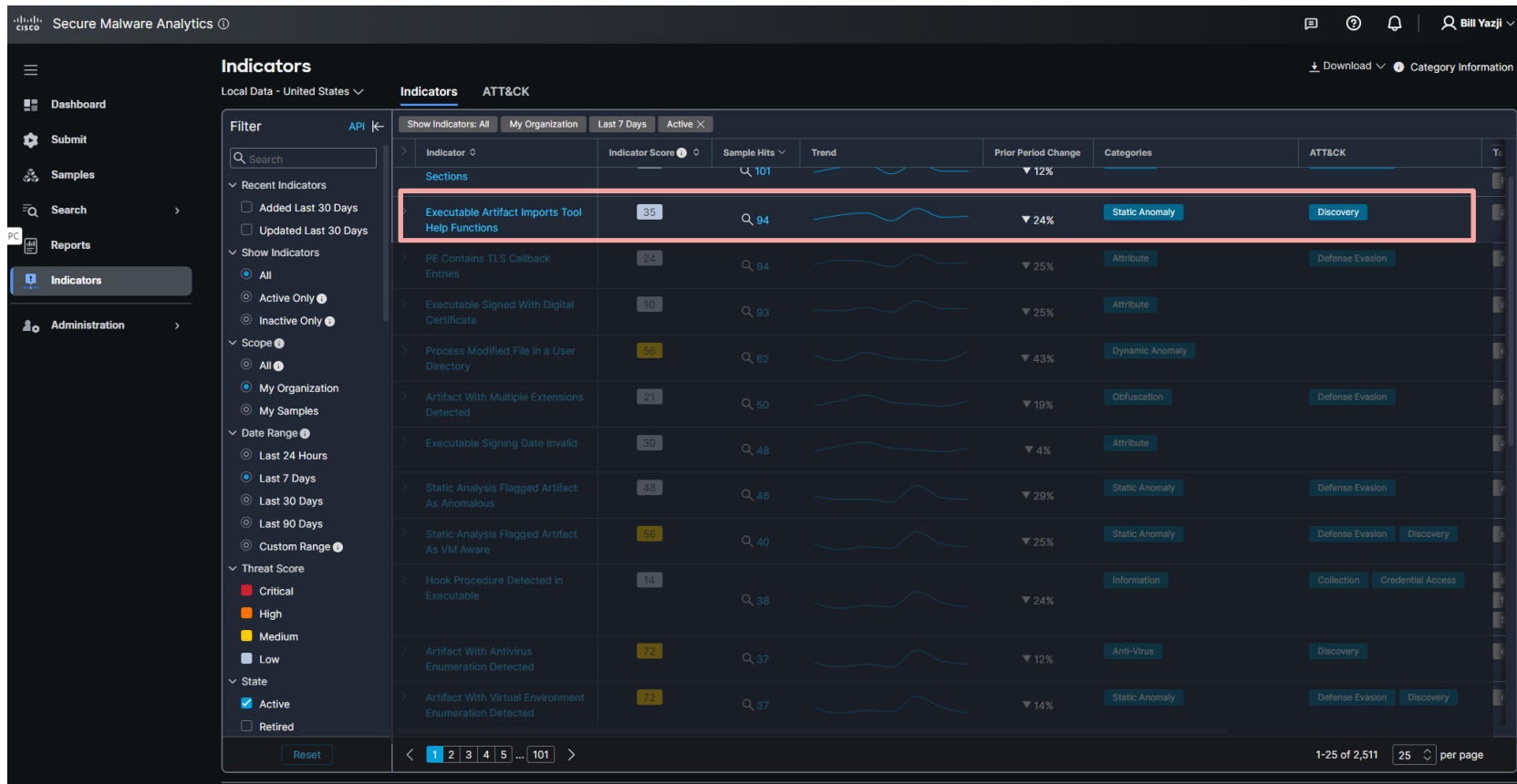
Read Descriptions

Tactic: Lateral Movement

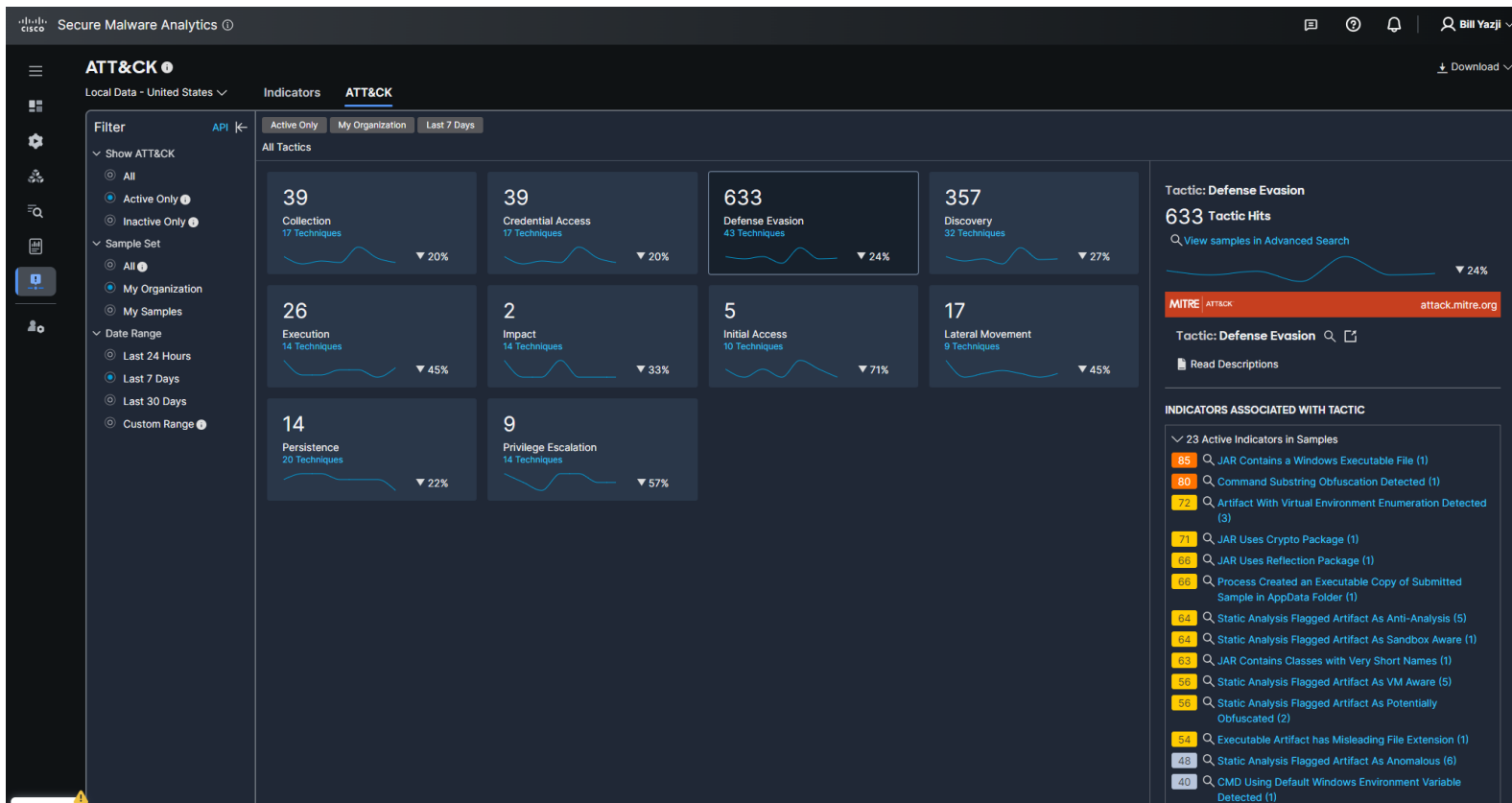
Technique: Replication Through Removable Media

Read Descriptions

Trend View



ATT&CK View



Offering Comparison

Tier offerings based on purchase

	Malware Defense-Enabled Secure Malware Analytics	Secure Malware Analytics Entitlement Portal	Secure Malware Analytics Cloud Portal
Automatic submissions from Cisco devices/services	✓ *	✓ *	✓ *
Access to “Device/Entitlements” portal views		✓	✓
Manual file & 3 rd party API submissions			✓ *
Search and pivot on Global Data			✓
Cisco XDR Integration			✓
Ability to interact with running sample (Glovebox)			✓
View Network\Process\Artifact\File\Disk\Registry Activity			✓
Easily delete submissions via GUI			✓
Orbital & MITRE Enhancements and Pivot			✓

* Requires Advanced File Analysis Submission package

Integrations feeding Secure Malware Analytics

Secure Email / Web / Firewall

- File Analysis (FA) Client ID identifies individual device

Umbrella / Secure Endpoint / Meraki / Cloud Mailbox Defense / Email Threat Defense

- Business/Service name identifies a service to Secure Malware Analytics

FA Client ID and Service Name are used to bind submissions to a Secure Malware Analytics Org

- Provides access to view in Cloud Portal if purchased
- Provides the ability to see samples submitted by Malware Defense-Enabled devices

Appliance Note: These are also used to register devices on a Secure Malware Analytics Appliance

- Device registers a new User at Appliance with Client ID as the Username
- This new User must be activated, otherwise Appliance will not accept submissions

Integrated Connector Registration

Malware Defense-Enabled Integration Registration to Secure Malware Analytics

Tech Note on obtaining File Analysis Client ID

- <https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/213667-file-analysis-client-id-on-content-secr.html>

Best to work with your Cisco Security account teams

- Gather FA-IDs and Service Names
- Group in Secure Malware Analytics Cloud organization (subscription) or Secure Malware Analytics Entitlement Portal organization (complimentary)
- tg-provisioning@cisco.com can also provide grouping assistance

Integrated Connector Registration

Secure Malware Analytics

Organizational view into Malware Defense-Enabled devices and cloud users

Users - CSE-Demo
Local Data - United States

Download ▾ + New User Feedback

Filter

Active X

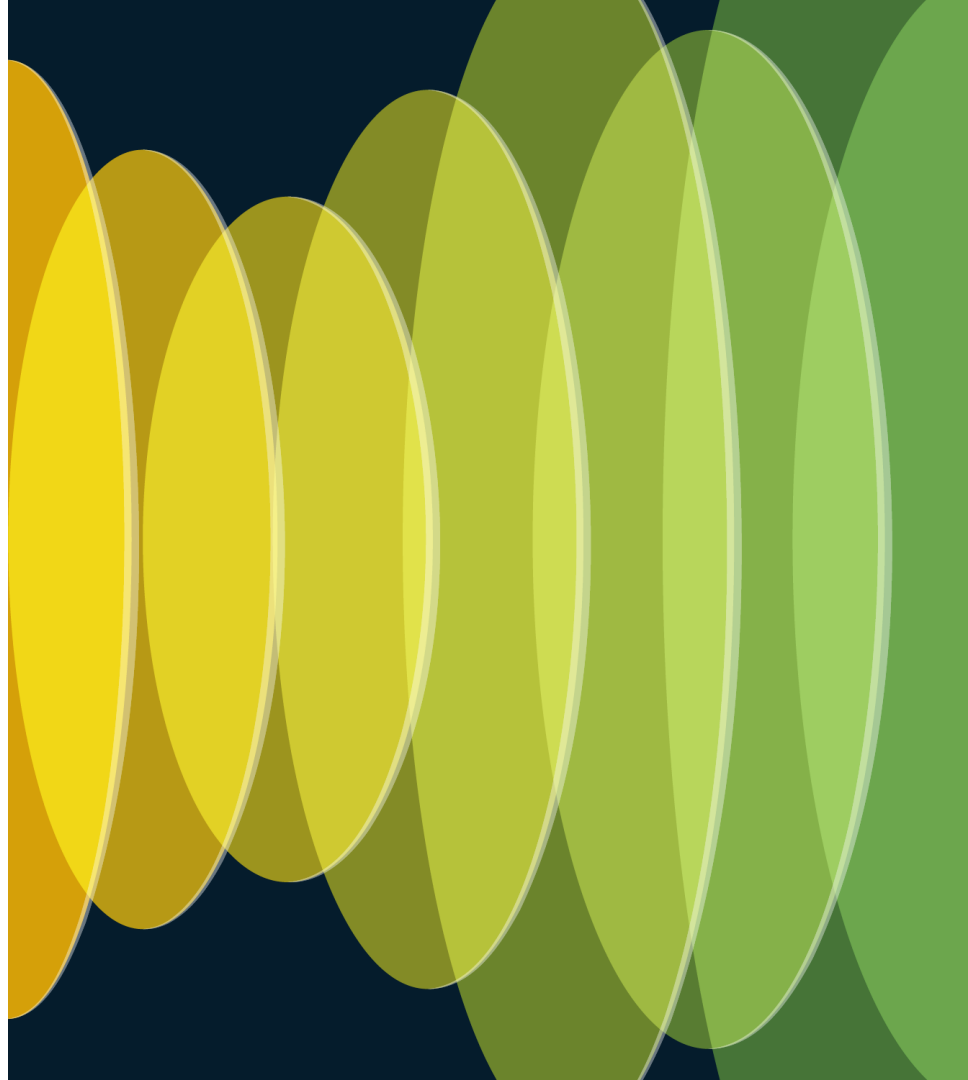
Search	Login	User Name	Email	Title	Role	Status	Device Groups	Integration	Type	Actions
<input checked="" type="checkbox"/> Active	meraki.csedemo.1	meraki.csedemo.1	byazji@cisco.com		User	Active		Meraki	device	...
<input type="checkbox"/> Inactive	sig.csedemo.1	sig.csedemo.1	byazji@cisco.com		User	Active	N/A	SIG	service	...
<input type="checkbox"/> Device	cse-device-admin1	cse-device-admin1	byazji@cisco.com		Device Admin	Active	N/A	Unspecified	person	...
<input type="checkbox"/> Person	cse-org-admin1	cse-org-admin1	byazji@cisco.com		Org Admin	Active	N/A	Unspecified	person	...
<input type="checkbox"/> Service	cse-byazji-admin	Bill Yazji	byazji@cisco.com	CSE-Demo admin	Org Admin	Active	N/A	Unspecified	person	...
<input type="checkbox"/> Device Admin	cse-user1	cse-user1	byazji@cisco.com		User	Active	N/A	Unspecified	person	...
<input type="checkbox"/> Org Admin	cmd.csedemo.1	cmd.csedemo.1	byazji@cisco.com		User	Active		CMD	device	...
<input type="checkbox"/> User	wsa-device-d57463bd...	WSA Device			User	Active		WSA	device	...
<input type="checkbox"/> Limited User	fmc-sensor-df2ed4db...	FMC Sensor			User	Active		FMC Sensor	device	...
<input type="checkbox"/> Integration	fmc-sensor-7f6b511b...	FMC Sensor			User	Active		FMC Sensor	device	...
<input type="checkbox"/> CMD	esa-device-8d70437e...	ESA Device			User	Active		ESA	device	...
<input type="checkbox"/> CSA										
<input type="checkbox"/> ESA										

Integrated Connector Registration

Things to keep in mind

- Firewall rules ~~can~~ will interfere with your device registering
- If a device is exchanged (hardware refresh/RMA, etc) – you will need to add that back to Secure Malware Analytics and your organization manually
- Firepower Threat Defense appliances have the FMC MAC address in its ID. If you change FMC – you will need to ensure all in same org.
- Register primary and failover FMC to Secure Malware Analytics Portal
- Consider Secure Malware Analytics Entitlement Portal for device visibility vs. Group Reporting feature of WSA/ESA/CES
- Consider Secure Malware Analytics Cloud upgrade for full visibility

Secure Malware Analytics APIs & Integrations



Secure Malware Analytics APIs

Data API

- Entity search */search/*
 - search observables by **specific criteria**
- Entity lookups */domains/*, */urls/*, */paths/*, etc
 - pivot from a known observable to other related information in Threat Grid data
- Sample mgmt: */samples/*
 - submit
 - retrieve data/analysis
 - raw observables feeds */samples/feeds/*
 - Get lists of observables associated with a filterable set of samples
 - Harvested from all sample activity, suspicious or not, therefore very high FP
 - Can filter to your user's or your org's samples only; eg "get all domains associated with samples my company submitted"
 - Results in JSON

CISCO *Live!*

CISCO *Live!*

Secure Malware Analytics – Curated Feeds

Curated feeds API */feeds/*

- Based on specific, high confidence human-curated BIs
- Whitelisted via TG and Talos intelligence
- Much lower FP
- Groups observables by IOC type (eg “DGA DNS domains”)
- Not filterable by sample ownership –
 - But you could combine with IOC feeds to do so!
- Least complex request structure
- Made for integrations – available output formats:
 - JSON / CSV / Short / STIX

Secure Malware Analytics APIs

Feed details summary:

	Sample Feeds	IOC feeds	Curated Feeds
Version	/v2	/v2	/v3
Endpoint	/samples/feeds/	/iocs/feeds/	/feeds/
Content	All observables seen	Observables seen – by BIs	Observables seen as part of a trusted high confidence BI trigger
FP rate*	High	Medium	Low
Pre-whitelisted	No	No	Yes
Filterable to only you/org?	Yes	Yes	No
Output Formats	JSON	JSON	JSON/CSV/Short/STIX**
Request Complexity	Low	Low	Lowest

* The factual FP rate is 0; these were all seen. The functional FP rate, as an indicator of local compromise, is dependent on the details of the observation and varies from feed to feed.

** additional formats not available for all curated feeds

Retrieving Data

Curated Feeds

- Based on human-vetted BIs (or collections of related BIs).
- Refreshed frequently
- Whitelisted: known good or known benign observables are scrubbed before publishing.
- Useful or benign domains could still be in the feed. While many customers do use these for automated blocking, be aware that this is a risk.

Feed Name	Short Description
autorun-registry	Contains registry entry data derived from querying registry changes known for persistence
banking-dns	Banking Trojan Network Communications
dga-dns	DGA Domains with pseudo-randomly generated names
dll-hijacking-dns	Feed contains Domains communicated to by samples leveraging DLL Sideloads and/or hijacking techniques
doc-net-com-dns	Document (PDF, Office) Network Communications
downloaded-pe-dns	Samples Downloading Executables Network Communications
dynamic-dns	Samples Leveraging Dynamic DNS Providers
irc-dns	Internet Relay Chat (IRC) Network Communications
modified-hosts-dns	Modified Windows Hosts File Network Communications
parked-dns	Parked Domains resolving to RFC1918, Localhost and Broadcast Addresses
public-ip-check-dns	Check For Public IP Address Network Communications
ransomware-dns	Samples Communicating with Ransomware Servers
rat-dns	Remote Access Trojan (RAT) Network Communications
scheduled-tasks	Feed containing scheduled task data observed during sample execution
sinkholed-ip-dns	DNS entries for samples communicating with a known dns sinkhole
stolen-cert-dns	DNS Entries observed from samples signed with a stolen certificate

Retrieving Data

Curated Feeds

Parameters	Description
feedname	The name of the feed.
time range	The date time stamp. Optional. Default = last one hour.
format	The output format.
api_key	The API key of the user or program requesting the data.

Making the request:

[Root, version, and endpoint]/[feed_name]_[date].[format]?[api_key]

Examples:

- DGA DNS as JSON for a specific day:

[https://panacea.threatgrid.com/api/v3/feeds/dga-dns_2022-12-08.json?api_key=\[API_KEY\]](https://panacea.threatgrid.com/api/v3/feeds/dga-dns_2022-12-08.json?api_key=[API_KEY])

- Last hour's Sinkholed IP/DNS as STIX:

[https://panacea.threatgrid.com/api/v3/feeds/sinkholed-ip-dns.stix?api_key=\[API_KEY\]](https://panacea.threatgrid.com/api/v3/feeds/sinkholed-ip-dns.stix?api_key=[API_KEY])

- Dynamic DNS Domains for a date as Short rules, in the browser, after logging in:

https://panacea.threatgrid.com/api/v3/feeds/dynamic-dns_2022-12-08.snort

SIEM/SOAR integrations with ease

Splunkbase

Threat Grid
This app supports executing investigative actions to analyze executables and URLs on the Threat Grid sandbox
Built by Splunk Inc.

Latest Version 2.4.1
November 4, 2022
[Release notes](#)

Compatibility
SOAR Cloud, SOAR On-Prem
Platform version: 5.4, 5.5

Rating
0 ★★★★★ (0)
[Log in to rate this app](#)

Support
Splunk Supported Connector
[Learn more](#)

Ranking
#5 in Sandbox

Summary Details Installation Troubleshooting Contact Version History

This app supports executing investigative actions to analyze executables and URLs on the Threat Grid sandbox

Supported Actions

- test connectivity: Validate the asset configuration for connectivity. This action logs into the device to check the connection and credentials
- detonate file: Run the file in the Threat Grid sandbox and retrieve the analysis results
- get report: Query for results of an already completed task in Threat Grid
- detonate url: Load a URL in the Threat Grid sandbox and retrieve the analysis results
- list playbooks: List the playbooks available in the connected ThreatGrid environment
- list vms: List the VMs available in the connected ThreatGrid environment
- list submissions: List the submissions present on ThreatGrid based on the query provided

Categories
Sandbox

Created by
Splunk Inc.

Source Code
[GitHub](#)

Type
connector

Downloads
15445

Licensing
[Splunk General Terms](#)

Splunk Answers
[Ask a question about this app listing](#)

Resources
[Login to report this app listing](#)

<https://github.com/splunk-soar-connectors/threatgrid>

Supported Actions

test connectivity - Validate the asset configuration for connectivity. This action logs into the device to check the connection and credentials

detonate file - Run the file in the Threat Grid sandbox and retrieve the analysis results

get report - Query for results of an already completed task in Threat Grid

detonate url - Load a URL in the Threat Grid sandbox and retrieve the analysis results

list playbooks - List the playbooks available in the connected ThreatGrid environment

list vms - List the VMs available in the connected ThreatGrid environment

list submissions - List the submissions present on ThreatGrid based on the query provided

action: 'detonate file'

Run the file in the Threat Grid sandbox and retrieve the analysis results

Type: generic

Read only: False

This action requires the input file to be present in the vault and therefore takes the vault id as the input parameter.

Action Parameters

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
vault_id	required	Vault ID of file to detonate	string	vault id pe file pdf shai
file_name	optional	Filename to use	string	file name
vm	optional	VM image to run on	string	threatgrid vm name
force_analysis	optional	Force re-run of sample	boolean	
private	optional	Mark file and results private (This parameter is ignored if the asset setting is checked)	boolean	
playbook	optional	ThreatGrid playbook to run on the submitted file	string	threatgrid playbook name
sample_password	optional	Password used to open the submitted file	string	password
tags	optional	A comma-separated list of tags applied to this sample	string	
vm_runtime	optional	The number of minutes the sample should be analyzed for (Must be set to either 2 or 5)	numeric	

Hands-on: Cisco Secure Malware Analytics (Threat Grid) APIs

In this section, you use the Cisco Secure Malware Analytics (Threat Grid) API to gain intelligence about the. This Lab helps you understand the basics of using Threat Grid APIs with Postman.

Objectives

When you have completed this Learning Lab, you will be able to:

- Harvest data from the Cisco Secure Malware Analytics (Threat Grid) API.
- Use the data from Cisco Secure Malware Analytics to hunt for specific information.

Documentation

In-product API documentation can be accessed with the link: <https://panacea.threatgrid.com/mask/doc/mask/api-getting-started>

Execute the function

Add the following code to the bottom of the script (after `if __name__ == "__main__":`). Review the code well:

```
print(f"vstest 4")

# Call function to find all samples, associated with malicious sha256
submission_info = threatgrid_search_submissions(threatgrid_id)

threatgrid_sample_id = submission_info['item']['sample']

print(f"Successfully retrieved Cisco Secure Malware Analytics sample ID {threatgrid_id}")
```

Execute the file in the terminal. Inspect the output thoroughly.

```
cd threat-hunting
python threat-hunting.py
```

Request sample domains

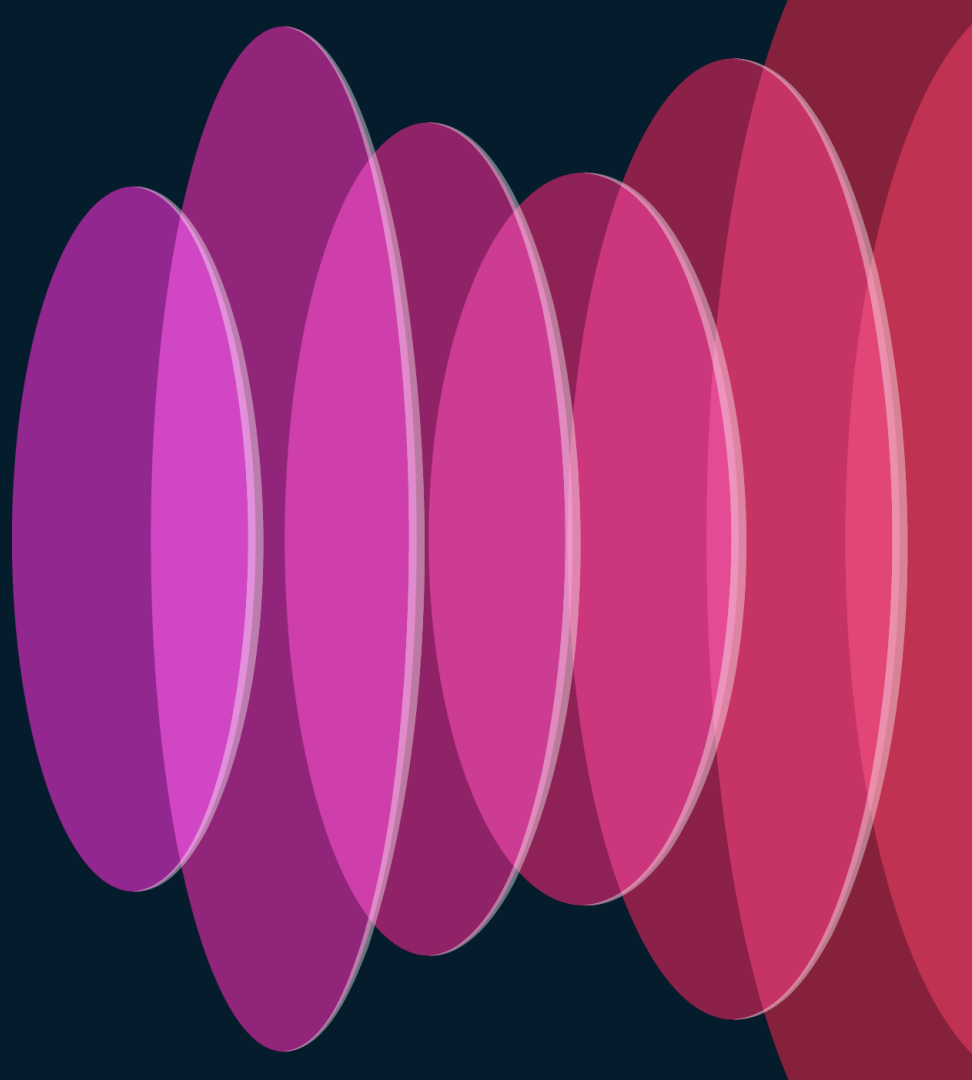
Use the sample ID to fetch the analysis report and retrieve associated domains that have been seen during analysis of this sample. Copy the following to your `threat-hunting.py` file, after the other functions.

```
def threatgrid_get_domains(sample_id,
    hunting_host,
    api_client_id, api_key,
):
    print(f"vstest 4")
    url = f"https://{hunting_host}/api/v2/samples/{sample_id}/domains"
    headers = {
        "Content-Type": "application/json",
        "X-Auth-Token": api_key,
    }
    response = requests.get(url, headers=headers)
```

Setup Steps:

- Step 1: Installing Python 3.10.12
- Step 2: Performing post installation in Cisco Secure Endpoint
- Step 3: Getting SHA256 from Cisco Secure Endpoint
- Step 4: Searching the ThreatGrid Submissions for sha256
- Step 5: Getting domains associated with the ThreatGrid Sample ID

Bringing it
together:
Connecting Cisco
Security to Malware
Defense Cloud



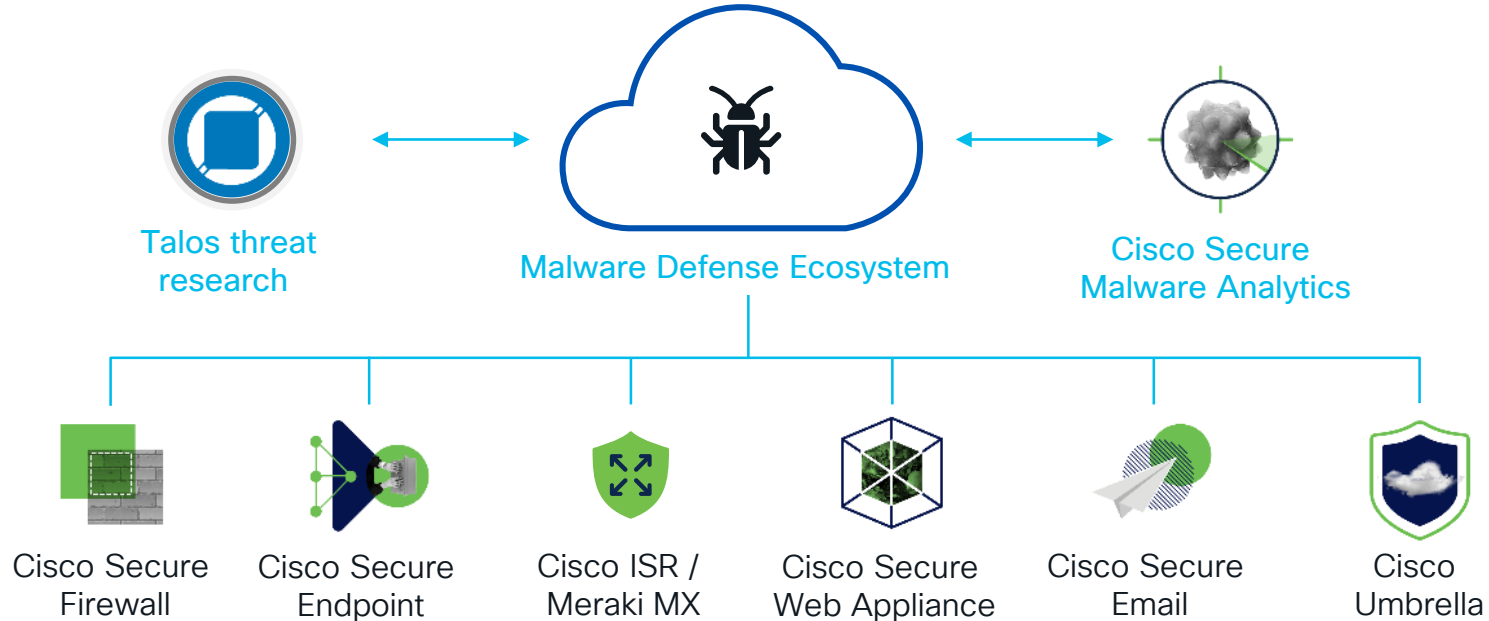
Questions you'll be able to answer after this section:

- I have a few of these products, how do they integrate?
- Wait, I can click once and block everywhere?

Security Architecture:

See once, block everywhere

(And likely to know about it before seeing it)

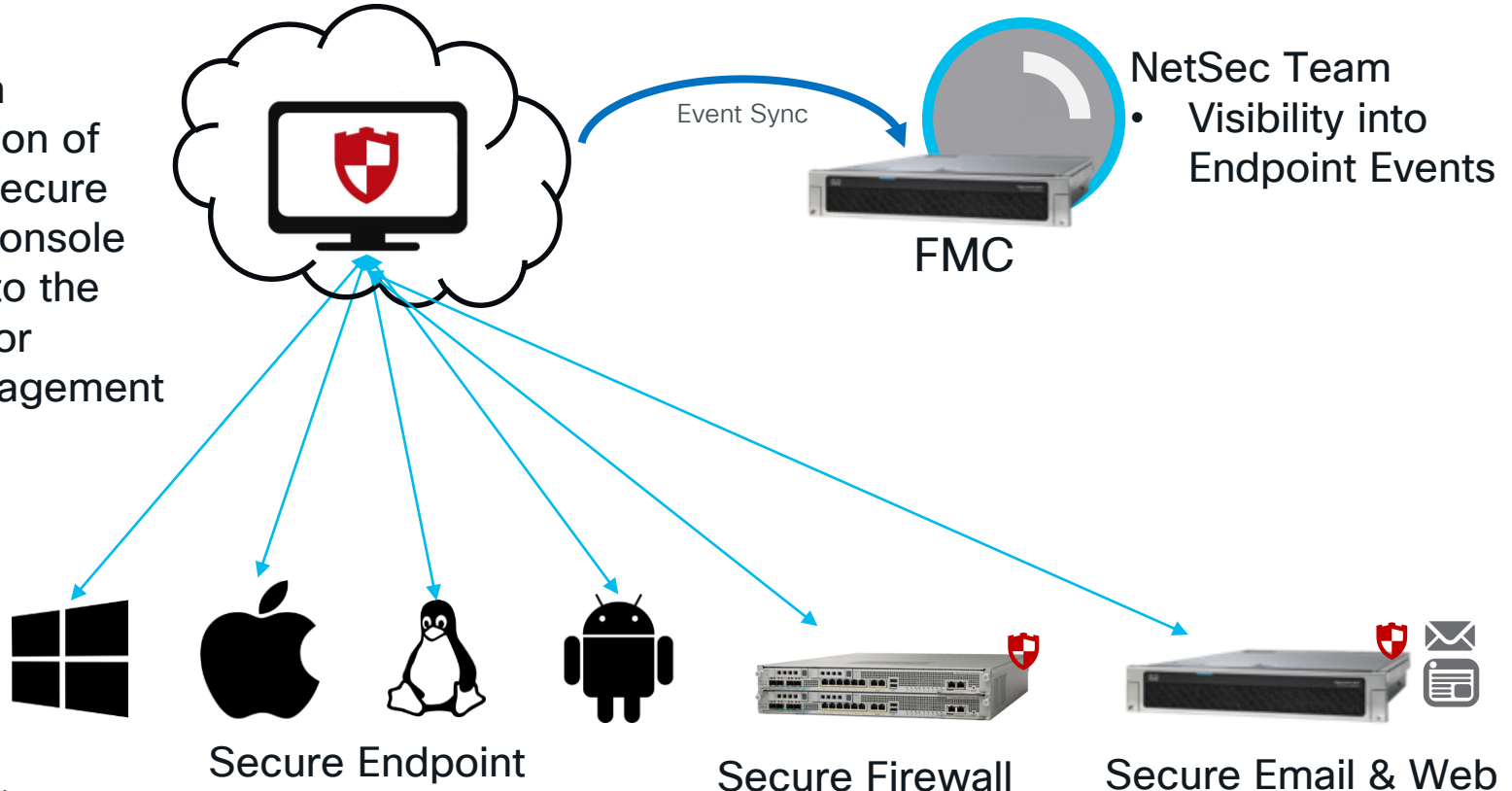


Unity

Enhanced Operational Visibility and Control – Secure Endpoint

Security Team

- Consolidation of events in Secure Endpoint Console
- Visibility into the threat vector
- Policy Management



- ### NetSec Team
- Visibility into Endpoint Events

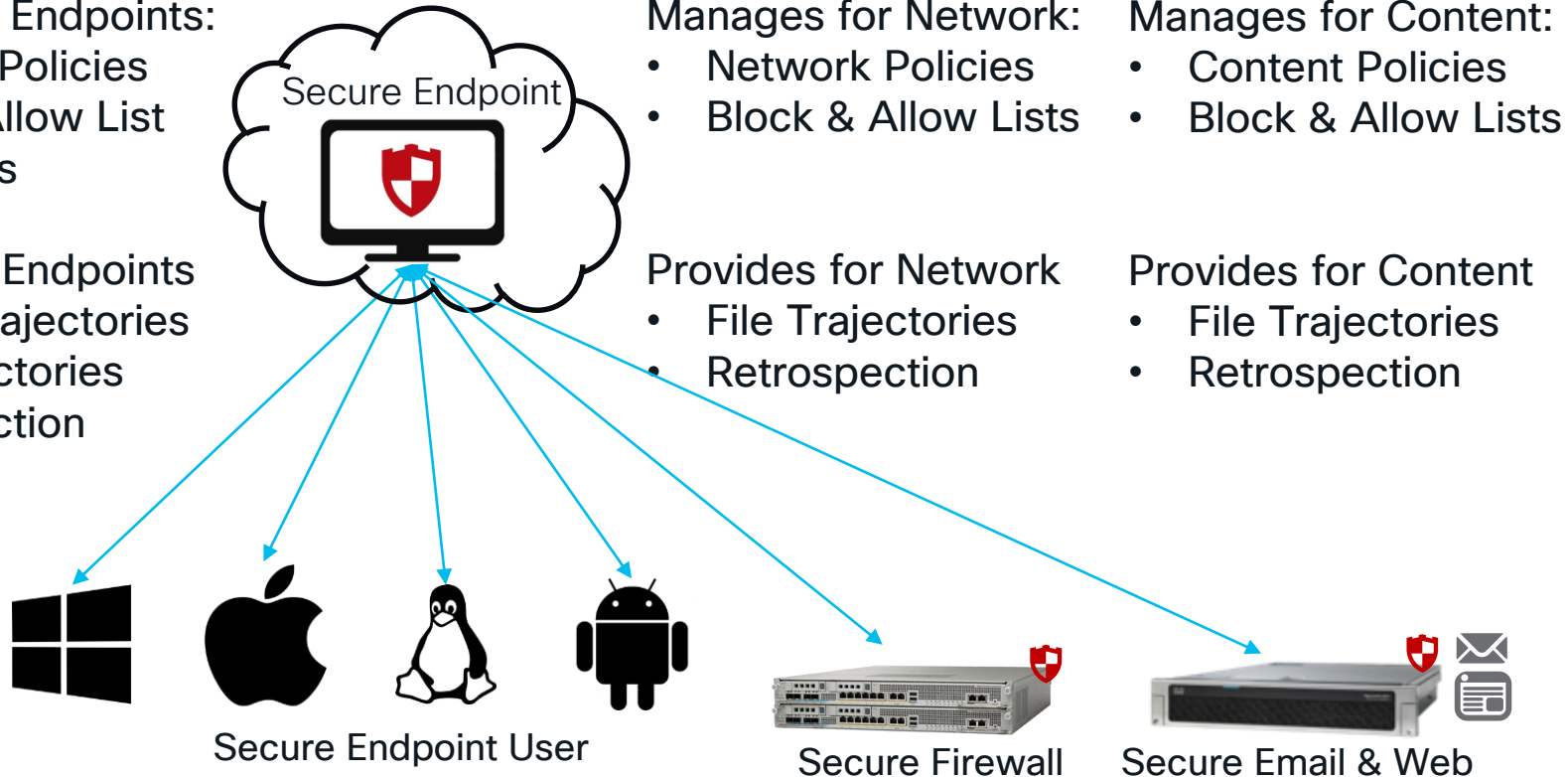
Unity

Manages for Endpoints:

- Endpoint Policies
- Block & Allow List
- Exclusions

Provides for Endpoints

- Device Trajectories
- File Trajectories
- Retrospection



Manages for Network:

- Network Policies
- Block & Allow Lists

Provides for Network

- File Trajectories
- Retrospection

Manages for Content:

- Content Policies
- Block & Allow Lists

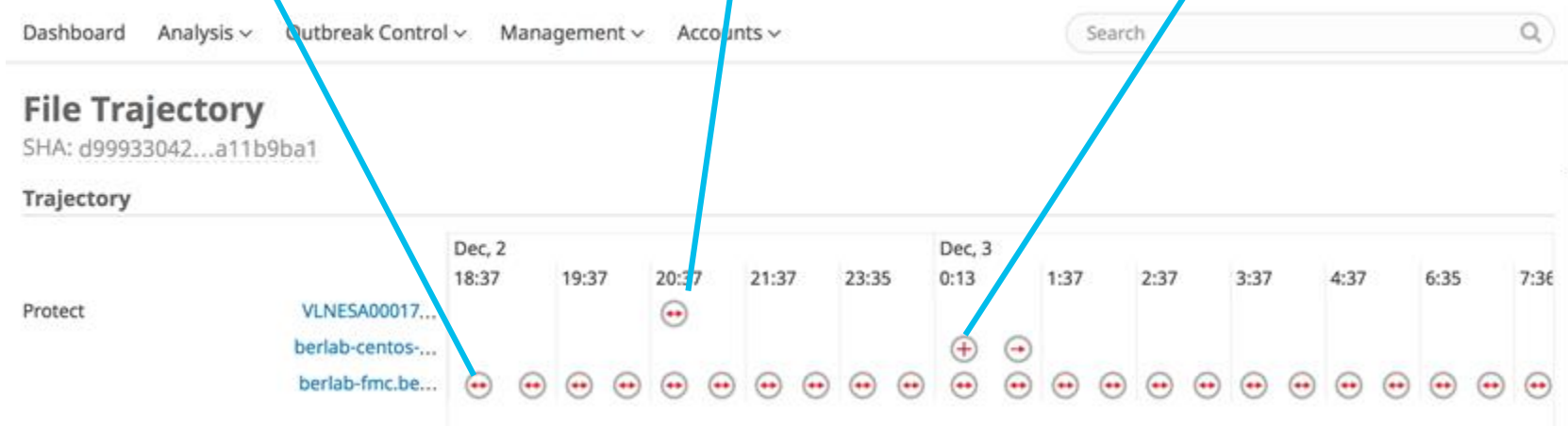
Provides for Content

- File Trajectories
- Retrospection

First, it traversed Secure Firewall

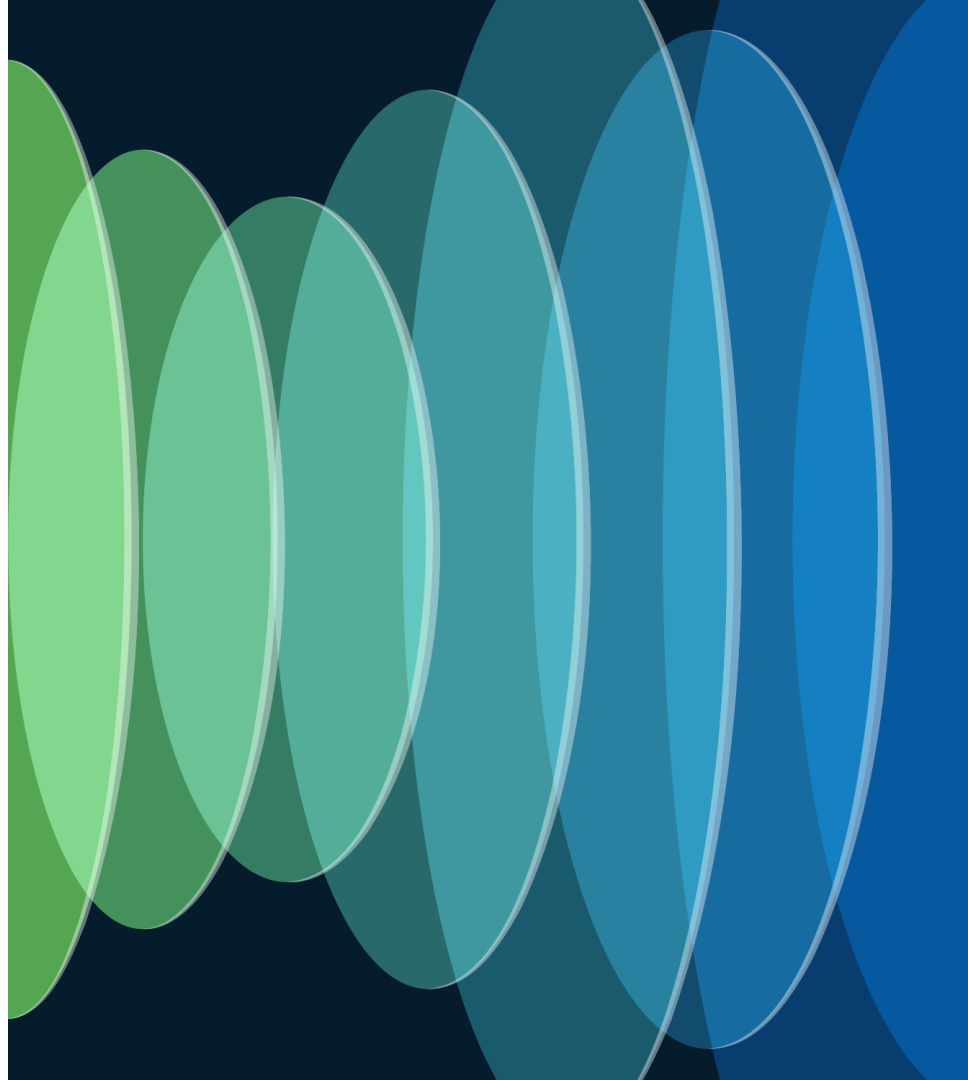
Then observed on Secure Email

And finally stored on the Endpoint

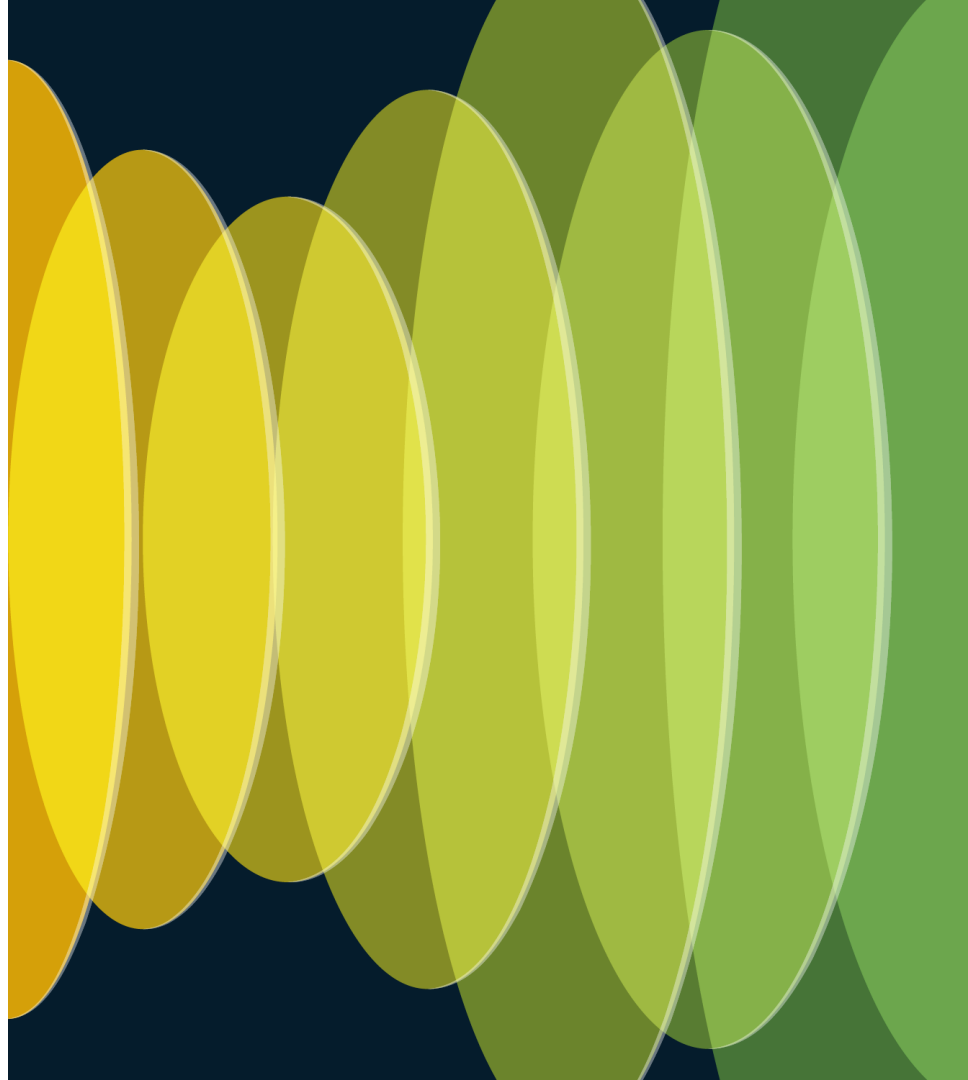


Secure Malware Analytics Demo

(if time...)



Closing



Other good stuff to check out

- Cisco Security APIs and Scripts
 - <https://github.com/CiscoSecurity>
- AMP and Secure Malware Analytics IP and Firewall requirements
 - <https://www.cisco.com/c/en/us/support/docs/security/sourcefire-amp-appliances/118121-technote-sourcefire-00.html>
- Status and outage notifications
 - <https://urgentnotices.statuspage.io/>
- Cisco Live Barcelona 2020 – BRKSEC-2890 [Bill Yazji]
 - Full configuration details for all integrations

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.



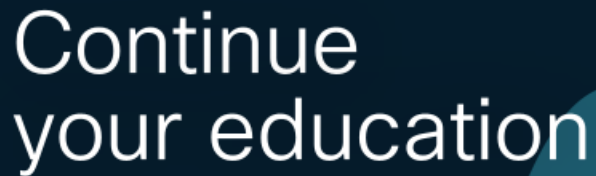
Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.



Level up and earn **exclusive prizes!**



Complete your surveys in the **Cisco Live mobile app**.



Securing User to Application and Everything in Between

Wednesday, June 5 | 1 - 2pm

- Visit us at the Security Innovation Zone (#4435) for demos and workshops



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

Contact me at: byazji@cisco.com



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLive