You make **possible**

Threat Grid & AMP

Integrations with Cisco Email, Web, Network, Cloud and Endpoint Security

Bill Yazji – Technical Security Architect
@billyazji

BRKSEC-2890

Barcelona | January 27-31, 2020

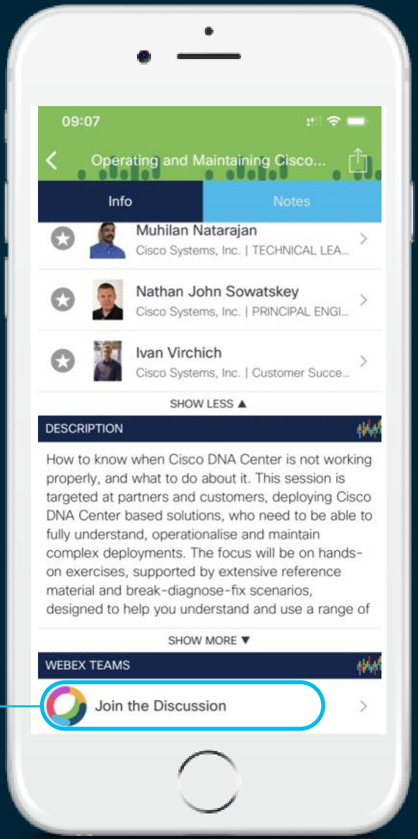
Cisco Webex Teams

Questions?

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

How

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



09:07

Operating and Maintaining Cisco...

Info | Notes

Muhilan Natarajan
Cisco Systems, Inc. | TECHNICAL LEA...

Nathan John Sowatskey
Cisco Systems, Inc. | PRINCIPAL ENGI...

Ivan Virchich
Cisco Systems, Inc. | Customer Succe...

SHOW LESS ▲

DESCRIPTION

How to know when Cisco DNA Center is not working properly, and what to do about it. This session is targeted at partners and customers, deploying Cisco DNA Center based solutions, who need to be able to fully understand, operationalise and maintain complex deployments. The focus will be on hands-on exercises, supported by extensive reference material and break-diagnose-fix scenarios, designed to help you understand and use a range of

SHOW MORE ▼

WEBEX TEAMS

Join the Discussion

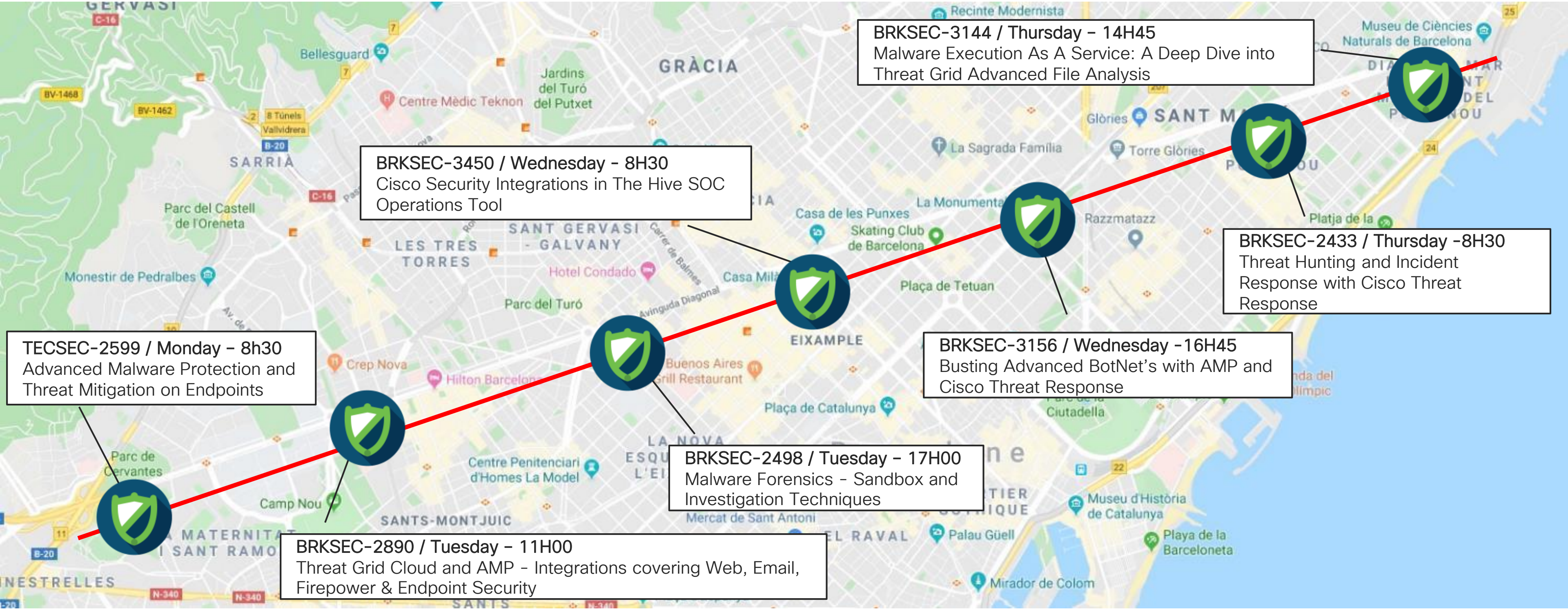
Agenda

- AMP and Threat Grid Architecture basics
- Flows and Deployment Details
  - Email & Web Security (ESA/CES/WSA)
  - Endpoint Security (AMP for Endpoints)
  - Firepower
  - Umbrella SWG & Meraki MX
- Continued Enhancements
  - Threat Grid Organizations, AMP Unity and Threat Response
- Threat Grid Cloud Demo
- Conclusion / Questions

About Your Speaker

- Cisco Live Distinguished Speaker
- Consulting Security Engineer for Enterprise Accounts – Central US
- Nearly 20 years of security and networking experience (10 with Cisco)
- Global Lead for Advanced Threat Technical Advisory Group
- Prior to Cisco…
  - Cisco Competitor in Web Security Space
  - Network and Security Consultant on the customer side
  - Large Design, Deployments, Integrations, and Troubleshooting
- Lives in Kenosha, WI (in between Chicago and Milwaukee – United States)

Advanced Threat Diagonal Learning Map



TECSEC-2599 / Monday – 8h30
Advanced Malware Protection and Threat Mitigation on Endpoints

BRKSEC-2890 / Tuesday – 11H00
Threat Grid Cloud and AMP – Integrations covering Web, Email, Firepower & Endpoint Security

BRKSEC-2498 / Tuesday – 17H00
Malware Forensics – Sandbox and Investigation Techniques

BRKSEC-3450 / Wednesday – 8H30
Cisco Security Integrations in The Hive SOC Operations Tool

BRKSEC-3156 / Wednesday -16H45
Busting Advanced BotNet's with AMP and Cisco Threat Response

BRKSEC-2433 / Thursday -8H30
Threat Hunting and Incident Response with Cisco Threat Response

BRKSEC-3144 / Thursday – 14H45
Malware Execution As A Service: A Deep Dive into Threat Grid Advanced File Analysis

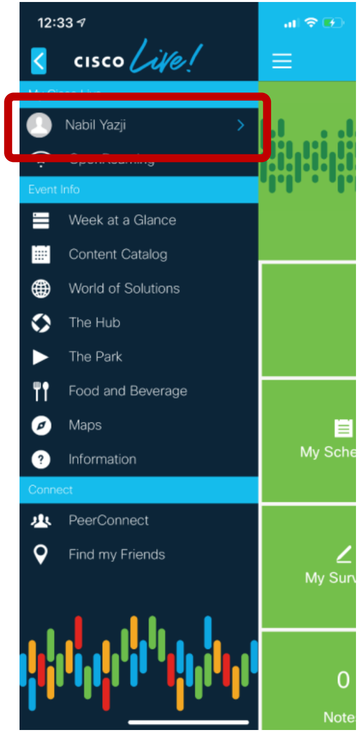
Important: Hidden Slide Alert

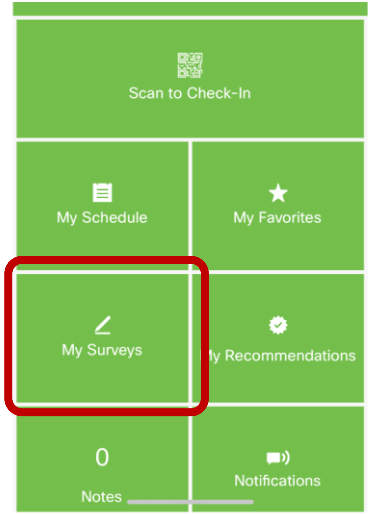
Look for this “For Your Reference” symbol in your PDFs.

There is a tremendous amount of hidden content for you to use later!

For Your Reference

Survey Results Matter...





○ Excellent
○ Above Average
○ Average
○ Below Average
○ Poor

Introduction:
The Basics

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

- What is AMP?
- What is Threat Grid?
- How do they create an ecosystem?
- What is available in the cloud vs. on-premise?
- What CAN go where?
- What things should you not do?

What are the AMP Ecosystem Components?

- **AMP Cloud** – A large data cloud that drives **File Reputation** and **File Retrospection**
  - Public Cloud
  - Private Cloud (Virtual Appliance or Appliance)
- **Threat Grid –** File Analysis and much, much more...
- **AMP-Enabled Integration –** A Cisco device that queries data from AMP Cloud, and submits files to Threat Grid
- **AMP for Endpoints –** A client, on an endpoint ;)

What is Threat Grid?

Unified malware analysis platform

Advanced static and dynamic analysis sandbox

Behavioral indicators

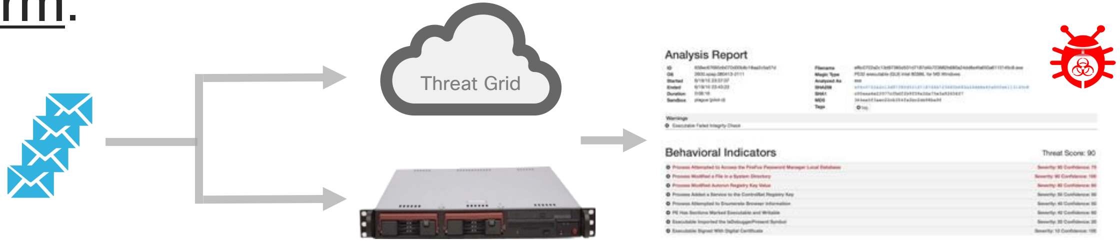
Scalability & Global Correlation

Threat Intelligence

Threat Grid is a unified malware analysis and threat intelligence platform. It performs automated static and dynamic analysis, producing human readable behavioral indicators for each file submitted. Threat Grid's global scalability drives context rich information, that can be consumed directly or via content rich threat intelligence feeds.

Introducing Threat Grid

- Threat Grid is Cisco's <u>unified malware analysis and threat intelligence platform</u>.



Analysis Report

ID	[illegible]	Filename	[illegible]
OS	2600.xpsp.080413-2111	Magic Type	PE32 executable (GUI) Intel 80386, for MS Windows
Started	[illegible]	Analyzed As	exe
Ended	[illegible]	SHA256	[illegible]
Duration	[illegible]	SHA1	[illegible]
Sandbox	[illegible]	MD5	[illegible]
		Tags	

Warnings

- Executable Failed Integrity Check

Behavioral Indicators — Threat Score: 90

Process Attempted to Access the FireFox Password Manager Local Database	Severity: 90 Confidence: 75
Process Modified a File in a System Directory	Severity: 90 Confidence: 100
Process Modified Autorun Registry Key Value	Severity: 80 Confidence: 80
Process Added a Service to the ControlSet Registry Key	Severity: 50 Confidence: 80
Process Attempted to Enumerate Browser Information	Severity: 40 Confidence: 80
PE Has Sections Marked Executable and Writable	Severity: 40 Confidence: 80
Executable Imported the IsDebuggerPresent Symbol	Severity: 20 Confidence: 20
Executable Signed With Digital Certificate	Severity: 10 Confidence: 100

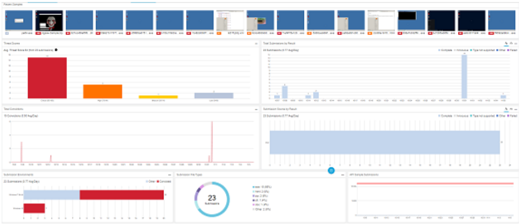
- Flexible Deployments: Cloud SaaS or On-Premise Appliance
- Submissions through Web Portal, AMP-Enabled Device, or API
- API automates sample analysis, enrichment and reporting
- Full Integration with Cisco and 3rd Party SEIM and Threat Solutions

Integration Use Cases

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

Threat Grid API

Malware Analysis & Threat Intelligence

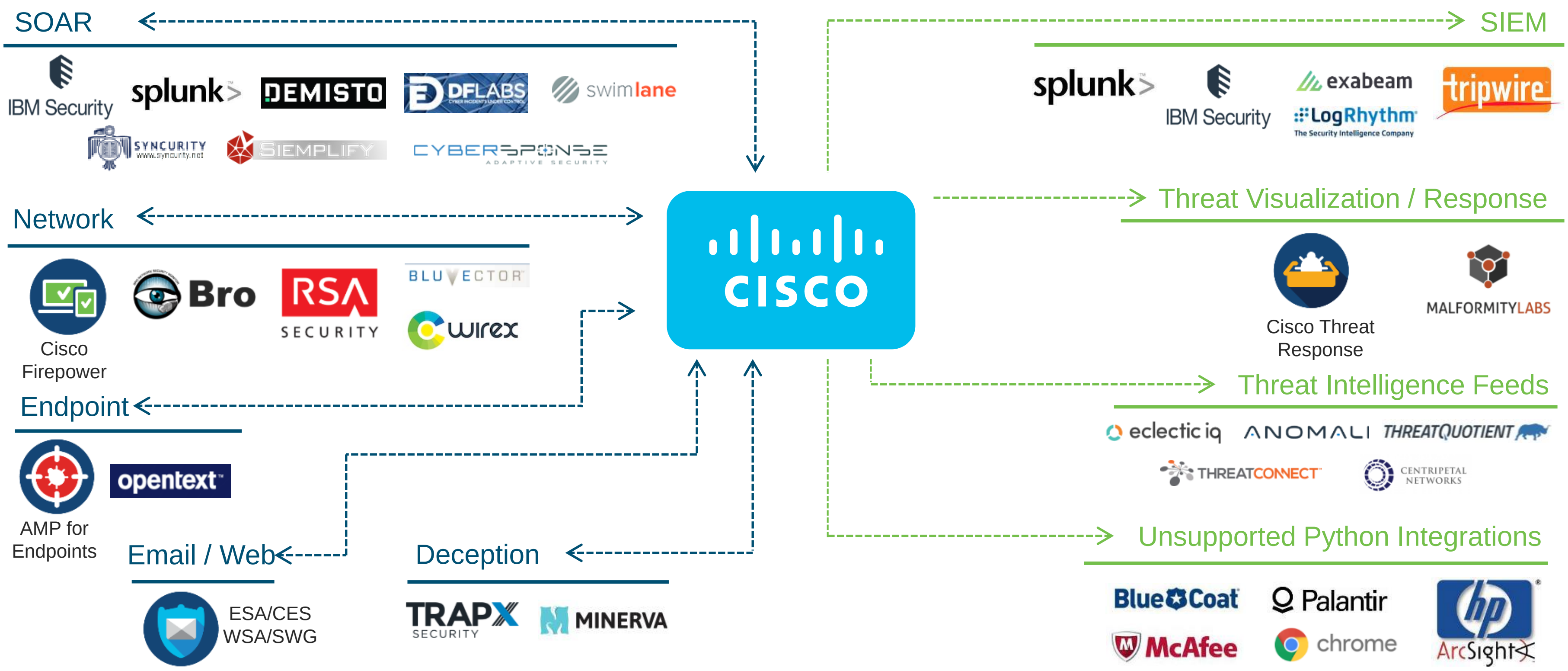


Cisco*live!*

Threat Grid Integrations

Submit Samples and Receive Analysis Results

Visualization of Submitted Samples



SOAR

Network

Cisco Firepower

Endpoint

AMP for Endpoints

Email / Web

ESA/CES
WSA/SWG

Deception

SIEM

Threat Visualization / Response

Cisco Threat Response

Threat Intelligence Feeds

Unsupported Python Integrations

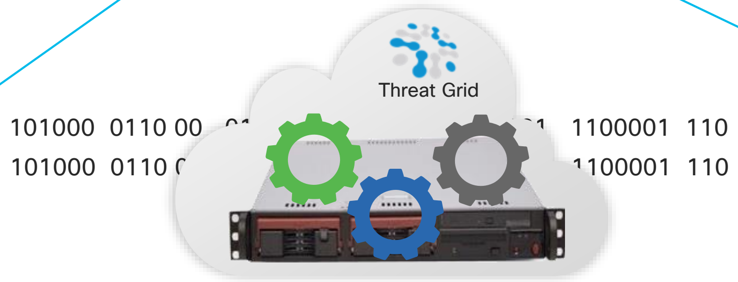
Open Ecosystem DevNet: https://developer.cisco.com/threat-grid/ GitHub: https://github.com/CiscoSecurity

cisco Live!

Introducing Threat Grid

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

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



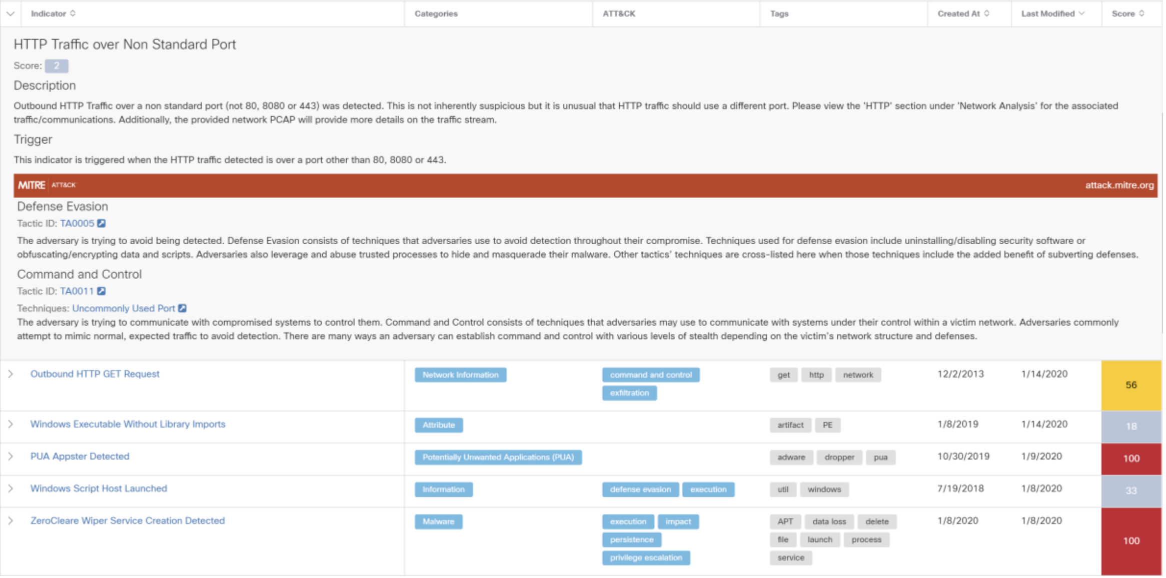
An automated engine observes, deconstructs, and analyzes using multiple techniques

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

- "Outside looking in" approach / No presence in the virtual machine
- Obscured virtual machine "tells"
- Observes all changes to local host and network communications
- Wide range of supported file types
- Network Exit Localization, Playbooks and Evasion Behavior Indicators

Introducing Threat Grid

- …producing <u>human readable behavioral indicators</u> for files submitted.
- 1650+ behavioral indicators that let you prioritize threats with confidence
- Malware families, malicious behaviors, and more (not just signatures)
- Detailed description and actionable information
- Mitre ATT&CK alignment
- Orbital query integration



HTTP Traffic over Non Standard Port

Score: 2

Description

Outbound HTTP Traffic over a non standard port (not 80, 8080 or 443) was detected. This is not inherently suspicious but it is unusual that HTTP traffic should use a different port. Please view the 'HTTP' section under 'Network Analysis' for the associated traffic/communications. Additionally, the provided network PCAP will provide more details on the traffic stream.

Trigger

This indicator is triggered when the HTTP traffic detected is over a port other than 80, 8080 or 443.

MITRE ATT&CK attack.mitre.org

Defense Evasion

Tactic ID: TA0005

The adversary is trying to avoid being detected. Defense Evasion consists of techniques that adversaries use to avoid detection throughout their compromise. Techniques used for defense evasion include uninstalling/disabling security software or obfuscating/encrypting data and scripts. Adversaries also leverage and abuse trusted processes to hide and masquerade their malware. Other tactics' techniques are cross-listed here when those techniques include the added benefit of subverting defenses.

Command and Control

Tactic ID: TA0011

Techniques: Uncommonly Used Port

The adversary is trying to communicate with compromised systems to control them. Command and Control consists of techniques that adversaries may use to communicate with systems under their control within a victim network. Adversaries commonly attempt to mimic normal, expected traffic to avoid detection. There are many ways an adversary can establish command and control with various levels of stealth depending on the victim's network structure and defenses.

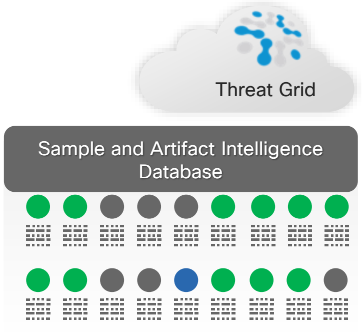
Indicator	Categories	ATT&CK	Tags	Created At	Last Modified	Score
Outbound HTTP GET Request	Network Information	command and control exfiltration	get http network	12/2/2013	1/14/2020	56
Windows Executable Without Library Imports	Attribute		artifact PE	1/8/2019	1/14/2020	18
PUA Appster Detected	Potentially Unwanted Applications (PUA)		adware dropper pua	10/30/2019	1/9/2020	100
Windows Script Host Launched	Information	defense evasion execution	util windows	7/19/2018	1/8/2020	33
ZeroCleare Wiper Service Creation Detected	Malware	execution impact persistence privilege escalation	APT data loss delete file launch process service	1/8/2020	1/8/2020	100

Introducing Threat Grid

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

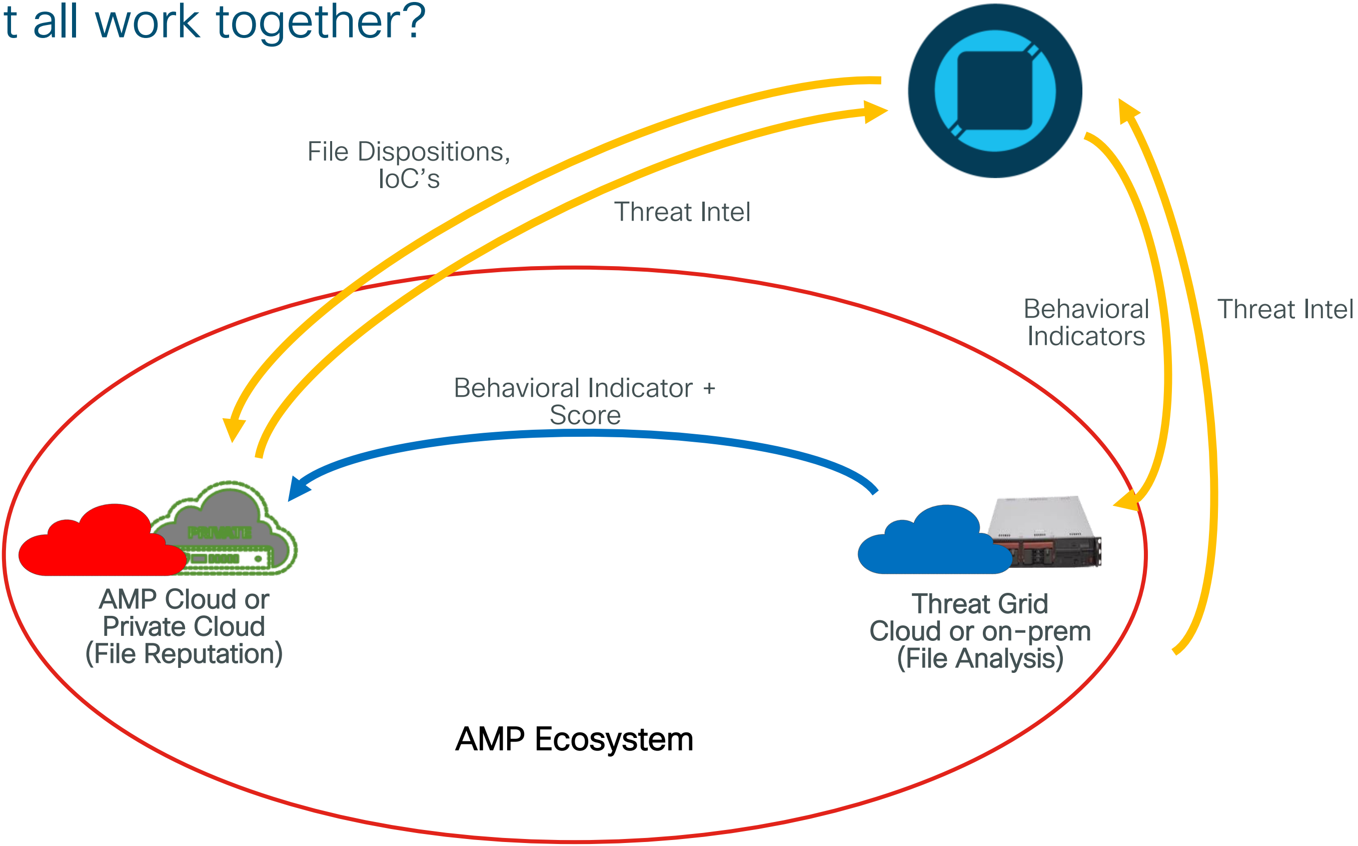
- Samples correlated with billions of malware artifacts
- Global / historical context on threat landscape

- Create custom feeds with context/metadata
- Download curated feeds
- Various formats (JSON, CyBOX, STIX, CSV, or Snort rules)



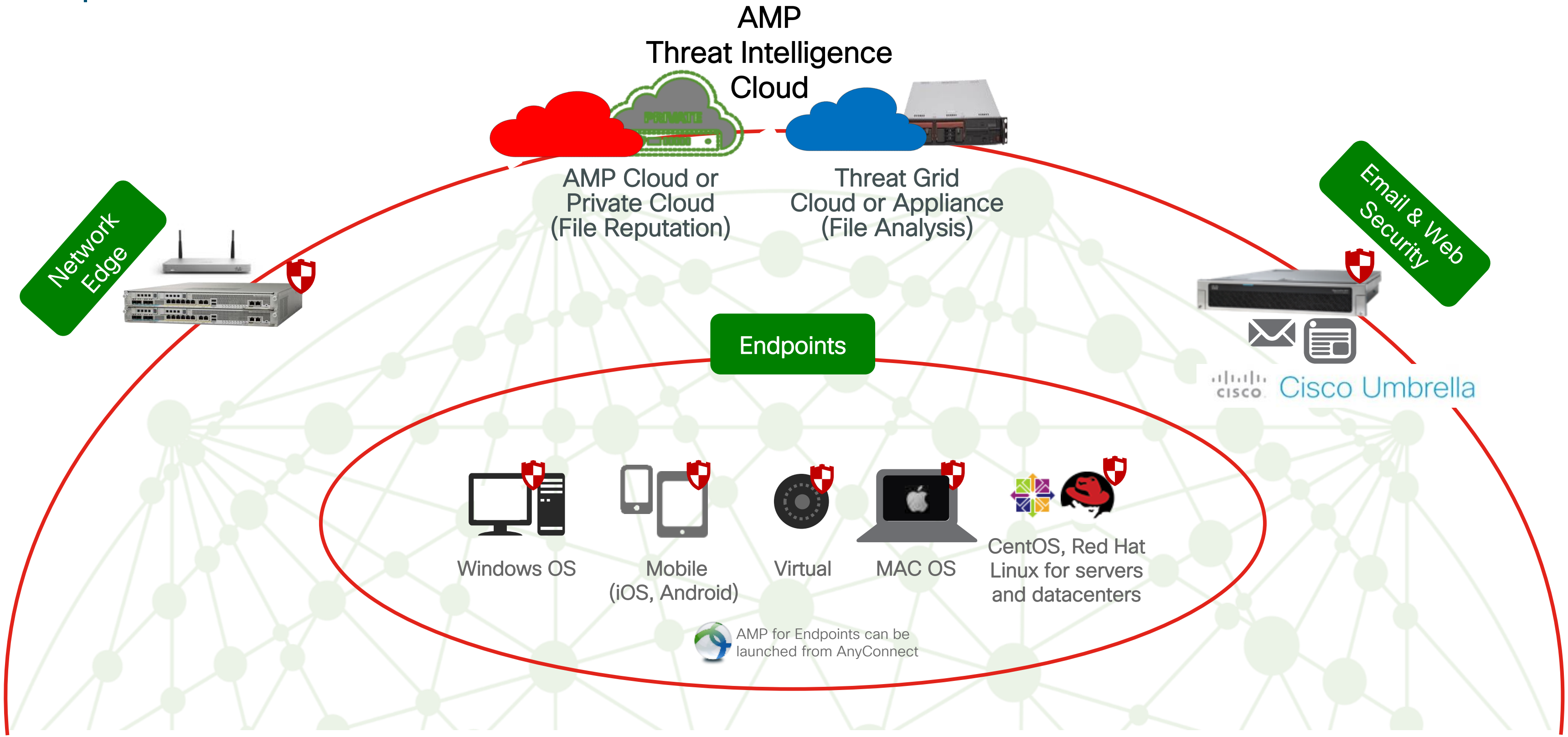
AMP and Threat Grid Integration

How does it all work together?


File Dispositions, IoC's
Threat Intel
Behavioral Indicators
Threat Intel
Behavioral Indicator + Score
AMP Cloud or Private Cloud (File Reputation)
Threat Grid Cloud or on-prem (File Analysis)
AMP Ecosystem

The AMP Everywhere Architecture

Simplified



AMP
Threat Intelligence
Cloud

AMP Cloud or
Private Cloud
(File Reputation)

Threat Grid
Cloud or Appliance
(File Analysis)

Network
Edge

Email & Web
Security

Cisco Umbrella

Endpoints

Windows OS

Mobile
(iOS, Android)

Virtual

MAC OS

CentOS, Red Hat
Linux for servers
and datacenters

AMP for Endpoints can be
launched from AnyConnect

Cisco Advanced Malware Protection Recap

What are we actually providing with the solution?

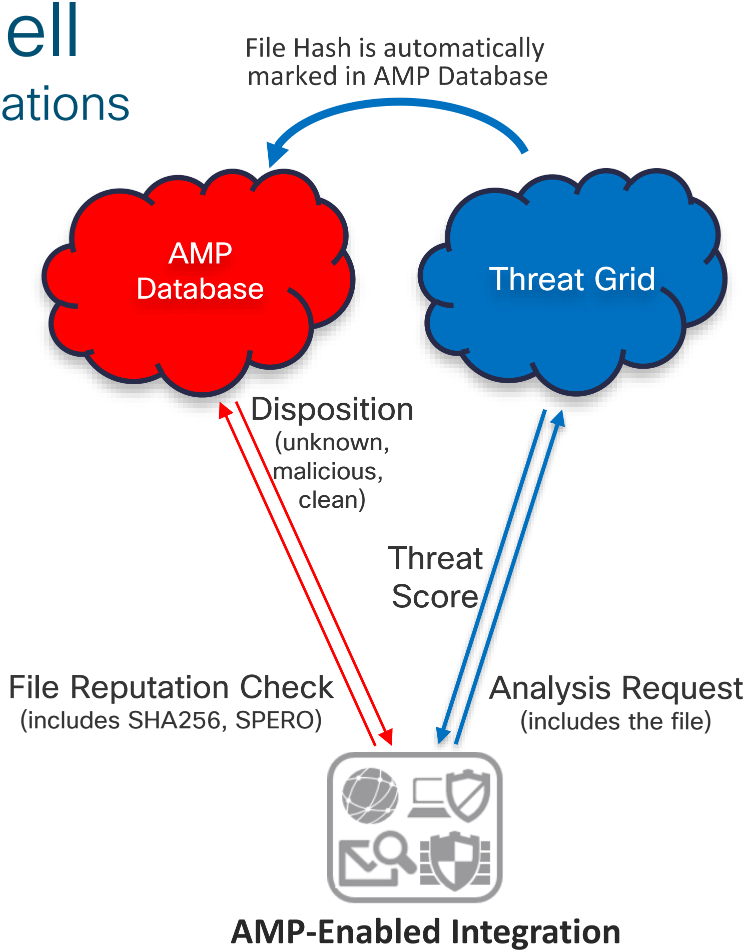
Service	File Reputation	File Analysis	File Retrospection
Function	Blocking of known malicious files	Behavior analysis of unknown files	Retrospective alerting upon disposition change
Powered by	AMP Cloud	Threat Grid Cloud	AMP Cloud
or	AMP PRIVATE	TGA PRIVATE	AMP PRIVATE

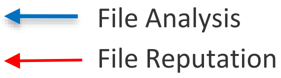
AMP-Enabled Integrations & Capabilities

Service	File Reputation	File Analysis	File Retrospection
Firepower	✓ Active Blocking during Transport	✓ Informative, Manual Remediation	✓ Informative, Manual Remediation
ESA/CES	✓ Active Blocking during Transport	✓ Active Blocking with Quarantine	✓ Manual Or Automatic Remediation with O365
WSA	✓ Active Blocking during Transport	✓ Informative, Manual Remediation	✓ Informative, Manual Remediation
Meraki MX	✓ Active Blocking during Transport	✓ Informative, Manual Remediation	✓ Informative, Manual Remediation
Umbrella	✓ Active Blocking during Transport	✓ Informative, Manual Remediation *SWG Only*	✓ Informative, Manual Remediation *SWG Only*
AMP for Endpoints	✓ Active Blocking at Create, Copy, Move, Execute	✓ Low Prevalence Exe + Manual Submissions	✓ Automatic Remediation

AMP in a Nutshell

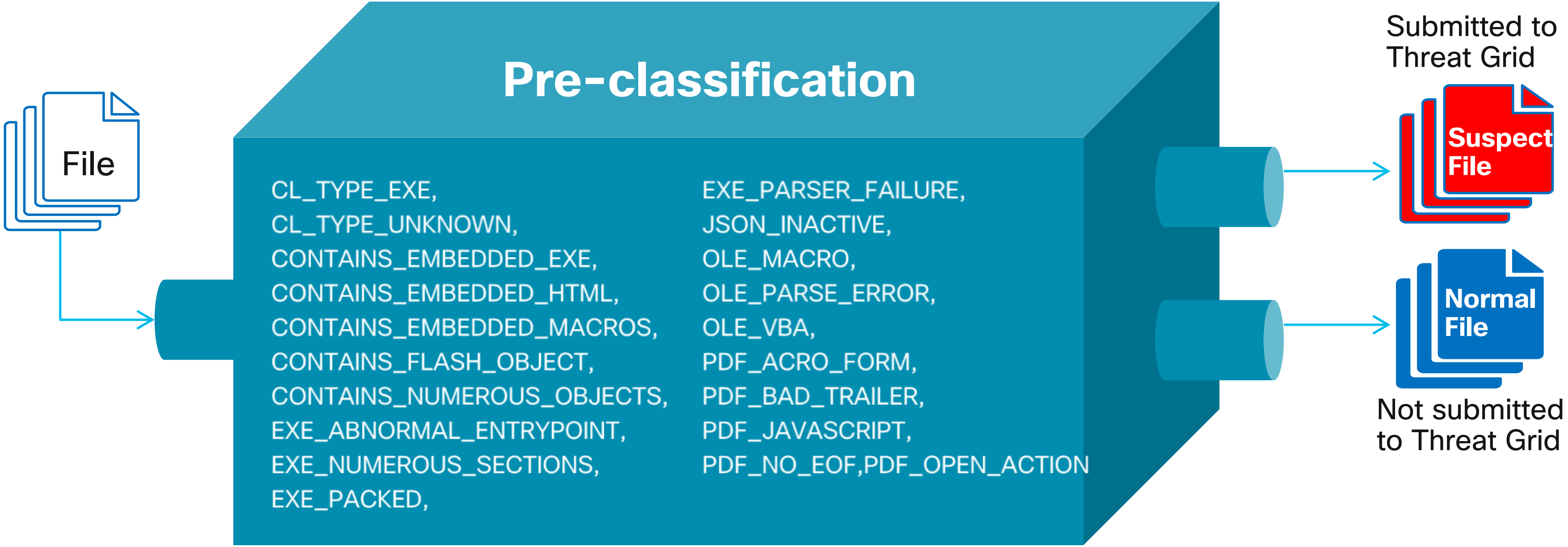
for AMP-Enabled Integrations





File Pre-Classification

Applies CES/ESA, WSA and Firepower



Pre-classification

CL_TYPE_EXE,
CL_TYPE_UNKNOWN,
CONTAINS_EMBEDDED_EXE,
CONTAINS_EMBEDDED_HTML,
CONTAINS_EMBEDDED_MACROS,
CONTAINS_FLASH_OBJECT,
CONTAINS_NUMEROUS_OBJECTS,
EXE_ABNORMAL_ENTRYPOINT,
EXE_NUMEROUS_SECTIONS,
EXE_PACKED,
EXE_PARSER_FAILURE,
JSON_INACTIVE,
OLE_MACRO,
OLE_PARSE_ERROR,
OLE_VBA,
PDF_ACRO_FORM,
PDF_BAD_TRAILER,
PDF_JAVASCRIPT,
PDF_NO_EOF,PDF_OPEN_ACTION

Submitted to Threat Grid

Not submitted to Threat Grid

AMP Deployments

Full Public Cloud

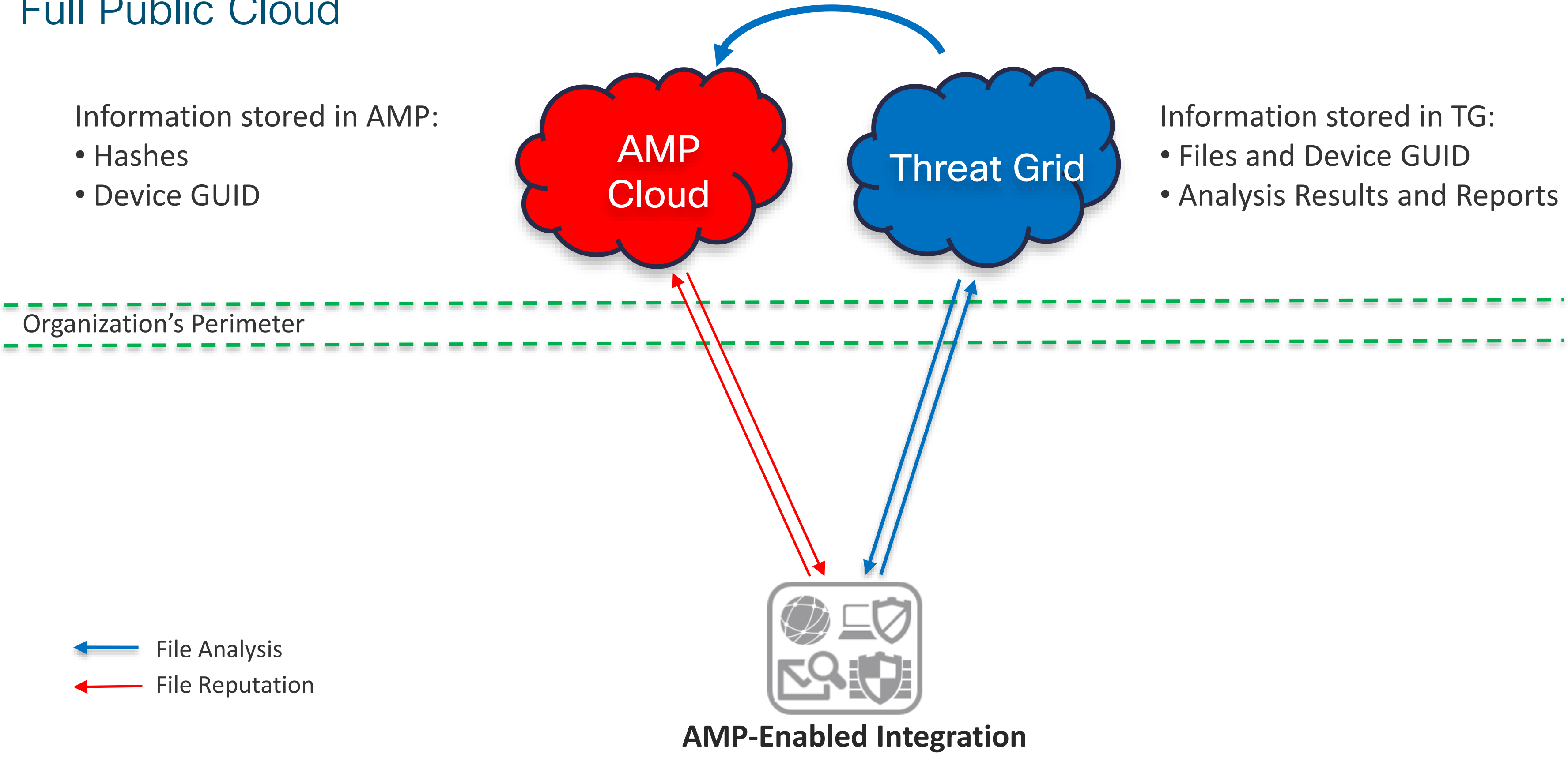
Malicious Files automatically marked in AMP Public Database

Information stored in AMP:

- Hashes
- Device GUID

Information stored in TG:

- Files and Device GUID
- Analysis Results and Reports



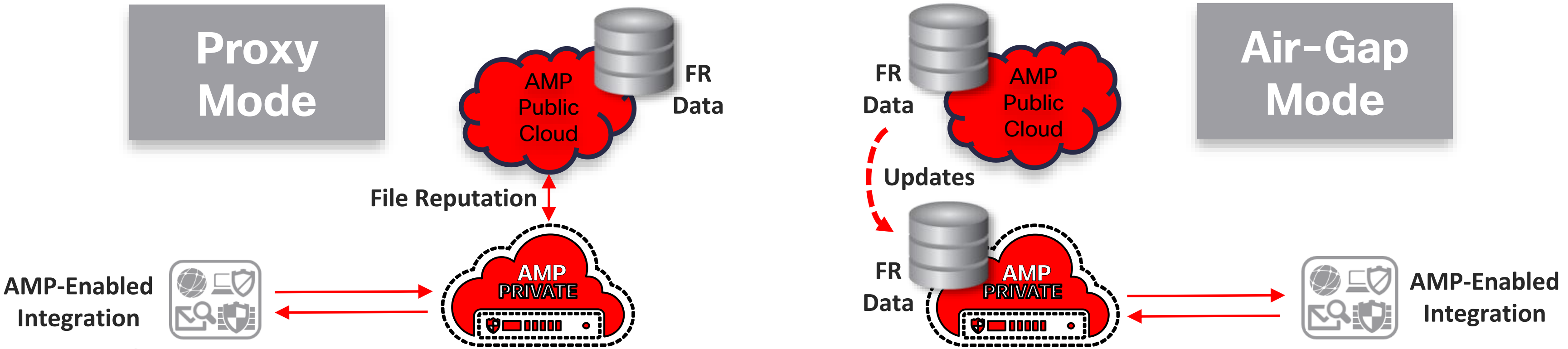
← File Analysis

← File Reputation

AMP Private Cloud (AMP-PC)

Two Deployment Options

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



Cisco Threat Grid On-Premise Appliance

- Provides nearly consistent user experience from cloud to appliance
- Threat Grid Appliances are equipped with a large amount of resources, being able to analyze a large number of files in parallel
- Easy scaling with licenses from 500 to 10,000 submissions per day, per appliance.

- TG5004/5504 (older version)
- TG M5 (current version)

- Appliances can be clustered for redundancy and increased capacity

AMP Deployments with Threat Grid Appliance

- TGA will NEVER send any information back to any cloud
  - Customer invests in TGA for a reason – PRIVACY
  - On-premise TGA's will NEVER be trusted sources for Disposition updates

- Current TGA versions only connect to the Internet for the following operations:
  - Software Updates
  - Internet Access for Samples running inside the VM's via Dirty Interface

Cisco Threat Grid

Appliance vs. Cloud

- Threat Grid Appliance
  - All Samples are local
  - All Artifacts are local
  - No data is sent to the cloud
  - Pivoting on Samples and Artifacts is only based on local data
  - AMP malicious marking can only be achieved on AMP Private Cloud and has only local relevance
  - Submission Limits based on appliance platform and license

- Threat Grid Cloud
  - Manual and API Samples are submitted either as Private or Public (depending on Tagging)
  - AMP-Enabled Integrations (ESA, WSA, Firepower, AMP for Endpoints) 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

For Your Reference

Cisco Threat Grid Appliance

Introduction

- Clean Interface
  - Manual file submissions via Web UI and automated API submissions
  - Need to have connectivity to ESA/WSA and Firepower sensors
- Admin Interface
  - Application management and monitoring
  - Setup & Configuration
  - Updates & Backup/Restore, Logging
- Dirty Interface
  - Provides Internet connectivity for the VMs running malware
  - Also leveraged for software updates

For Your Reference

Threat Grid Appliance Firewall Rules

- Between Dirty Interface and Outside world:
  - Allow:
    - Outbound IP/ANY
    - Outbound TCP/22 (SSH)
    - Outbound TCP/19791 and TCP/20433 for Threat Grid Support
  - Deny
    - Outbound SMTP to prevent Spamming
    - Inbound IP/ANY

- Clean Interface
  - Inbound TCP/443, TCP/8443, TCP/9443 from Internal Network
  - Outbound TCP/19143 to rash.threatgrid.com
- Administrative Interface
  - Inbound TCP/443, TCP/8443 from Internal Network

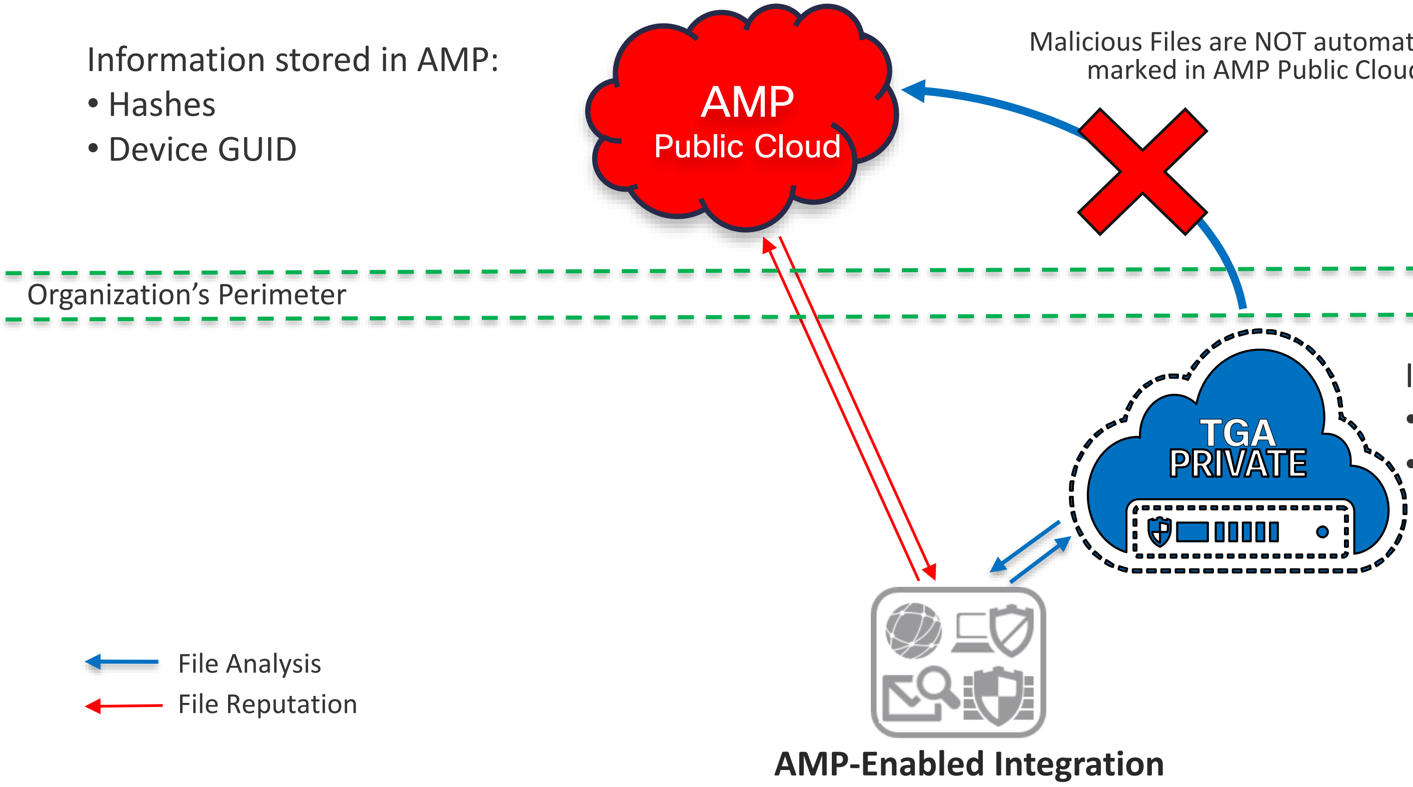
https://techzone.cisco.com/t5/Advanced-Malware-Protection/Required-Ports-for-ThreatGrid-appliance-Communication/ta-p/792218

AMP Deployments

Hybrid for Integrations (except A4E)

Information stored in AMP:

- Hashes
- Device GUID



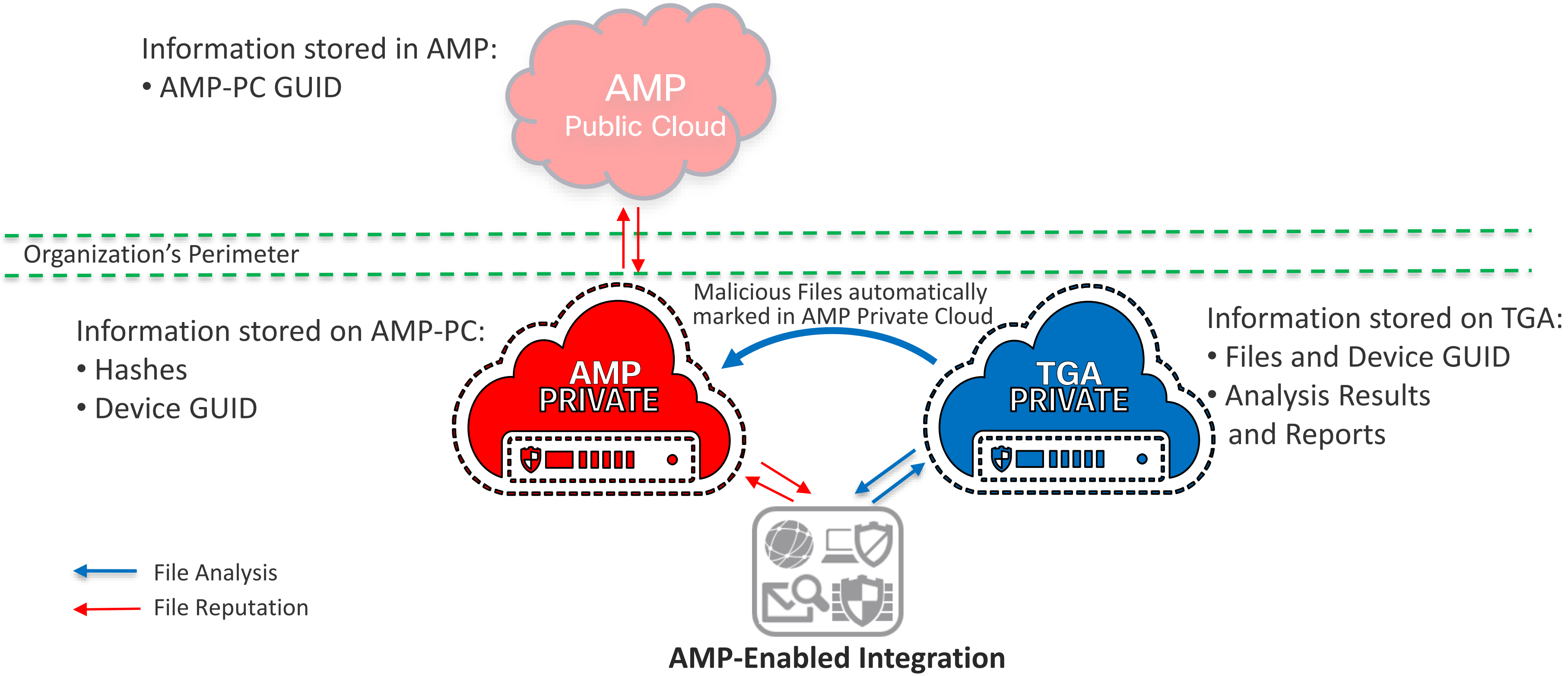
Malicious Files are NOT automatically marked in AMP Public Cloud

Information stored on TGA:

- Files and Device GUID
- Analysis Results and Reports

AMP Deployments

Full Private Cloud for Integrations



Information stored in AMP:
- AMP-PC GUID

Malicious Files automatically marked in AMP Private Cloud

Information stored on AMP-PC:
- Hashes
- Device GUID

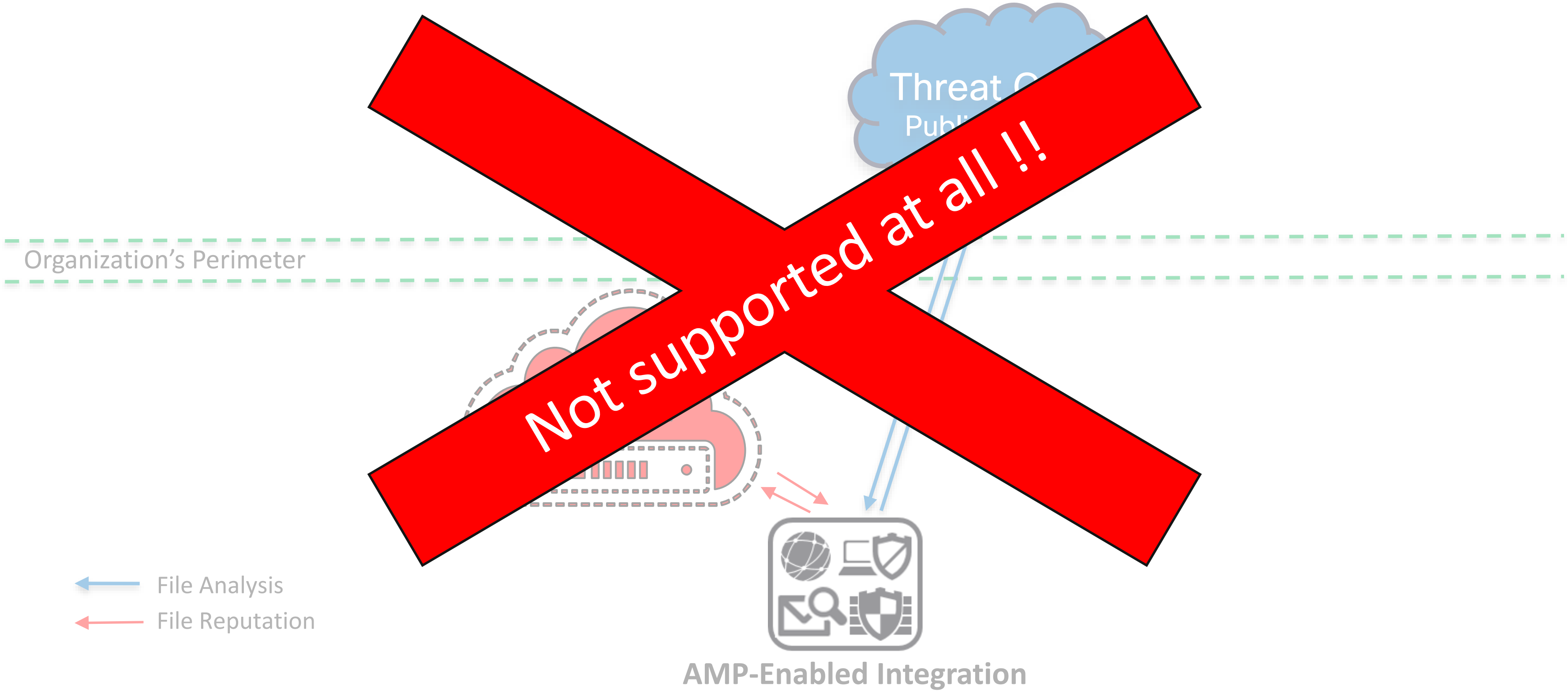
Information stored on TGA:
- Files and Device GUID
- Analysis Results and Reports

← File Analysis

← File Reputation

AMP Deployments

Hybrid for Integrations



AMP & Threat Grid Deployment Options

Deployment Option	**Full Public** AMP Cloud + TG Cloud	**Full Private** AMP PC + TG Appliance	**Hybrid** AMP Cloud + TG Appliance	**Hybrid** AMP PC + TG Cloud
AMP4E	✓	✓	✗	✗
Firepower	✓	✓	✔	✗
ESA/CES	✓	✓ *ESA Only	✔	✗
WSA	✓	✓	✔	✗
Meraki MX	✓	✗	✗	✗
Umbrella	✓	✗	✗	✗

Caution! Breaks the architecture!

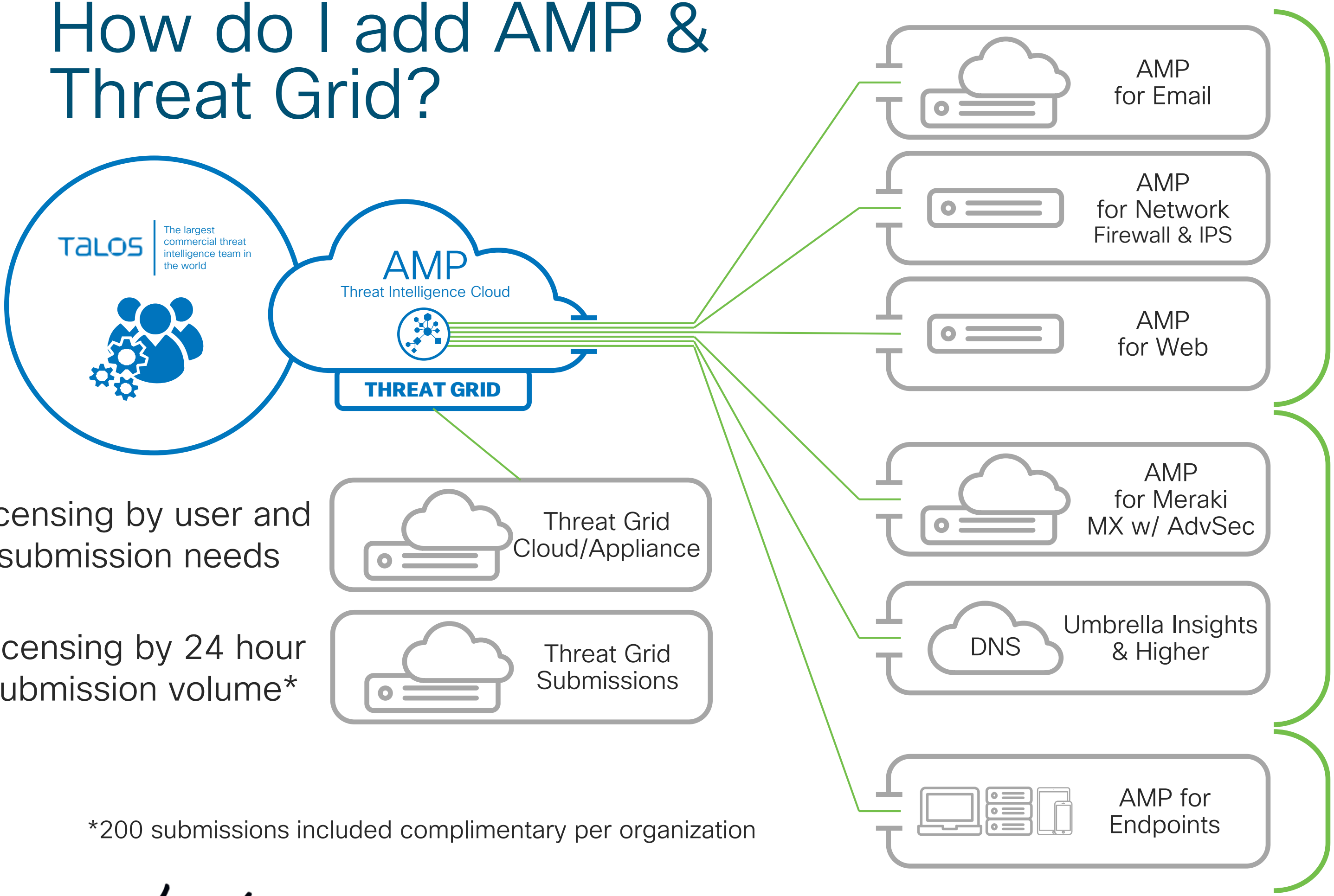
Doesn‘t really make sense...

✓ – recommended deployment option, Full Private for customers with high privacy requirements

✔ – supported, but has drawbacks, Threat Grid Appliance does not talk to the AMP Cloud (does not share analysis results)

✗ – not supported today

How do I add AMP & Threat Grid?



TALOS
The largest commercial threat intelligence team in the world
AMP
Threat Intelligence Cloud
THREAT GRID
Threat Grid Cloud/Appliance
Threat Grid Submissions
AMP for Email
AMP for Network Firewall & IPS
AMP for Web
AMP for Meraki MX w/ AdvSec
DNS
Umbrella Insights & Higher
AMP for Endpoints

Licensing by user and submission needs

Licensing by 24 hour submission volume*

AMP is a simple, quick, **add-on** license – or included in bundles

AMP is **included** in license options

AMP is licensed by **machine**

*200 submissions included complimentary per organization

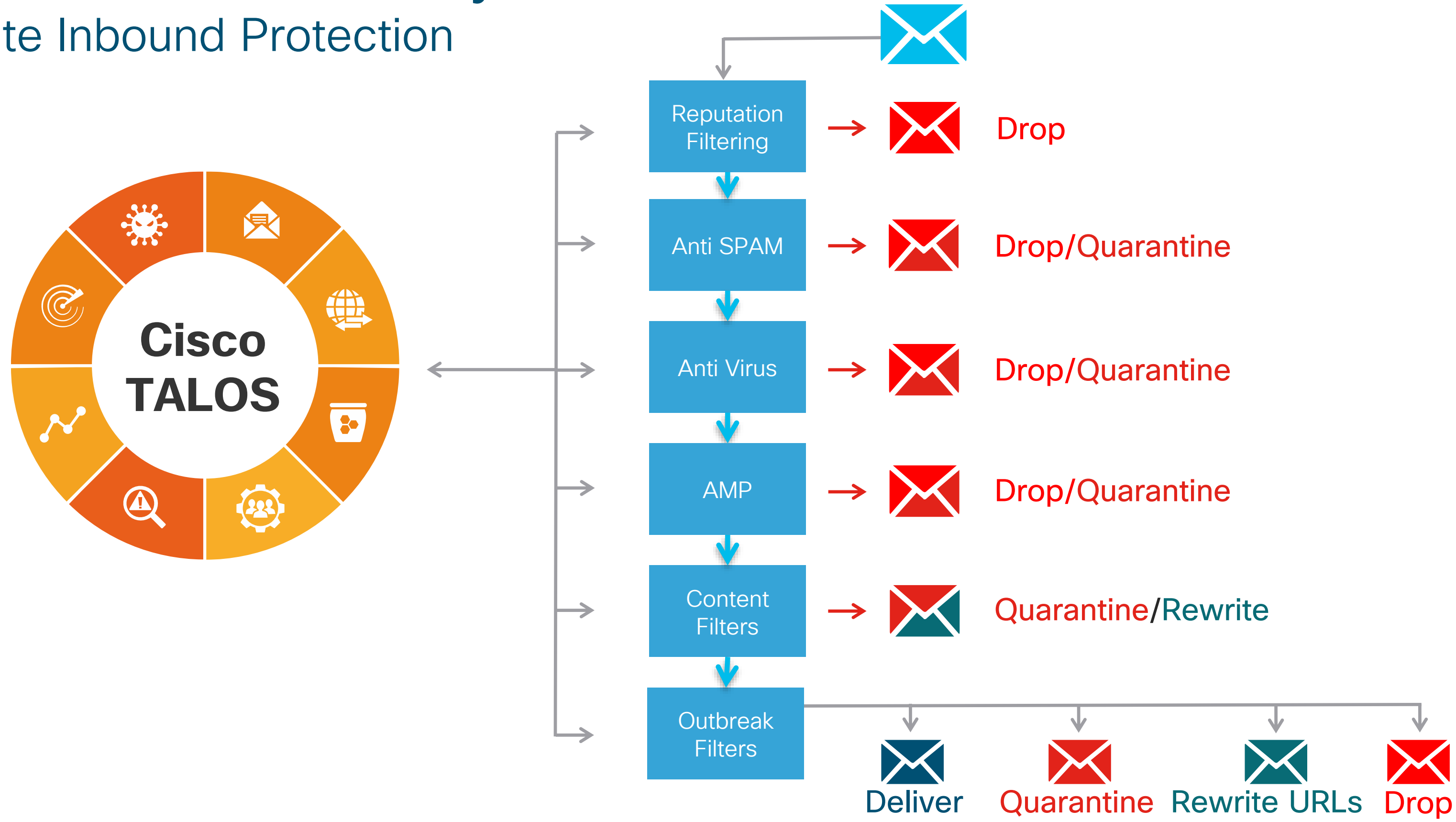
Cisco AMP & Threat Grid for Email Security (ESA/CES)

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

- How the does ESA/CES security stack protect my company?
- Where does AMP fit in, and what happens when?
- How do I configure all this so it works?
- What kind of reporting is available?

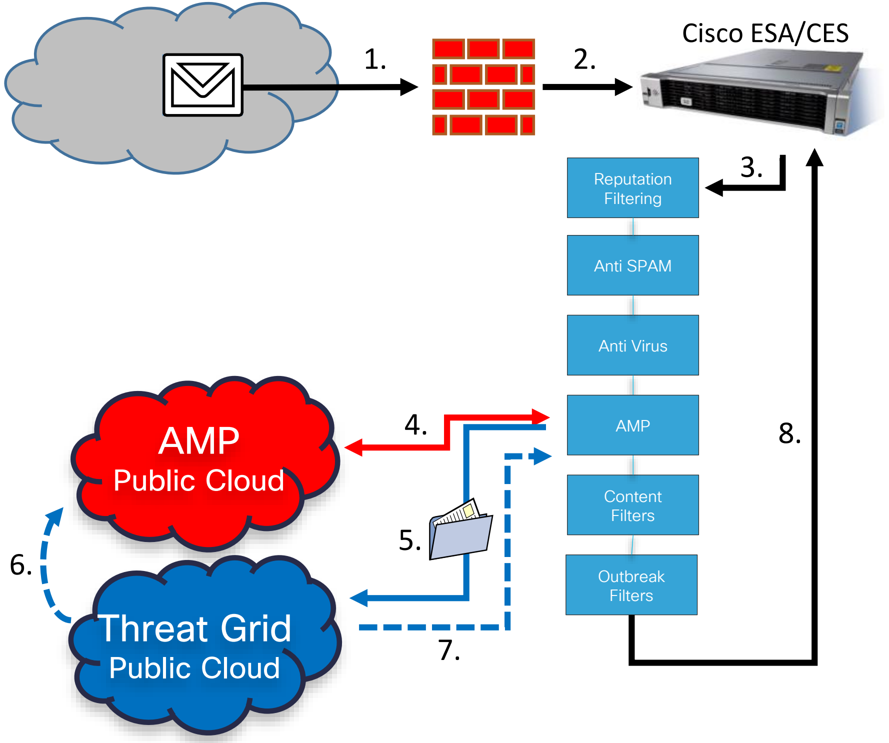
Cisco Email Security

Complete Inbound Protection



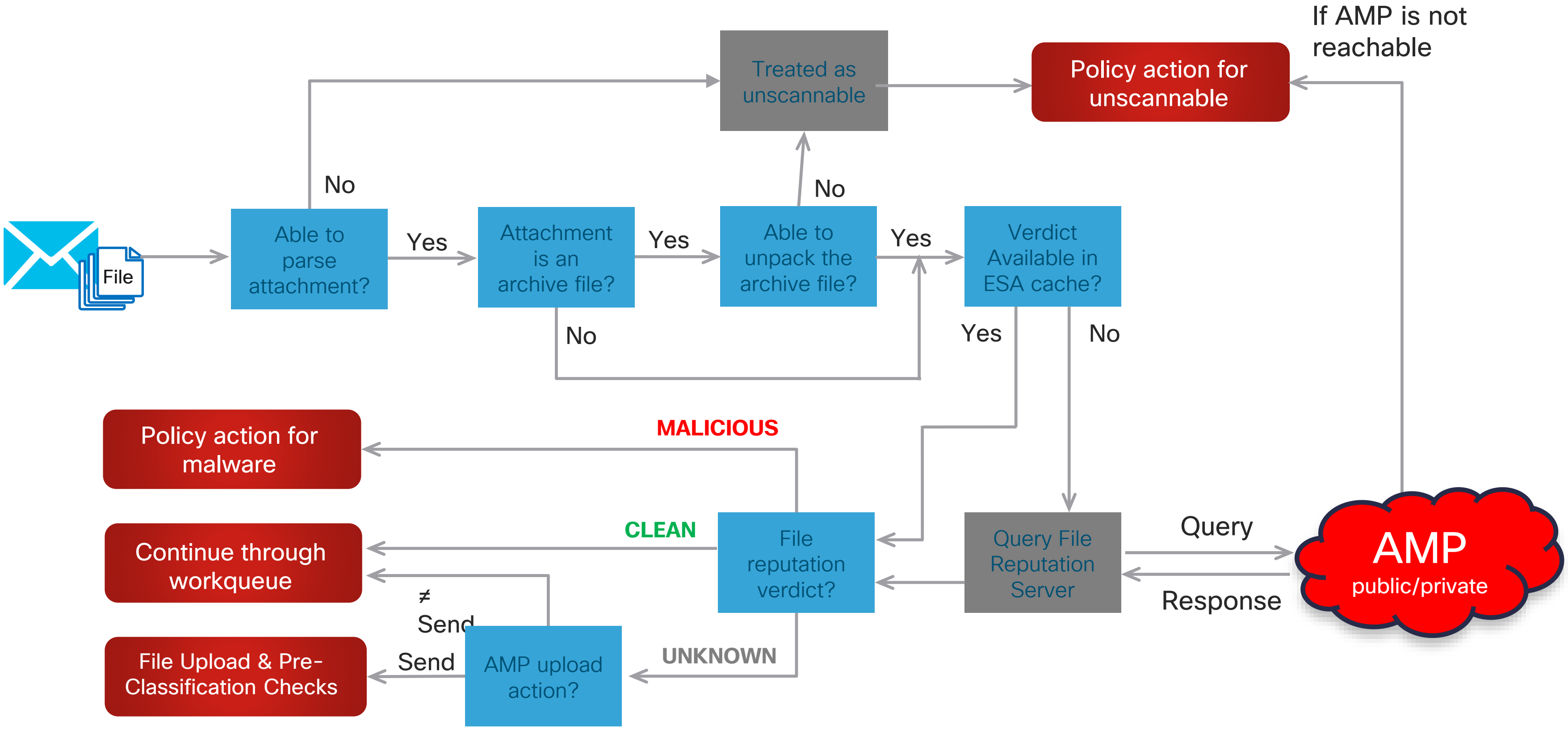
ESA/CES – AMP & Threat Grid Process Flow

Full Public Cloud



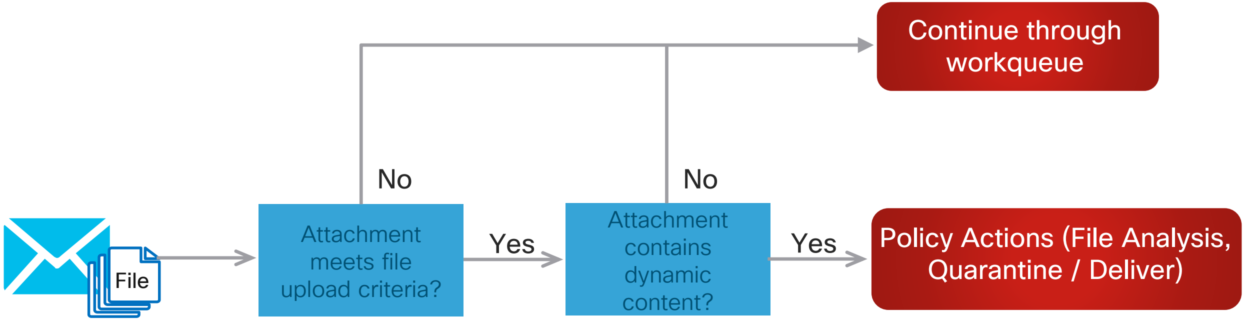
1. Email sent from Internet
2. Accepted by ESA/CES Architecture
3. Email passed through security stack on ESA/CES
4. Threat intelligence from AMP Cloud used to determine if email or attachments match known malicious (SHA Lookup)
5. If file is unknown, may be sent to Threat Grid for analysis, email sent to quarantine per policy
6. Threat Grid analyzes file and updates AMP Cloud with score derived from behavioral indicators. AMP Cloud could mark as malicious from that score.
7. ESA/CES polls for analysis completed and releases message from temporary quarantine if <90, assumes malicious if >90
8. ESA/CES further processes email per policy

AMP File Reputation Workflow


If AMP is not reachable
Treated as unscannable
Policy action for unscannable
No
No
File
Able to parse attachment?
Yes
Attachment is an archive file?
Yes
Able to unpack the archive file?
Yes
Verdict Available in ESA cache?
No
Yes
No
MALICIOUS
Policy action for malware
CLEAN
Continue through workqueue
File reputation verdict?
Query File Reputation Server
Query
Response
AMP
public/private
≠
Send
Send
File Upload & Pre-Classification Checks
AMP upload action?
UNKNOWN

File Upload Criteria and Pre-Classification

For Your Reference


Continue through workqueue
No
No
File
Attachment meets file upload criteria?
Yes
Attachment contains dynamic content?
Yes
Policy Actions (File Analysis, Quarantine / Deliver)

File Upload Criteria:

- Supported File Type
- Attachment size <= 100 MB

AMP on Email – File Types & Pre-Classification

- Number of supported file types has been enhanced with ESA/CES version v11.1. File Types are now on par with Threat Grid Cloud.
- Before an unknown file is submitted the on-box pre-classification engine [ClamAV] scans it to select only files with active or suspicious content
  - Pre-classification signatures
  - Byte code rules that uncover suspicious indicators
  - Signatures developed and updated by Talos – updated via cloud regularly
- Additional Threat Grid classification occurs on v11.1+
  - Saves on Threat Grid dynamic analysis
- Highly recommend v12.5.0-66 or newer

AMP on Email with Threat Grid Public Cloud

Considerations

- Threat Grid updates AMP Cloud with file scores from Analysis
  - AMP Cloud will determine final disposition from this and other sources
- If the file was submitted to Threat Grid cloud and receives a Threat Score of 90 or higher then ESA/CES considers the file malicious until a true disposition comes from AMP Cloud (Retrospective)
- ESA/CES waits for the analysis to finish, updates the file reputation cache and then sends the file through AV and AMP again
- Malware can also be convicted by AMP File Reputation due to the adjusted disposition (Retrospective)

AMP on ESA with Threat Grid Appliance

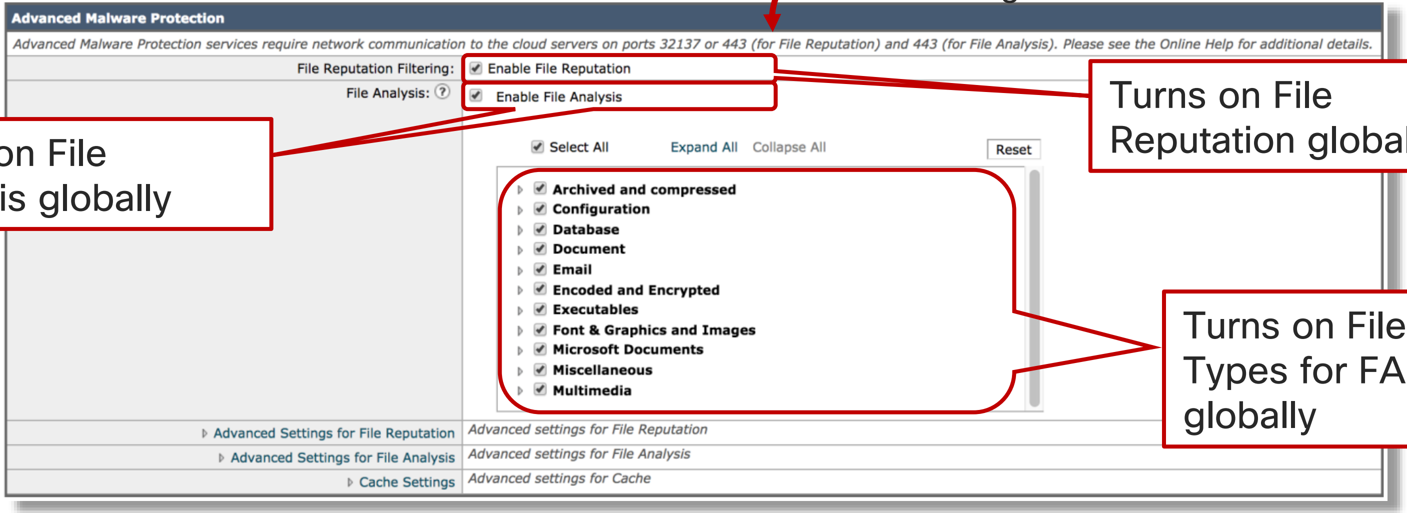
Considerations

- Reminder: TGA will NEVER send any information back to any cloud!!
- ESA receives a score from the TGA
  - ESA will consider a file malicious if score is 95 or higher (default setting)
  - A score of under 95 will not have an effect on processing
  - In this case, Malware will be convicted directly by TGA score
- This does have further implications:
  - For hybrid deployments, further AMP file reputation checks for the same SHA256 on the AMP cloud could still result in “unknown” disposition until AMP cloud is updated from another source
  - For fully on-premise deployments, TGA integrates with AMP Private Cloud Appliance (AMP-PC) and does update disposition there
  - Those updated AMP-PC dispositions are only locally significant

Configuring AMP for Email

Enable AMP Services

- Security Services > File Reputation and Analysis
- You can choose whether to enable or disable two services:
  - File Reputation (SHA-256)
  - File Analysis (Threat Grid integration)



Advanced Malware Protection

Advanced Malware Protection services require network communication to the cloud servers on ports 32137 or 443 (for File Reputation) and 443 (for File Analysis). Please see the Online Help for additional details.

File Reputation Filtering: ☑ Enable File Reputation

File Analysis: ☑ Enable File Analysis

☑ Select All — Expand All — Collapse All — Reset

- ☑ Archived and compressed
- ☑ Configuration
- ☑ Database
- ☑ Document
- ☑ Email
- ☑ Encoded and Encrypted
- ☑ Executables
- ☑ Font & Graphics and Images
- ☑ Microsoft Documents
- ☑ Miscellaneous
- ☑ Multimedia

Advanced Settings for File Reputation	*Advanced settings for File Reputation*
Advanced Settings for File Analysis	*Advanced settings for File Analysis*
Cache Settings	*Advanced settings for Cache*

Note the ports, recommendation to enable 443 in advanced settings

Turns on File Reputation globally

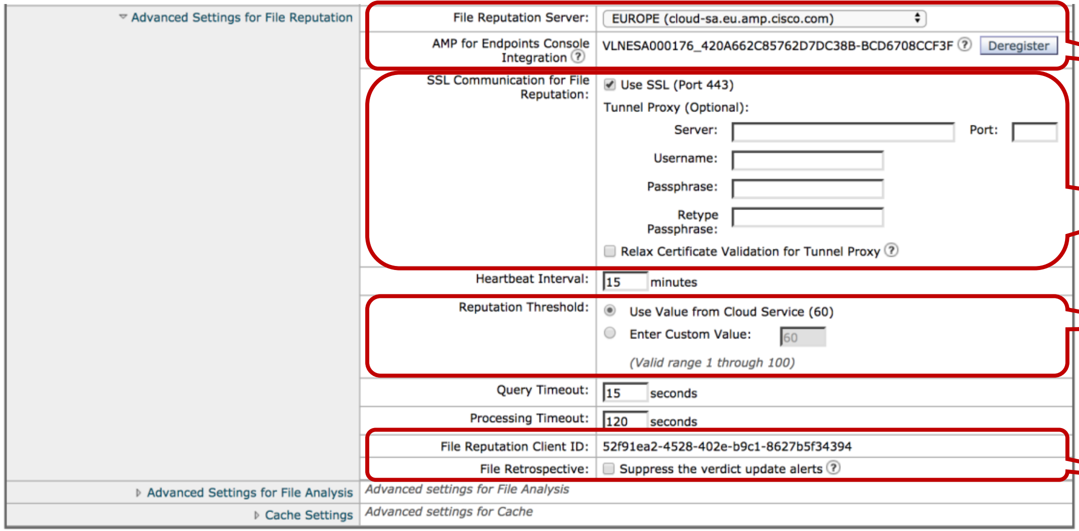
Turns on File Analysis globally

Turns on File Types for FA globally

Configuring AMP for Email

Advanced Settings for File Reputation

- Can be left as defaults in most of the cases
- Configuration to enable AMP PC, AMP Unity, Internet Proxies and via SSL TCP/443



▿ Advanced Settings for File Reputation

File Reputation Server:	EUROPE (cloud-sa.eu.amp.cisco.com)
AMP for Endpoints Console Integration ?	VLNESA000176_420A662C85762D7DC38B-BCD6708CCF3F ? Deregister
SSL Communication for File Reputation:	☑ Use SSL (Port 443) Tunnel Proxy (Optional): Server: Port: Username: Passphrase: Retype Passphrase: □ Relax Certificate Validation for Tunnel Proxy ?
Heartbeat Interval:	15 minutes
Reputation Threshold:	● Use Value from Cloud Service (60) ○ Enter Custom Value: 60 *(Valid range 1 through 100)*
Query Timeout:	15 seconds
Processing Timeout:	120 seconds
File Reputation Client ID:	52f91ea2-4528-402e-b9c1-8627b5f34394
File Retrospective:	□ Suppress the verdict update alerts ?

▹ Advanced Settings for File Analysis — *Advanced settings for File Analysis*

▹ Cache Settings — *Advanced settings for Cache*

Select Data Center for File Reputation. Register For AMP Unity (AMP Cloud)

Use SSL is highly recommended. Optional configuration of proxy server

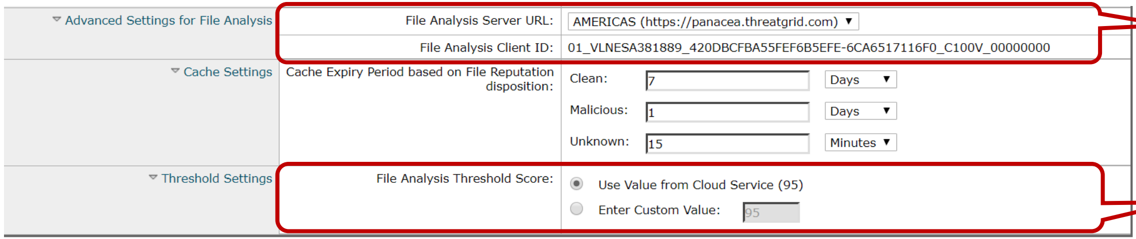
Deprecated, please ignore these settings in versions >12.x

File Reputation Client ID and ability to enable suppression of Retrospective Events for dropped messages

Configuring AMP for Email

Advanced Settings for File Analysis

- Defaults are valid for North America Threat Grid Cloud, can select Europe or Private Analysis Cloud (Threat Grid)



▽ Advanced Settings for File Analysis

File Analysis Server URL: AMERICAS (https://panacea.threatgrid.com) ▼

File Analysis Client ID: 01_VLNESA381889_420DBCFBA55FEF6B5EFE-6CA6517116F0_C100V_00000000

▽ Cache Settings

Cache Expiry Period based on File Reputation disposition:

Clean: 7 Days ▼

Malicious: 1 Days ▼

Unknown: 15 Minutes ▼

▽ Threshold Settings

File Analysis Threshold Score:

● Use Value from Cloud Service (95)

○ Enter Custom Value: 95

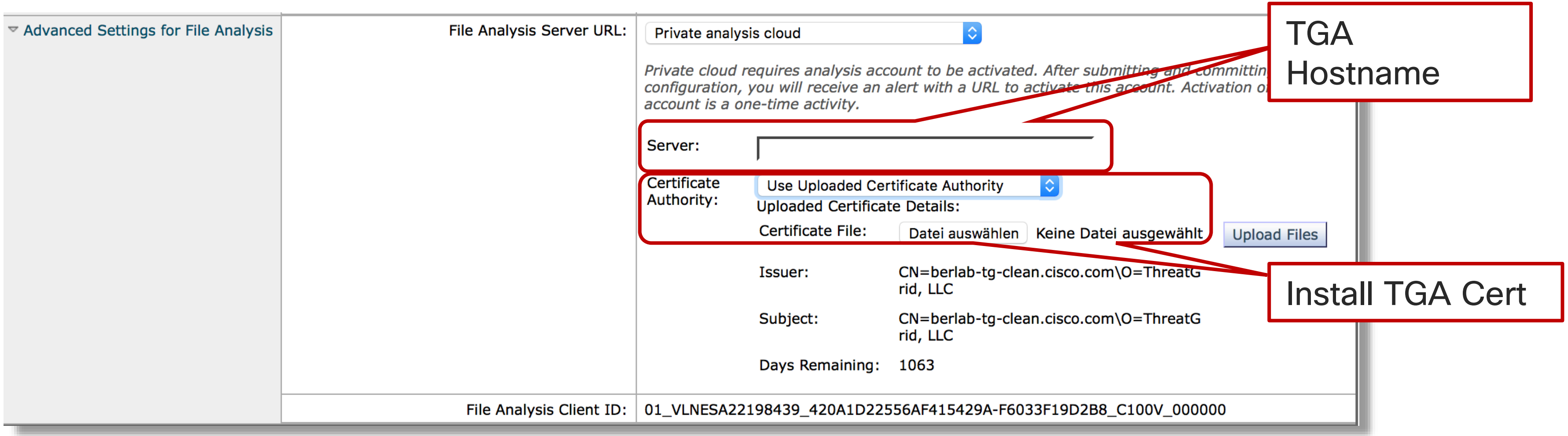
Configure Threat Grid datacenter (or appliance) and view File Analysis ID.

(v12.1+) Configure score to consider malicious for Threat Grid results. Bill recommends the default.

Configuring AMP for Email

Advanced Settings for File Analysis (TG Appliance)

- Selecting Private analysis cloud reveals more options
- Upload TGA self-signed certificate or issued certificate from PKI
- If an organization’s PKI is used, upload complete certificate chain



Advanced Settings for File Analysis

File Analysis Server URL: Private analysis cloud

Private cloud requires analysis account to be activated. After submitting and committin configuration, you will receive an alert with a URL to activate this account. Activation o account is a one-time activity.

Server:

Certificate Authority: Use Uploaded Certificate Authority

Uploaded Certificate Details:

Certificate File: Datei auswählen Keine Datei ausgewählt

Issuer: CN=berlab-tg-clean.cisco.com\O=ThreatGrid, LLC

Subject: CN=berlab-tg-clean.cisco.com\O=ThreatGrid, LLC

Days Remaining: 1063

File Analysis Client ID: 01_VLNESA22198439_420A1D22556AF415429A-F6033F19D2B8_C100V_000000

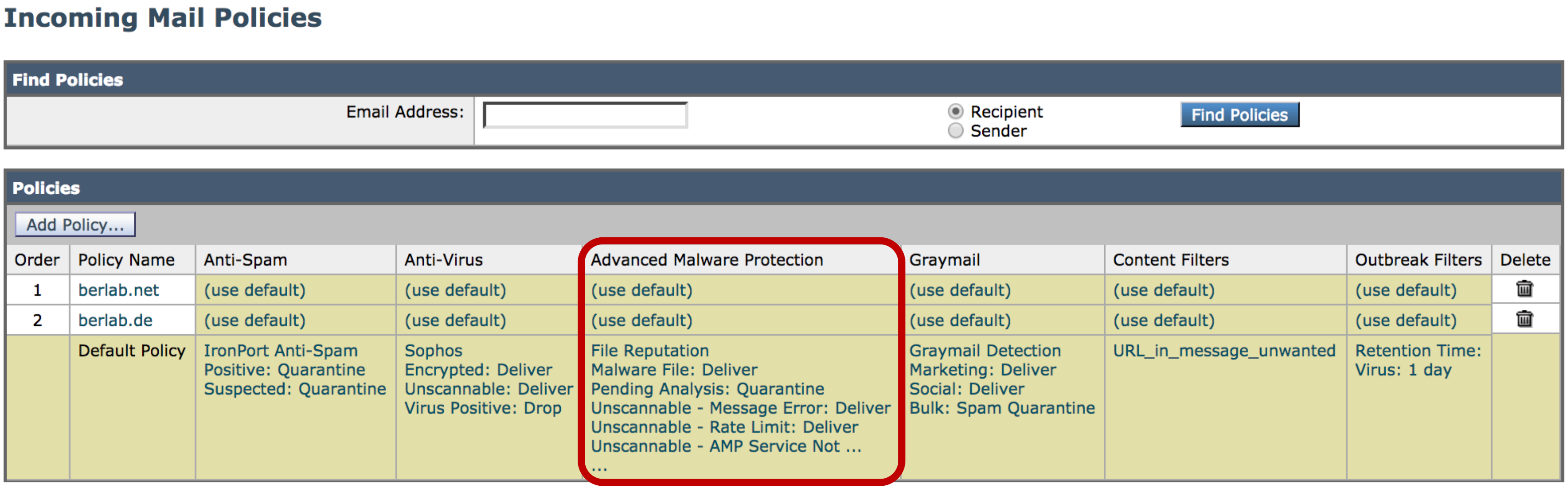
TGA Hostname

Install TGA Cert

Configuring AMP for Email

Incoming Mail Policy

- Mail Policies > Incoming (or Outgoing) Mail Policies
- Click on the link to change AMP-related policy settings



Incoming Mail Policies

Find Policies

Email Address: ______ ● Recipient ○ Sender Find Policies

Policies

Add Policy...

Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Delete
1	berlab.net	(use default)	(use default)	(use default)	(use default)	(use default)	(use default)	🗑
2	berlab.de	(use default)	(use default)	(use default)	(use default)	(use default)	(use default)	🗑
	Default Policy	IronPort Anti-Spam Positive: Quarantine Suspected: Quarantine	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	File Reputation Malware File: Deliver Pending Analysis: Quarantine Unscannable - Message Error: Deliver Unscannable - Rate Limit: Deliver Unscannable - AMP Service Not	Graymail Detection Marketing: Deliver Social: Deliver Bulk: Spam Quarantine	URL_in_message_unwanted	Retention Time: Virus: 1 day	

Configuring AMP for Email

Edit Incoming Mail Policy

How to handle Unscannable Attachments

How to handle File Analysis Submission limits

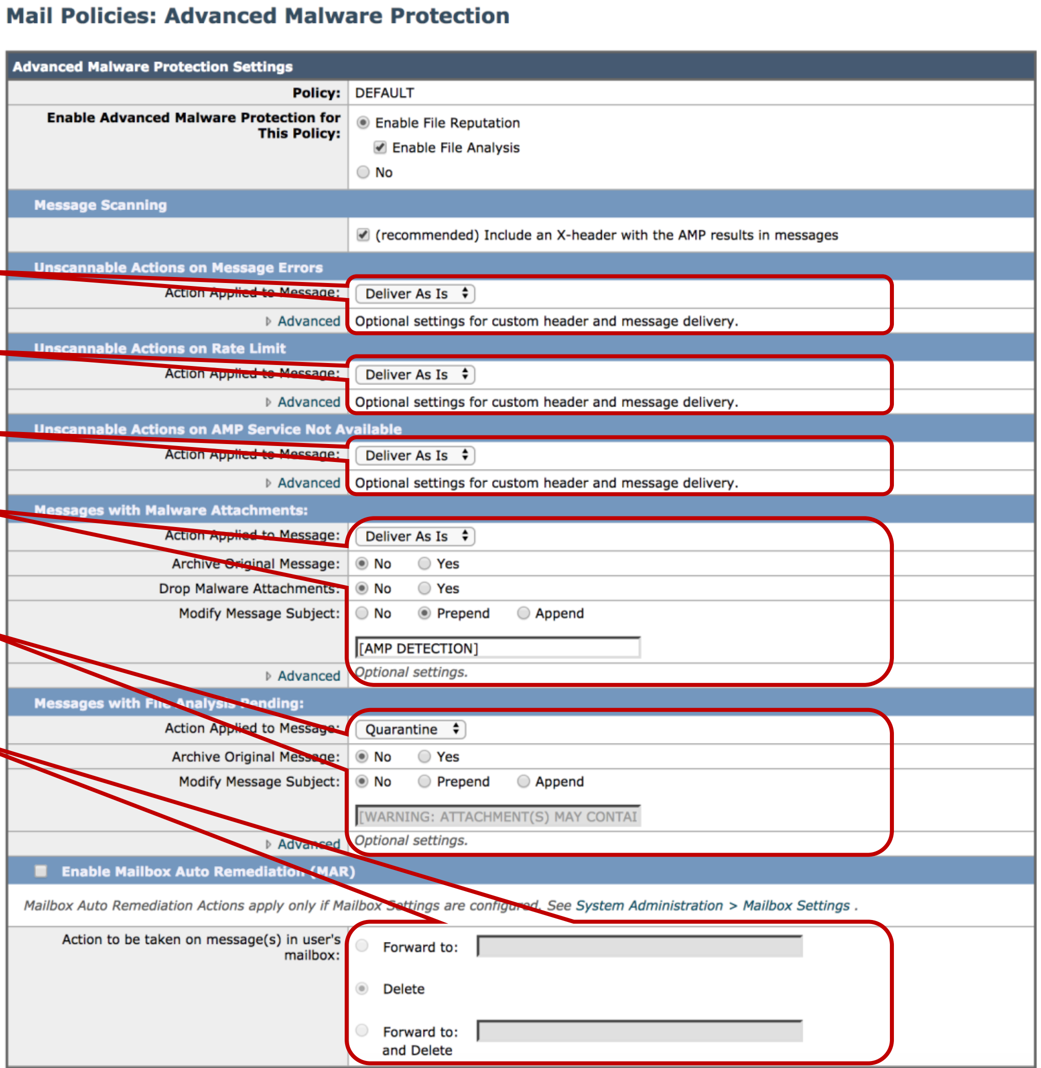
How to hand File Reputation unavailable

How to handle Malicious Attachments

How should ESA handle Messages with Attachments currently in File Analysis

Mailbox Auto Remediation, see next slides ...

- General Policy options:
  - Drop entire message or attachment
  - Modify message subject, add header
  - Hold message in temporary quarantine



Mail Policies: Advanced Malware Protection

Advanced Malware Protection Settings

Policy:	DEFAULT
Enable Advanced Malware Protection for This Policy:	● Enable File Reputation ☑ Enable File Analysis ○ No

Message Scanning

☑ (recommended) Include an X-header with the AMP results in messages

Unscannable Actions on Message Errors

Action Applied to Message:	Deliver As Is
▹ Advanced	Optional settings for custom header and message delivery.

Unscannable Actions on Rate Limit

Action Applied to Message:	Deliver As Is
▹ Advanced	Optional settings for custom header and message delivery.

Unscannable Actions on AMP Service Not Available

Action Applied to Message:	Deliver As Is
▹ Advanced	Optional settings for custom header and message delivery.

Messages with Malware Attachments:

Action Applied to Message:	Deliver As Is
Archive Original Message:	● No ○ Yes
Drop Malware Attachments:	● No ○ Yes
Modify Message Subject:	○ No ● Prepend ○ Append [AMP DETECTION]
▹ Advanced	Optional settings.

Messages with File Analysis Pending:

Action Applied to Message:	Quarantine
Archive Original Message:	● No ○ Yes
Modify Message Subject:	● No ○ Prepend ○ Append [WARNING: ATTACHMENT(S) MAY CONTAI
▹ Advanced	Optional settings.

☐ **Enable Mailbox Auto Remediation (MAR)**

Mailbox Auto Remediation Actions apply only if Mailbox Settings are configured. See System Administration > Mailbox Settings .

Action to be taken on message(s) in user's mailbox:	○ Forward to: ● Delete ○ Forward to: and Delete

cisco Live!

Mailbox Auto Remediation (MAR)

Use Case and Overview

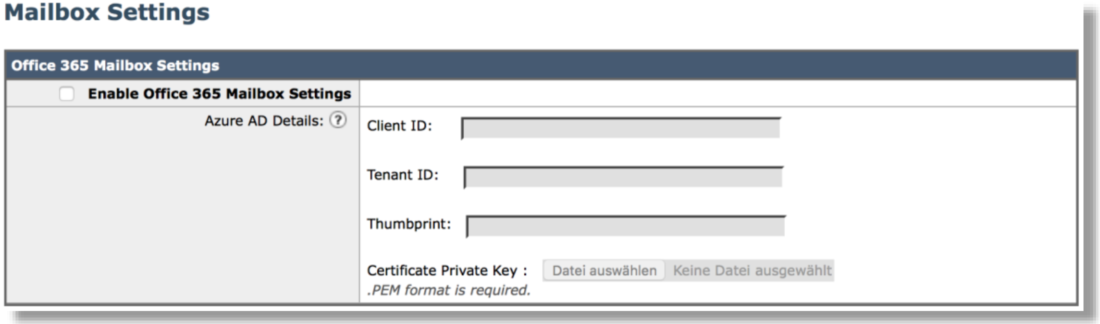
- The AMP engine on the ESA/CES provides reports for retrospective events (aka verdict changes) to let an administrator know if a file has evaded detection and was delivered to a user's inbox, but was detected malicious later
- MAR goes beyond that and allows an administrator to configure ESA/CES to recall a message from:
  - Microsoft Office 365 cloud: supported in v10+ of ESA/CES
  - Exchange 2013 and 2016: supported in v13+ of ESA/CES
- ESA/CES is able to leverage API calls to pull the related messages and their malicious attachments from the user's inbox and quarantine them
- This automation allows for faster action to be taken upon discovery of message attachments that have evaded detection at the first place

For Your Reference

Configuring AMP for Email

Mailbox Auto Remediation

- Systems Administration -> Mailbox Settings
  - Configure your Office 365 Credentials
  - Import Certificate



Mailbox Settings

Office 365 Mailbox Settings

☐ **Enable Office 365 Mailbox Settings**

Azure AD Details: ?

Client ID:

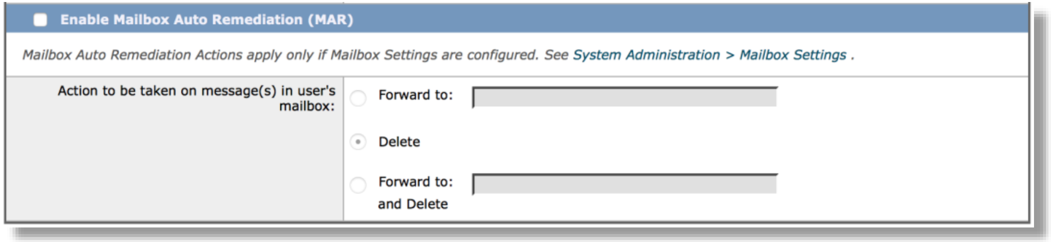
Tenant ID:

Thumbprint:

Certificate Private Key : Datei auswählen Keine Datei ausgewählt

.PEM format is required.

- Incoming Mail Policy -> Edit
  - Configure Action to be taken as soon as a retrospective event is triggering



☐ **Enable Mailbox Auto Remediation (MAR)**

Mailbox Auto Remediation Actions apply only if Mailbox Settings are configured. See System Administration > Mailbox Settings .

Action to be taken on message(s) in user's mailbox:

○ Forward to:

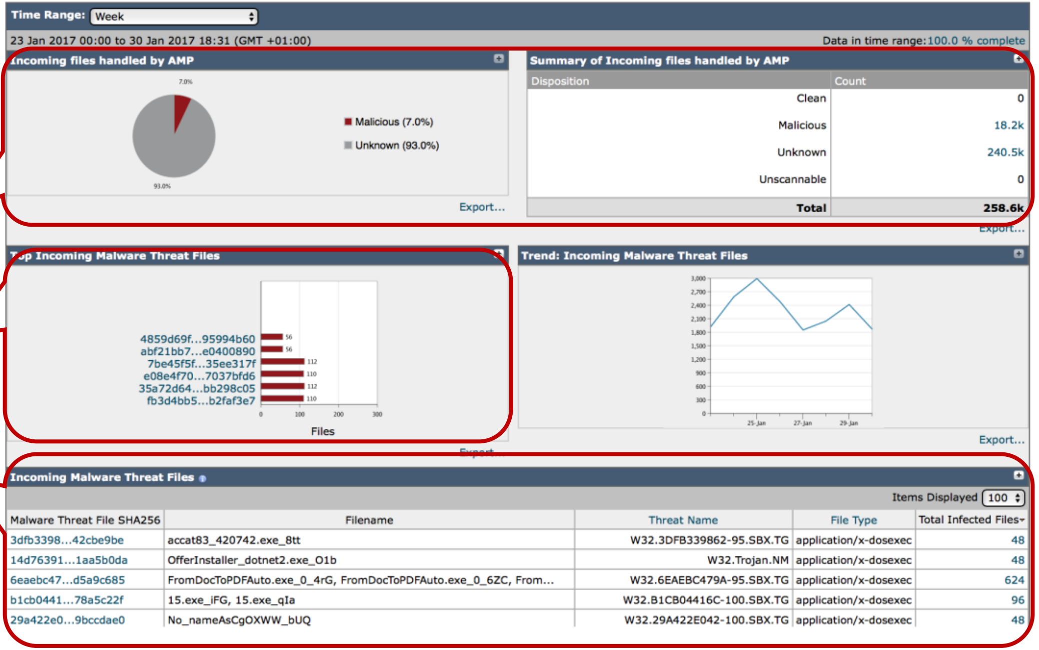
● Delete

○ Forward to: and Delete

AMP Event Analysis

AMP Malware Events

- Reporting > Advanced Malware Protection
  - These statistics are intended to provide detailed AMP file reputation results



Time Range: Week

23 Jan 2017 00:00 to 30 Jan 2017 18:31 (GMT +01:00)

Data in time range: 100.0 % complete

Incoming files handled by AMP

Summary of Incoming files handled by AMP

Disposition	Count
Clean	0
Malicious	18.2k
Unknown	240.5k
Unscannable	0
Total	258.6k

Export...

Top Incoming Malware Threat Files

Trend: Incoming Malware Threat Files

Incoming Malware Threat Files

Items Displayed 100

Malware Threat File SHA256	Filename	Threat Name	File Type	Total Infected Files
3dfb3398...42cbe9be	accat83_420742.exe_8tt	W32.3DFB339862-95.SBX.TG	application/x-dosexec	48
14d76391...1aa5b0da	OfferInstaller_dotnet2.exe_O1b	W32.Trojan.NM	application/x-dosexec	48
6eaebc47...d5a9c685	FromDocToPDFAuto.exe_0_4rG, FromDocToPDFAuto.exe_0_6ZC, From...	W32.6EAEBC479A-95.SBX.TG	application/x-dosexec	624
b1cb0441...78a5c22f	15.exe_iFG, 15.exe_qIa	W32.B1CB04416C-100.SBX.TG	application/x-dosexec	96
29a422e0...9bccdae0	No_nameAsCgOXWW_bUQ	W32.29A422E042-100.SBX.TG	application/x-dosexec	48

AMP Summary, Numbers by Disposition

Top Malicious Files, click on SHA-256 value to get more information for the file

List of files (hashes) that were blocked by AMP, click on SHA-256 value to get more information for the file. Threat name tells us a lot....

Cisco AMP “Threat Name”

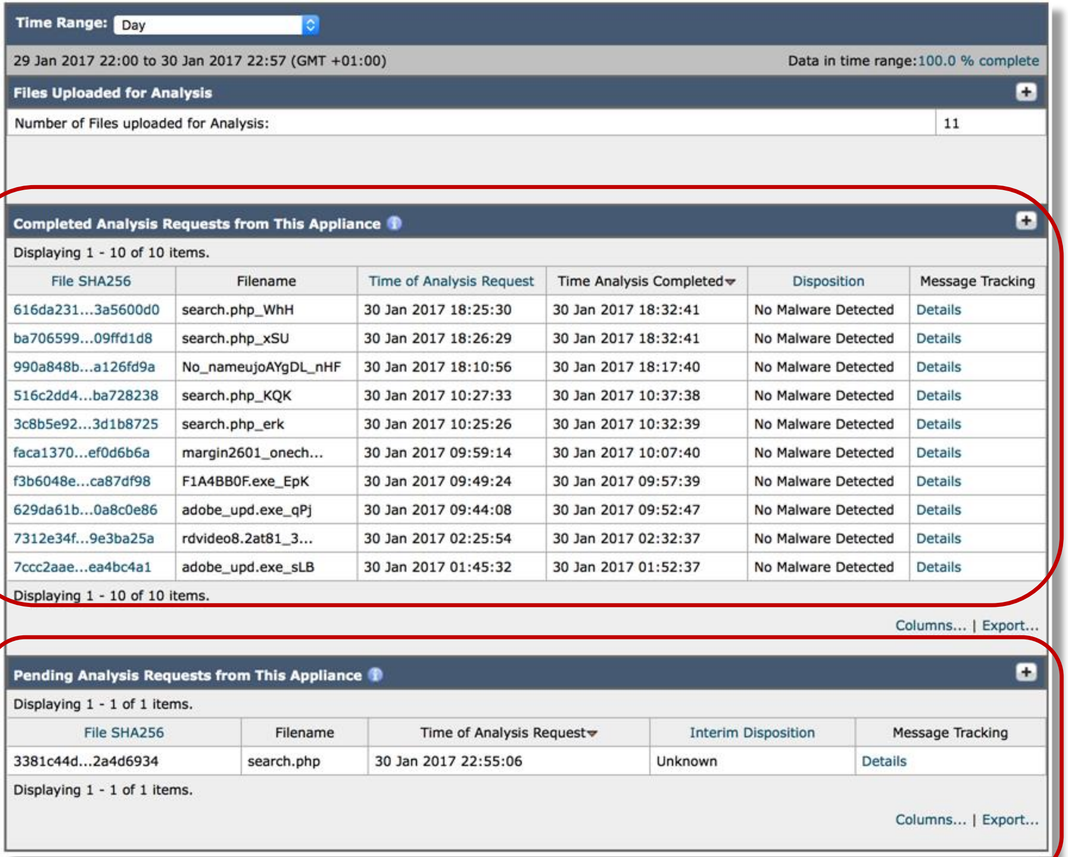
For Your Reference

- Also called “Spyname” or “Malware Name”
- It is only visible in AMP Integrations (ESA/WSA/Firepower)
- It gives an indication about where the actual malicious disposition came from, i.e.:
    - ClamAV Heuristic Rules, Threat Grid sandbox
    - Third Party comparison engine
    - Analysis engines written by the Talos Team
    - And many more …
- Detailed descriptions posted here: https://www.talosintelligence.com/amp-naming/

AMP Event Analysis

AMP File Analysis Events

- Reporting > AMP File Analysis



Time Range: Day

29 Jan 2017 22:00 to 30 Jan 2017 22:57 (GMT +01:00) Data in time range: 100.0 % complete

Files Uploaded for Analysis

Number of Files uploaded for Analysis:	11

Completed Analysis Requests from This Appliance

Displaying 1 - 10 of 10 items.

File SHA256	Filename	Time of Analysis Request	Time Analysis Completed	Disposition	Message Tracking
616da231...3a5600d0	search.php_WhH	30 Jan 2017 18:25:30	30 Jan 2017 18:32:41	No Malware Detected	Details
ba706599...09ffd1d8	search.php_xSU	30 Jan 2017 18:26:29	30 Jan 2017 18:32:41	No Malware Detected	Details
990a848b...a126fd9a	No_nameujoAYgDL_nHF	30 Jan 2017 18:10:56	30 Jan 2017 18:17:40	No Malware Detected	Details
516c2dd4...ba728238	search.php_KQK	30 Jan 2017 10:27:33	30 Jan 2017 10:37:38	No Malware Detected	Details
3c8b5e92...3d1b8725	search.php_erk	30 Jan 2017 10:25:26	30 Jan 2017 10:32:39	No Malware Detected	Details
faca1370...ef0d6b6a	margin2601_onech...	30 Jan 2017 09:59:14	30 Jan 2017 10:07:40	No Malware Detected	Details
f3b6048e...ca87df98	F1A4BB0F.exe_EpK	30 Jan 2017 09:49:24	30 Jan 2017 09:57:39	No Malware Detected	Details
629da61b...0a8c0e86	adobe_upd.exe_qPj	30 Jan 2017 09:44:08	30 Jan 2017 09:52:47	No Malware Detected	Details
7312e34f...9e3ba25a	rdvideo8.2at81_3...	30 Jan 2017 02:25:54	30 Jan 2017 02:32:37	No Malware Detected	Details
7ccc2aae...ea4bc4a1	adobe_upd.exe_sLB	30 Jan 2017 01:45:32	30 Jan 2017 01:52:37	No Malware Detected	Details

Displaying 1 - 10 of 10 items.

Columns... | Export...

Pending Analysis Requests from This Appliance

Displaying 1 - 1 of 1 items.

File SHA256	Filename	Time of Analysis Request	Interim Disposition	Message Tracking
3381c44d...2a4d6934	search.php	30 Jan 2017 22:55:06	Unknown	Details

Displaying 1 - 1 of 1 items.

Columns... | Export...

Completed File Analysis Requests

Currently Running File Analysis Requests

AMP Event Analysis

On-box File Analysis Details

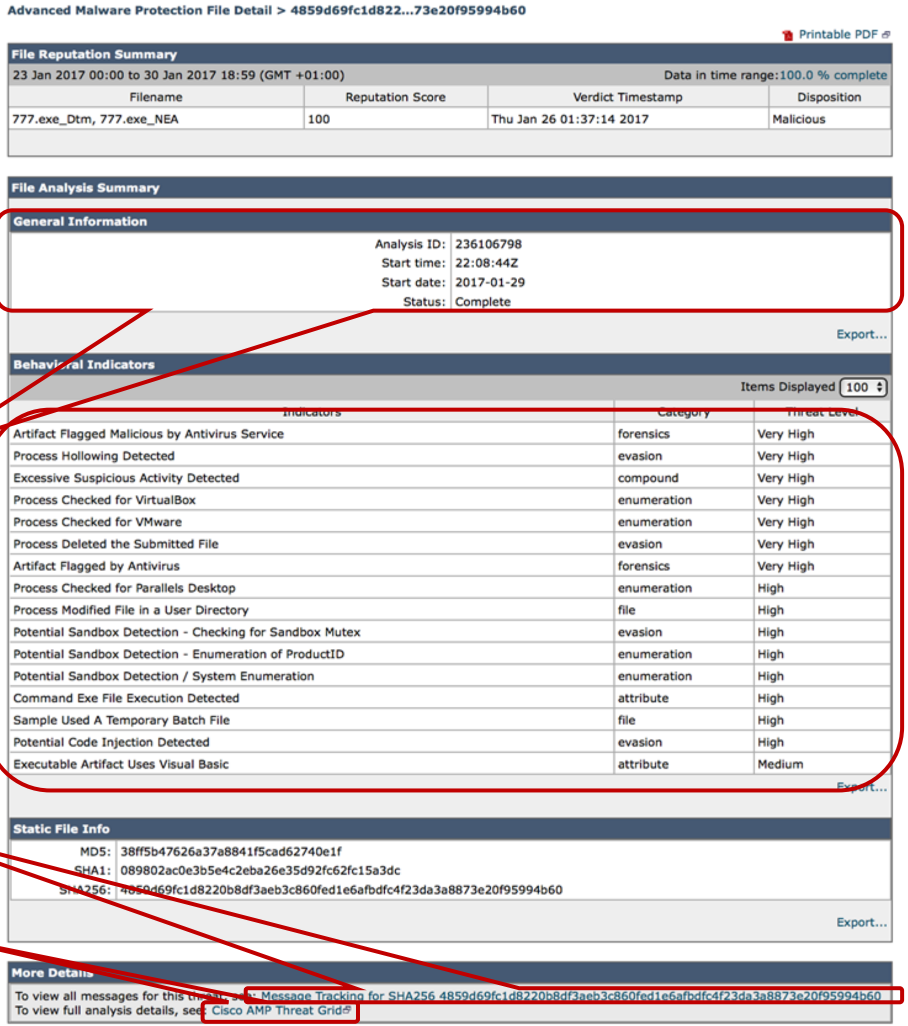
- Reporting > Advanced Malware Protection
  - Click on SHA256 to see summarized file analysis results from Threat Grid

File Analysis Date & Time

Behavioral Indicators discovered during dynamic File Analysis

Link to Message Tracking for this SHA256, a way to track delivery of message with this attachment

Link to detailed TG Report for this file



Advanced Malware Protection File Detail > 4859d69fc1d822...73e20f95994b60

Printable PDF

File Reputation Summary

23 Jan 2017 00:00 to 30 Jan 2017 18:59 (GMT +01:00) Data in time range:100.0 % complete

Filename	Reputation Score	Verdict Timestamp	Disposition
777.exe_Dtm, 777.exe_NEA	100	Thu Jan 26 01:37:14 2017	Malicious

File Analysis Summary

General Information

Analysis ID:	236106798
Start time:	22:08:44Z
Start date:	2017-01-29
Status:	Complete

Export...

Behavioral Indicators

Items Displayed 100

Indicators	Category	Threat Level
Artifact Flagged Malicious by Antivirus Service	forensics	Very High
Process Hollowing Detected	evasion	Very High
Excessive Suspicious Activity Detected	compound	Very High
Process Checked for VirtualBox	enumeration	Very High
Process Checked for VMware	enumeration	Very High
Process Deleted the Submitted File	evasion	Very High
Artifact Flagged by Antivirus	forensics	Very High
Process Checked for Parallels Desktop	enumeration	High
Process Modified File in a User Directory	file	High
Potential Sandbox Detection - Checking for Sandbox Mutex	evasion	High
Potential Sandbox Detection - Enumeration of ProductID	enumeration	High
Potential Sandbox Detection / System Enumeration	enumeration	High
Command Exe File Execution Detected	attribute	High
Sample Used A Temporary Batch File	file	High
Potential Code Injection Detected	evasion	High
Executable Artifact Uses Visual Basic	attribute	Medium

Export...

Static File Info

MD5:	38ff5b47626a37a8841f5cad62740e1f
SHA1:	089802ac0e3b5e4c2eba26e35d92fc62fc15a3dc
SHA256:	4859d69fc1d8220b8df3aeb3c860fed1e6afbdfc4f23da3a8873e20f95994b60

Export...

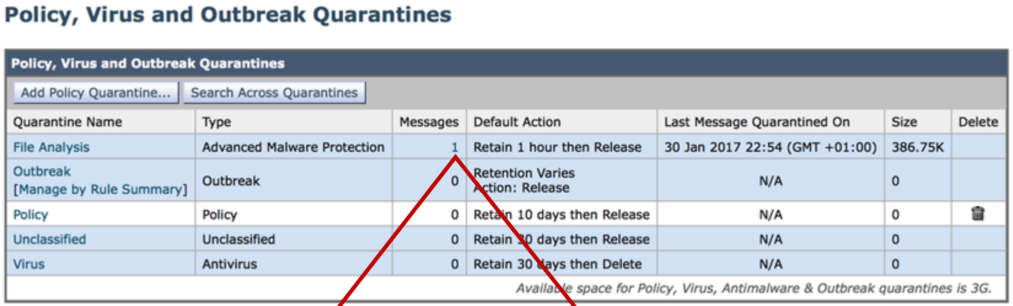
More Details

To view all messages for this threat, see: Message Tracking for SHA256 4859d69fc1d8220b8df3aeb3c860fed1e6afbdfc4f23da3a8873e20f95994b60
To view full analysis details, see: Cisco AMP Threat Grid

AMP Event Analysis

File Analysis Quarantine

- Monitoring -> Policy, Virus and Outbreak Quarantines
  - Click on Messages column to see all messages currently in File Analysis Quarantine

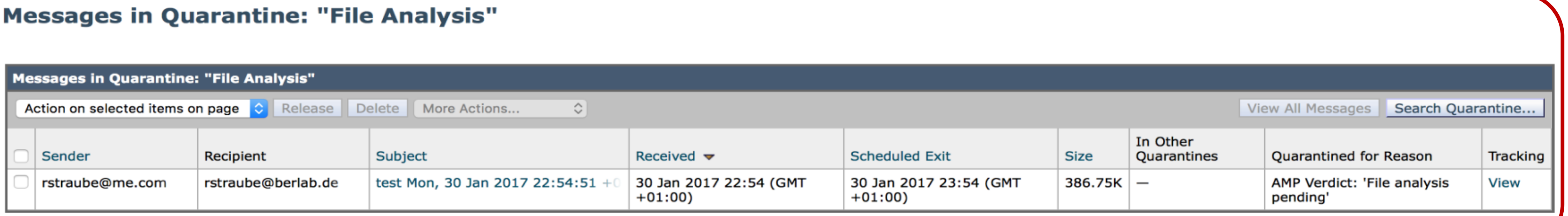


Policy, Virus and Outbreak Quarantines

Policy, Virus and Outbreak Quarantines

Quarantine Name	Type	Messages	Default Action	Last Message Quarantined On	Size	Delete
File Analysis	Advanced Malware Protection	1	Retain 1 hour then Release	30 Jan 2017 22:54 (GMT +01:00)	386.75K	
Outbreak [Manage by Rule Summary]	Outbreak	0	Retention Varies Action: Release	N/A	0	
Policy	Policy	0	Retain 10 days then Release	N/A	0	🗑
Unclassified	Unclassified	0	Retain 30 days then Release	N/A	0	
Virus	Antivirus	0	Retain 30 days then Delete	N/A	0	

Available space for Policy, Virus, Antimalware & Outbreak quarantines is 3G.



Messages in Quarantine: "File Analysis"

Messages in Quarantine: "File Analysis"

□	Sender	Recipient	Subject	Received ▼	Scheduled Exit	Size	In Other Quarantines	Quarantined for Reason	Tracking
□	rstraube@me.com	rstraube@berlab.de	test Mon, 30 Jan 2017 22:54:51 +0	30 Jan 2017 22:54 (GMT +01:00)	30 Jan 2017 23:54 (GMT +01:00)	386.75K	—	AMP Verdict: 'File analysis pending'	View

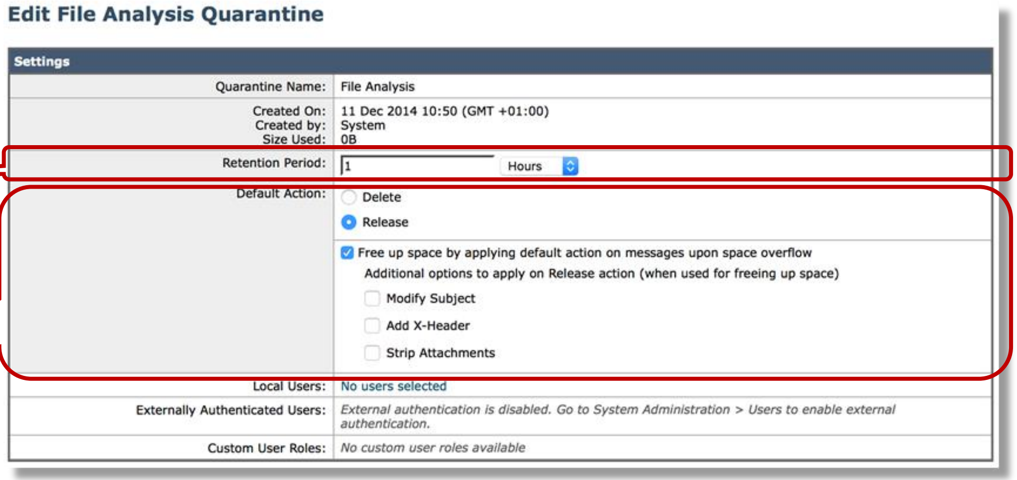
AMP Event Analysis

AMP File Analysis Quarantine Settings

- Monitoring -> Policy, Virus and Outbreak Quarantines
  - Click on File Analysis to open the Quarantine Settings

Quarantine Retention Time: Max time for keeping messages in quaratine – safety net

Action to take if retention period expires, default releases and further processes the message



Edit File Analysis Quarantine

Settings	
Quarantine Name:	File Analysis
Created On: Created by: Size Used:	11 Dec 2014 10:50 (GMT +01:00) System 0B
Retention Period:	1 Hours
Default Action:	○ Delete ● Release ☑ Free up space by applying default action on messages upon space overflow Additional options to apply on Release action (when used for freeing up space) □ Modify Subject □ Add X-Header □ Strip Attachments
Local Users:	No users selected
Externally Authenticated Users:	*External authentication is disabled. Go to System Administration > Users to enable external authentication.*
Custom User Roles:	*No custom user roles available*

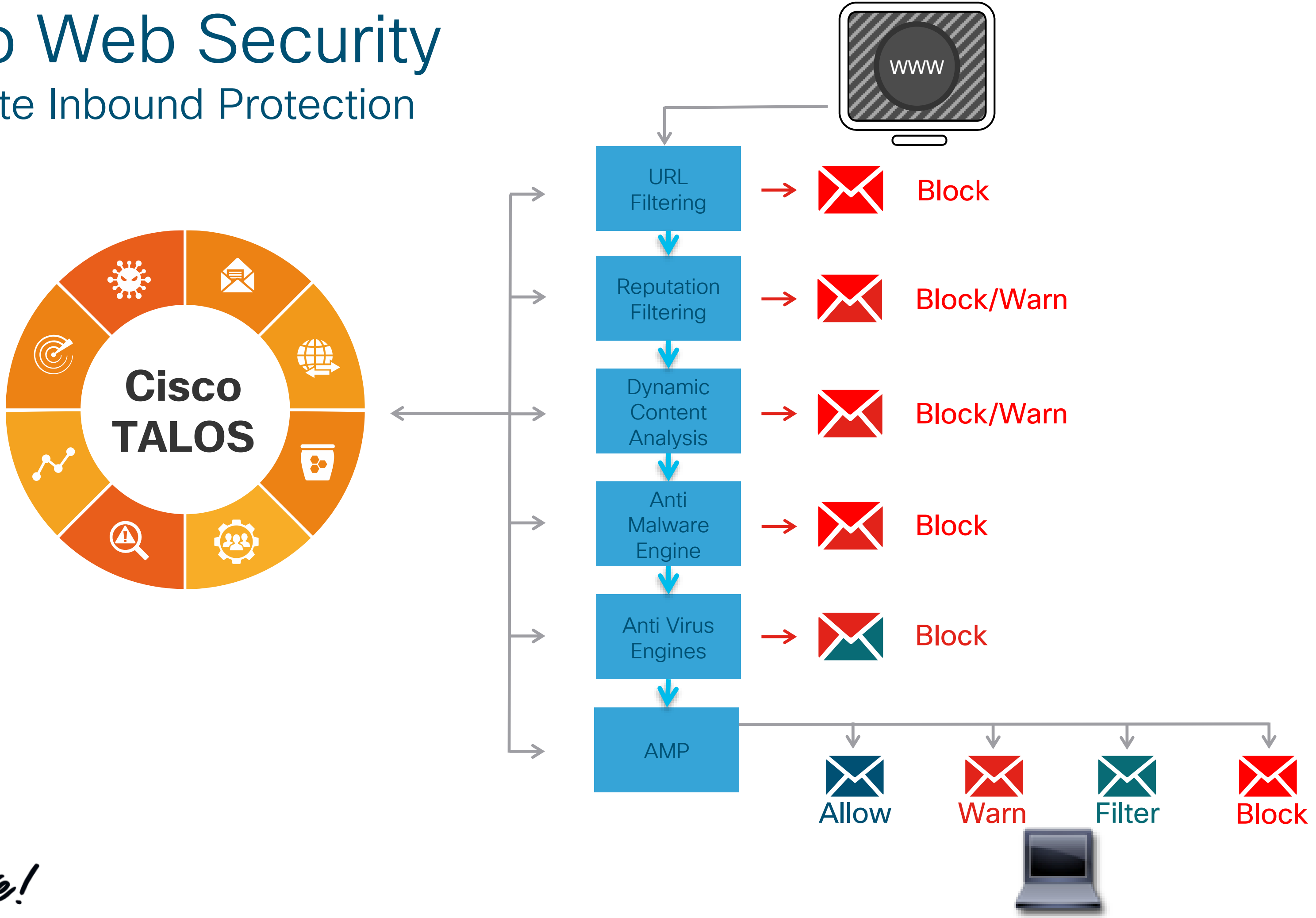
Cisco AMP and Threat Grid for Web Security (WSA)

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

- How the does the WSA security stack protect my company?
- Where does AMP fit in, and what happens when?
- How do I configure all this so it works?

Cisco Web Security

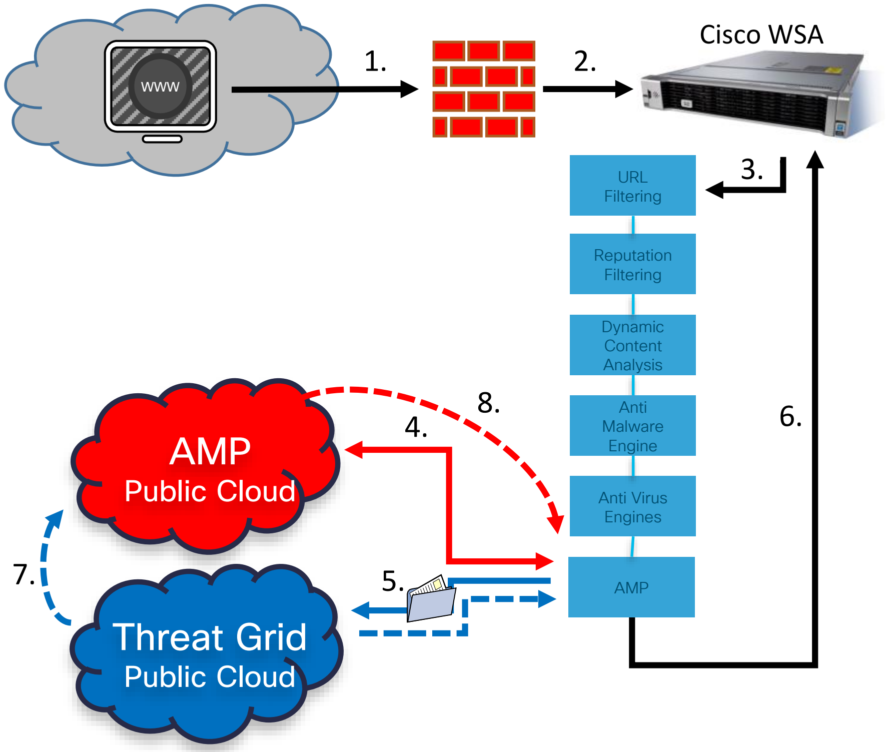
Complete Inbound Protection



cisco Live!

WSA – AMP & Threat Grid Process Flow

Threat Grid in the Cloud



1. Web page content from Internet
2. Directed through WSA Appliance
3. Content passed through security stack on WSA
4. Threat intelligence from AMP Cloud used to determine if page object matches malicious indicators (File Reputation - SHA Lookup)
5. If object is “unknown” and qualifies, it is sent to Threat Grid cloud for analysis
6. WSA **does not wait** for results from TG and allows object to be delivered
7. If Threat Grid malware analysis determines that it has serious malicious behaviors and indicators, the AMP Cloud is updated
8. Update leads to a Retrospective Event

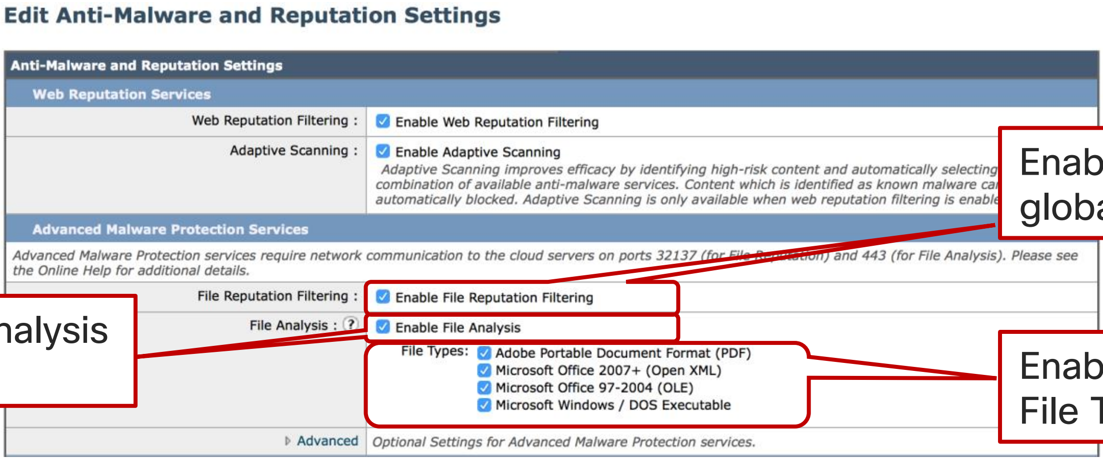
AMP on WSA – File Types & Pre-Classification

- Number of supported file types has been enhanced with WSA version v11.7. File Types are now on par with Threat Grid Cloud.
- Before an unknown file is submitted the on-box pre-classification engine [ClamAV] scans it to select only files with active or suspicious content
  - Pre-classification signatures
  - Byte code rules that uncover suspicious indicators
  - Signatures developed and updated by Talos – updated via cloud regularly
- Additional Threat Grid classification occurs on v11.7+ on WSA
  - Saves on Threat Grid dynamic analysis
- Highly recommend v11.8.0-407 or newer

Configuring AMP for WSA

Enable AMP Services

- Security Services > Anti-Malware and Reputation Settings
- You can choose whether to enable or disable two services:
  - File Reputation (SHA-256)
  - File Analysis (Threat Grid)



Edit Anti-Malware and Reputation Settings

Anti-Malware and Reputation Settings

Web Reputation Services

Web Reputation Filtering : ☑ Enable Web Reputation Filtering

Adaptive Scanning : ☑ Enable Adaptive Scanning

Adaptive Scanning improves efficacy by identifying high-risk content and automatically selecting combination of available anti-malware services. Content which is identified as known malware ca automatically blocked. Adaptive Scanning is only available when web reputation filtering is enable

Advanced Malware Protection Services

Advanced Malware Protection services require network communication to the cloud servers on ports 32137 (for File Reputation) and 443 (for File Analysis). Please see the Online Help for additional details.

File Reputation Filtering : ☑ Enable File Reputation Filtering

File Analysis : ? ☑ Enable File Analysis

File Types:
☑ Adobe Portable Document Format (PDF)
☑ Microsoft Office 2007+ (Open XML)
☑ Microsoft Office 97-2004 (OLE)
☑ Microsoft Windows / DOS Executable

▷ Advanced — *Optional Settings for Advanced Malware Protection services.*

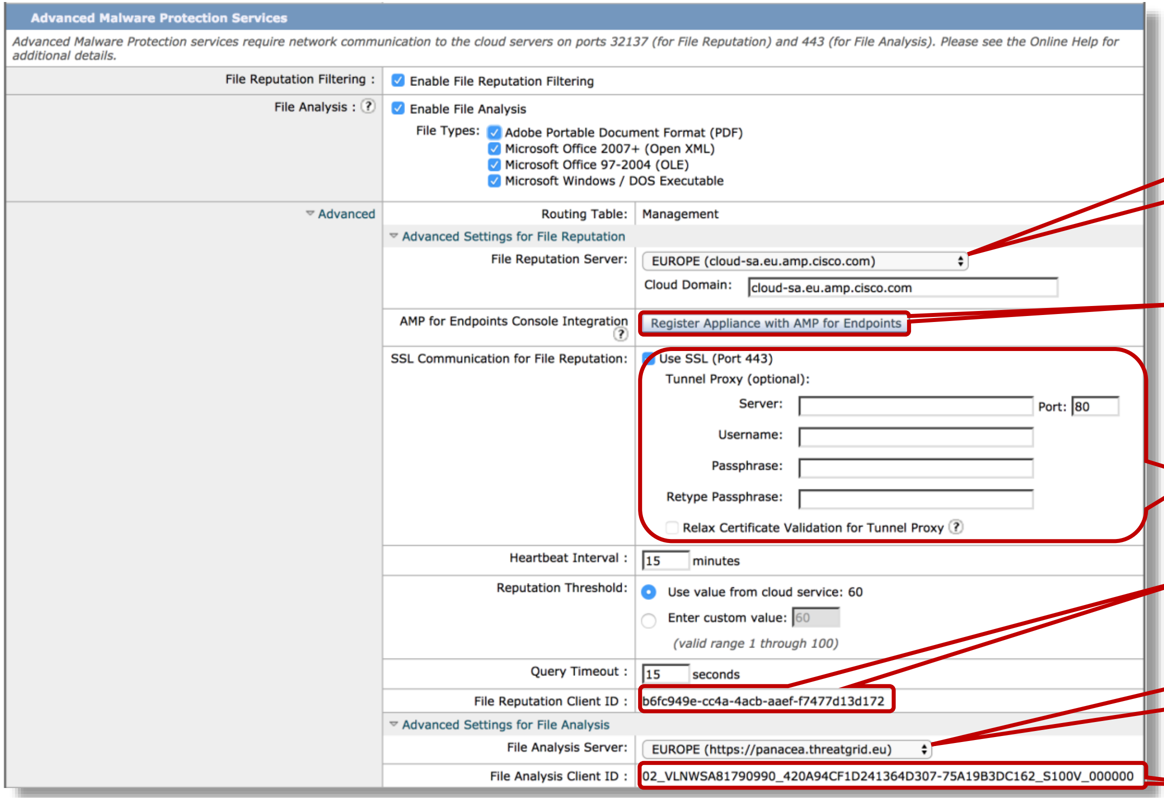
Enables File Reputation globally

Enables File Analysis globally

Enables specific File Types globally

Configuring AMP for WSA

AMP Services Advanced Settings



Advanced Malware Protection Services

Advanced Malware Protection services require network communication to the cloud servers on ports 32137 (for File Reputation) and 443 (for File Analysis). Please see the Online Help for additional details.

File Reputation Filtering :	☑ Enable File Reputation Filtering
File Analysis : ?	☑ Enable File Analysis File Types: ☑ Adobe Portable Document Format (PDF) ☑ Microsoft Office 2007+ (Open XML) ☑ Microsoft Office 97-2004 (OLE) ☑ Microsoft Windows / DOS Executable
Advanced	Routing Table: Management

Advanced Settings for File Reputation

File Reputation Server:	EUROPE (cloud-sa.eu.amp.cisco.com)
Cloud Domain:	cloud-sa.eu.amp.cisco.com
AMP for Endpoints Console Integration ?	Register Appliance with AMP for Endpoints
SSL Communication for File Reputation:	☑ Use SSL (Port 443) Tunnel Proxy (optional): Server: Port: 80 Username: Passphrase: Retype Passphrase: □ Relax Certificate Validation for Tunnel Proxy ?
Heartbeat Interval :	15 minutes
Reputation Threshold:	● Use value from cloud service: 60 ○ Enter custom value: 60 *(valid range 1 through 100)*
Query Timeout :	15 seconds
File Reputation Client ID :	b6fc949e-cc4a-4acb-aaef-f7477d13d172

Advanced Settings for File Analysis

File Analysis Server:	EUROPE (https://panacea.threatgrid.eu)
File Analysis Client ID :	02_VLNWSA81790990_420A94CF1D241364D307-75A19B3DC162_S100V_000000

AMERICAS (cloud-sa.amp.cisco.com)
AMERICAS(Legacy) (cloud-sa.amp.sourcefire.com)
✓ EUROPE (cloud-sa.eu.amp.cisco.com)
Private Cloud

Select Data Center and register WSA in your AMP for Endpoints Console, more details in a sec ...

Configure Upstream Proxy for File Reputation checks

AMP Client ID

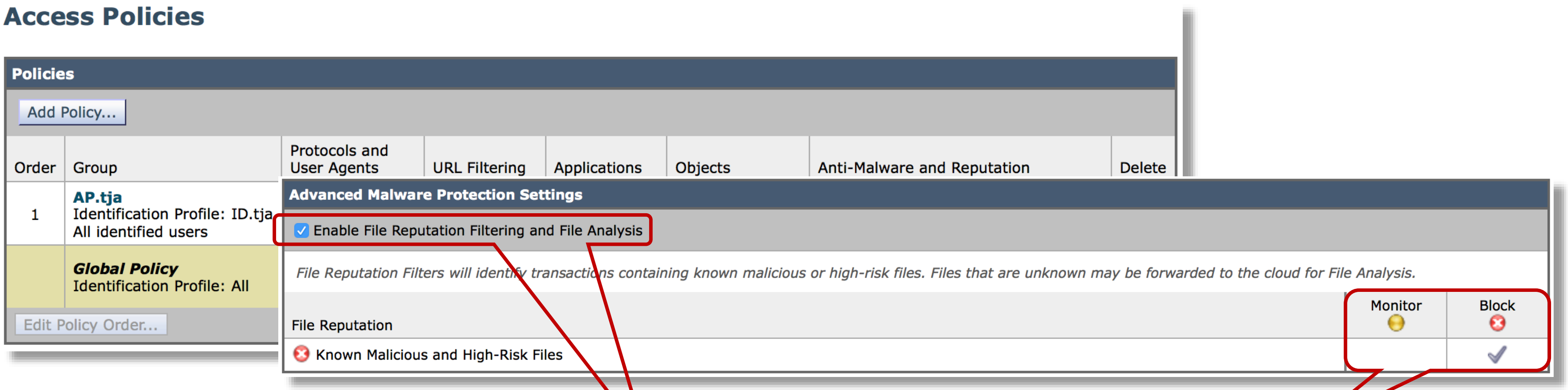
AMERICAS (https://panacea.threatgrid.com)
✓ EUROPE (https://panacea.threatgrid.eu)
Private Cloud

File Analysis Client ID

Configuring AMP for WSA

Access Policy

- Web Security Manager > Access Policies
- Click on the link to change AMP-related policy settings



Access Policies

Policies

Add Policy...

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	Delete
1	**AP.tja** Identification Profile: ID.tja All identified users						
	Global Policy Identification Profile: All						

Edit Policy Order...

Advanced Malware Protection Settings

☑ Enable File Reputation Filtering and File Analysis

File Reputation Filters will identify transactions containing known malicious or high-risk files. Files that are unknown may be forwarded to the cloud for File Analysis.

File Reputation	Monitor ●	Block ☒
☒ Known Malicious and High-Risk Files		✓

Turns on File Reputation for traffic matching this Access Policy

Select the action to take for malicious objects

Cisco AMP and Threat Grid for Endpoint Security

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

- What additional protection engines are available in AMP for Endpoints?
- How does AMP for Endpoint traffic flow?
- How is AMP for Endpoints different from everything we have been talking about?
- What is Low Prevelance?

AMP for Endpoints

Multiple Prevention, Detection and Monitoring Features

Prevent

- **Cloud lookups** (1:1, 1:many)
- **Antivirus** (TETRA, ClamAV)
- **Exploit Prevention**:
  - Fileless malware detection
  - Adware Removal
  - Process Hollowing
- **System Process Protection**
- **Client Indicators of Compromise**

Detect

- **Static analysis**
- **Sandboxing** (Dynamic analysis)
- **Malicious Activity Protection**
- **Machine Learning**
- **Device Flow Correlation**
- **Cloud Indicators of Compromise**

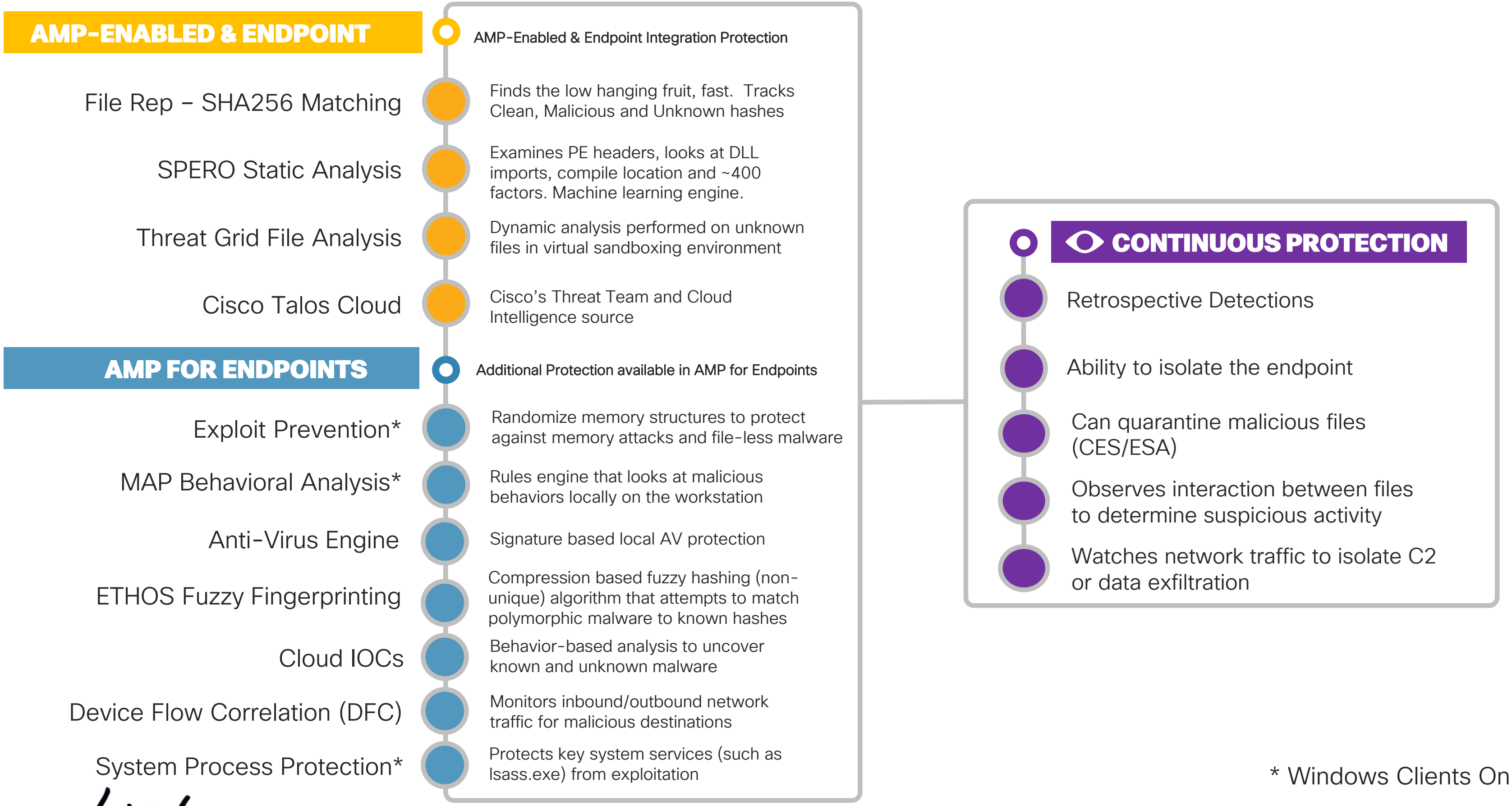
Reduce Risk

- **Vulnerable Software**
- **Low Prevalence**
- **Proxy Log Analysis** (Cognitive)
- **Endpoint Isolation** New!
- **Advanced Search** (Orbital) New!
- **API Integrations**

cisco Live!

For Your Reference

How does AMP protect our systems?



AMP-ENABLED & ENDPOINT	AMP-Enabled & Endpoint Integration Protection
File Rep – SHA256 Matching	Finds the low hanging fruit, fast. Tracks Clean, Malicious and Unknown hashes
SPERO Static Analysis	Examines PE headers, looks at DLL imports, compile location and ~400 factors. Machine learning engine.
Threat Grid File Analysis	Dynamic analysis performed on unknown files in virtual sandboxing environment
Cisco Talos Cloud	Cisco's Threat Team and Cloud Intelligence source
AMP FOR ENDPOINTS	Additional Protection available in AMP for Endpoints
Exploit Prevention*	Randomize memory structures to protect against memory attacks and file-less malware
MAP Behavioral Analysis*	Rules engine that looks at malicious behaviors locally on the workstation
Anti-Virus Engine	Signature based local AV protection
ETHOS Fuzzy Fingerprinting	Compression based fuzzy hashing (non-unique) algorithm that attempts to match polymorphic malware to known hashes
Cloud IOCs	Behavior-based analysis to uncover known and unknown malware
Device Flow Correlation (DFC)	Monitors inbound/outbound network traffic for malicious destinations
System Process Protection*	Protects key system services (such as lsass.exe) from exploitation

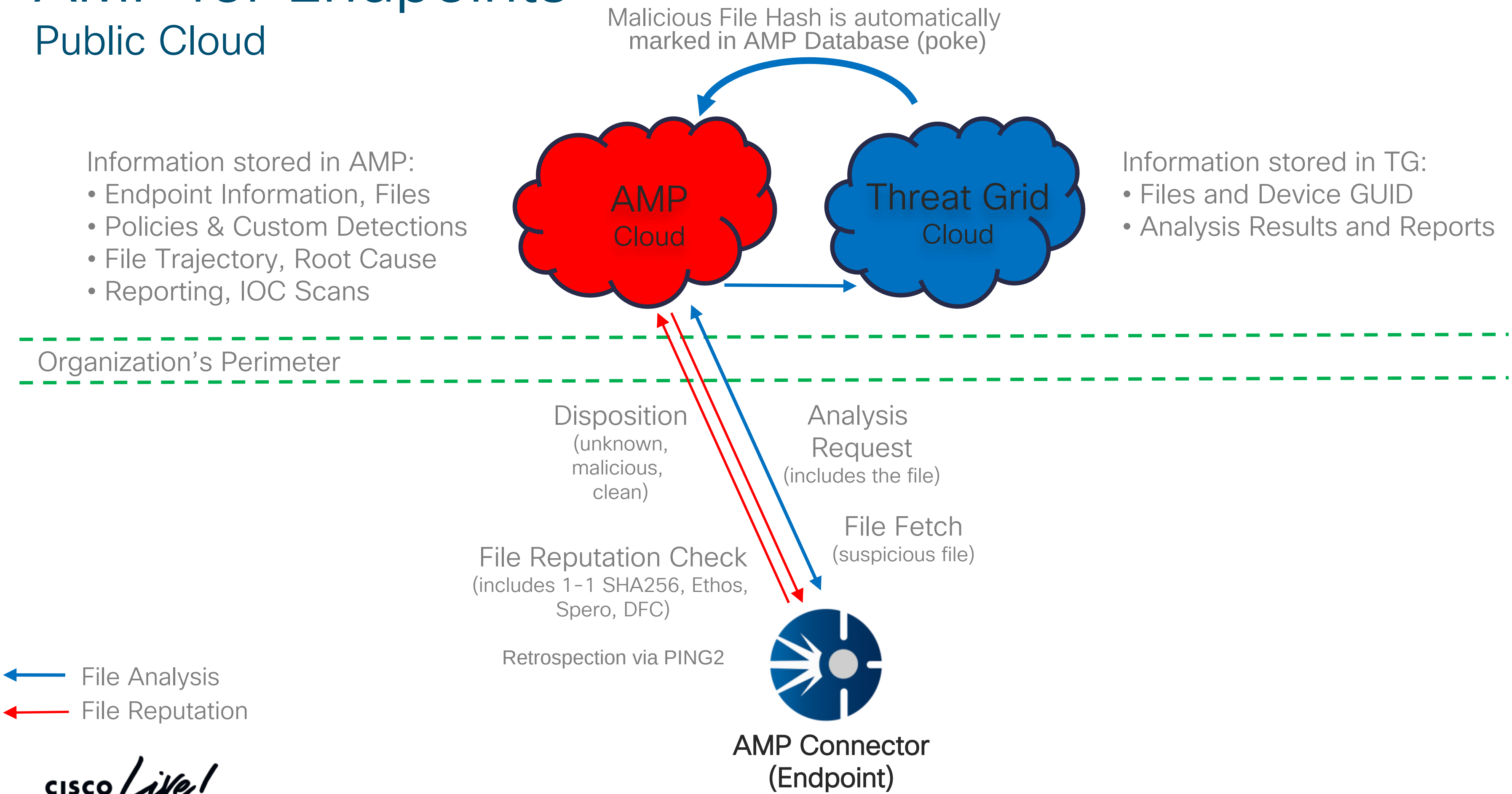
CONTINUOUS PROTECTION

- Retrospective Detections
- Ability to isolate the endpoint
- Can quarantine malicious files (CES/ESA)
- Observes interaction between files to determine suspicious activity
- Watches network traffic to isolate C2 or data exfiltration

* Windows Clients Only

AMP for Endpoints

Public Cloud



Malicious File Hash is automatically marked in AMP Database (poke)

Information stored in AMP:
- Endpoint Information, Files
- Policies & Custom Detections
- File Trajectory, Root Cause
- Reporting, IOC Scans

AMP Cloud

Threat Grid Cloud

Information stored in TG:
- Files and Device GUID
- Analysis Results and Reports

Organization’s Perimeter

Disposition (unknown, malicious, clean)

Analysis Request (includes the file)

File Fetch (suspicious file)

File Reputation Check (includes 1-1 SHA256, Ethos, Spero, DFC)

Retrospection via PING2

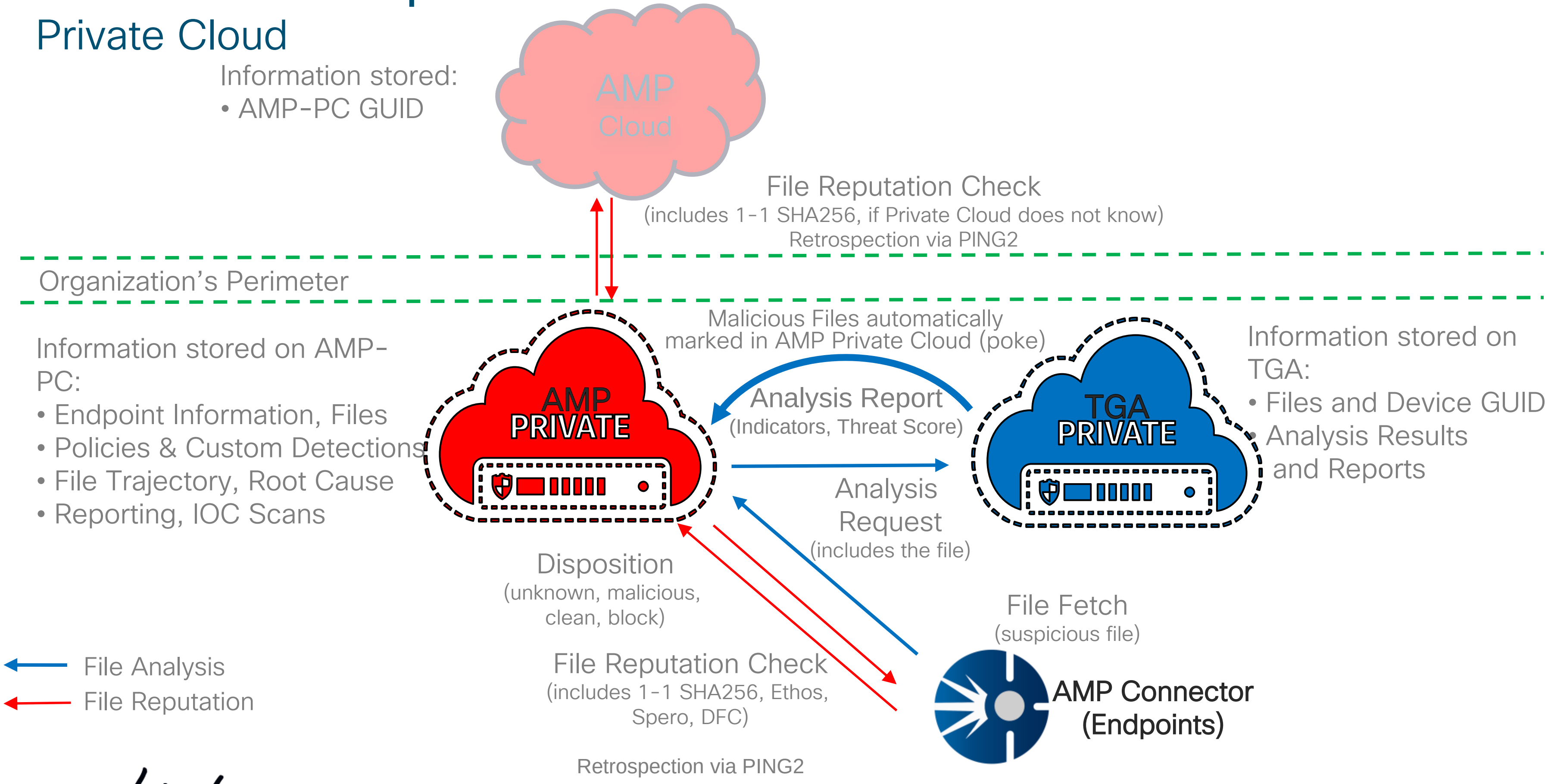
AMP Connector (Endpoint)

File Analysis

File Reputation

AMP for Endpoints

Private Cloud



Information stored:
- AMP-PC GUID

File Reputation Check
(includes 1-1 SHA256, if Private Cloud does not know)
Retrospection via PING2

Organization’s Perimeter

Information stored on AMP-PC:
- Endpoint Information, Files
- Policies & Custom Detections
- File Trajectory, Root Cause
- Reporting, IOC Scans

Malicious Files automatically marked in AMP Private Cloud (poke)

Analysis Report
(Indicators, Threat Score)

Analysis Request
(includes the file)

Information stored on TGA:
- Files and Device GUID
- Analysis Results and Reports

Disposition
(unknown, malicious, clean, block)

File Fetch
(suspicious file)

File Reputation Check
(includes 1-1 SHA256, Ethos, Spero, DFC)

Retrospection via PING2

AMP Connector (Endpoints)

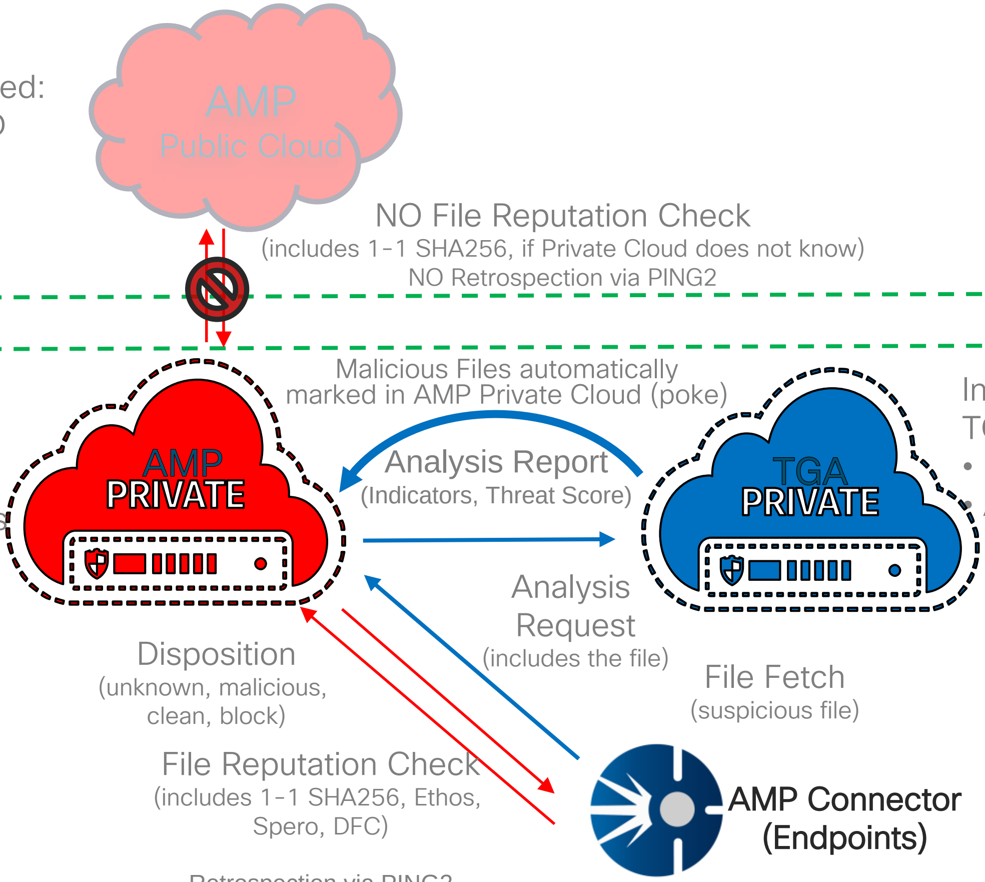
File Analysis

File Reputation

AMP for Endpoints

Private / Air-Gap

Information stored:
- AMP-PC GUID



NO File Reputation Check
(includes 1-1 SHA256, if Private Cloud does not know)
NO Retrospection via PING2

Organization’s Perimeter

Malicious Files automatically marked in AMP Private Cloud (poke)

Analysis Report
(Indicators, Threat Score)

Analysis Request
(includes the file)

File Fetch
(suspicious file)

Disposition
(unknown, malicious, clean, block)

File Reputation Check
(includes 1-1 SHA256, Ethos, Spero, DFC)

Retrospection via PING2

Information stored on AMP-PC:
- Endpoint Information, Files
- Policies & Custom Detections
- File Trajectory, Root Cause
- Reporting, IOC Scans

Information stored on TGA:
- Files and Device GUID
- Analysis Results and Reports

← File Analysis

← File Reputation

AMP Deployments

Hybrid Deployments for Endpoints

Remember:
AMP for Endpoints does not support any hybrid deployment modes !!!

Threat Grid in AMP for Endpoints

Automatic submission differences

- The Threat Grid Integration into AMP for Endpoints focuses exclusively on executables, no other files are submitted for sandboxing **automatically**
- Low Prevalence – Process to select files to be submitted for File Analysis in Threat Grid automatically
  - Prevalence – How widely spread a file is on a global perspective; files get tagged by Low Prevalence if they are only seen on a very low number of Endpoints globally
  - Those Low Prevalence Executables will be automatically submitted to Threat Grid for analysis
- Additionally, an Administrator can also initiate File Analysis **manually**
  - AMP Console requests file from endpoint, endpoint receives request via heartbeat
  - Endpoint uploads file to AMP Console
  - AMP Console submits the file for analysis and presents results

AMP for Endpoints File Analysis

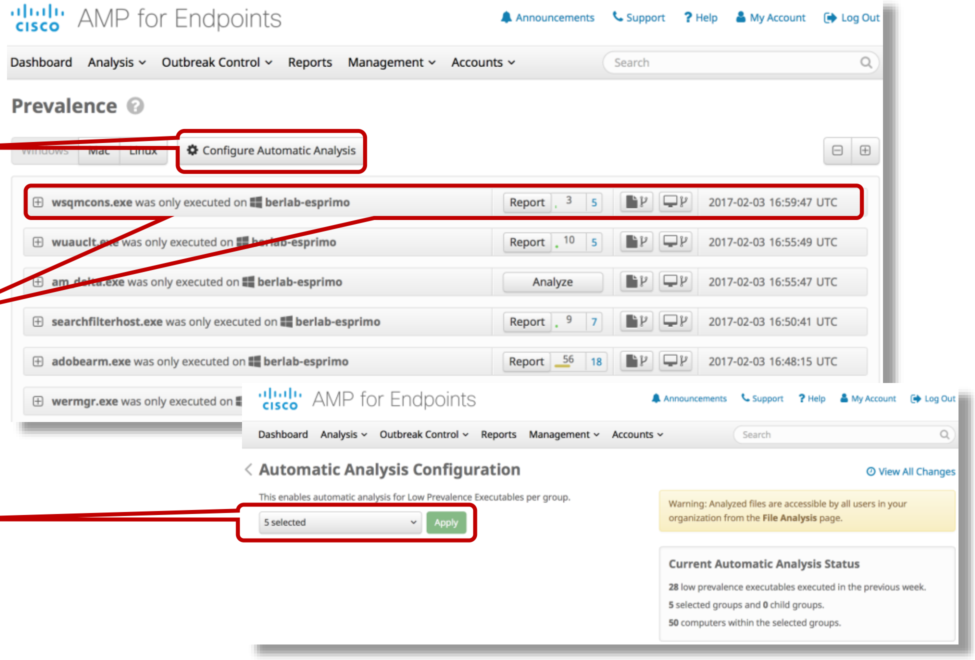
Automatic Sample Submissions with Low Prevalence Files

- Analysis -> Prevalence
- Configured per group basis
- Shows all Low Prevalence files

Enable/Disable/Configure Automatic File Analysis per group

File Information with number of ocurrences, Analysis Report, and links to File and Device Trajectories

Select/De-Select endpoint groups for Automatic File Analysis



Prevalence

wsqmcons.exe was only executed on berlab-esprimo | Report 3 5 | 2017-02-03 16:59:47 UTC

wuauclt.exe was only executed on berlab-esprimo | Report 10 5 | 2017-02-03 16:55:49 UTC

am_delta.exe was only executed on berlab-esprimo | Analyze | 2017-02-03 16:55:47 UTC

searchfilterhost.exe was only executed on berlab-esprimo | Report 9 7 | 2017-02-03 16:50:41 UTC

adobearm.exe was only executed on berlab-esprimo | Report 56 18 | 2017-02-03 16:48:15 UTC

wermgr.exe was only executed on

Automatic Analysis Configuration

View All Changes

This enables automatic analysis for Low Prevalence Executables per group.

5 selected | Apply

Warning: Analyzed files are accessible by all users in your organization from the **File Analysis** page.

Current Automatic Analysis Status

28 low prevalence executables executed in the previous week.

5 selected groups and **0** child groups.

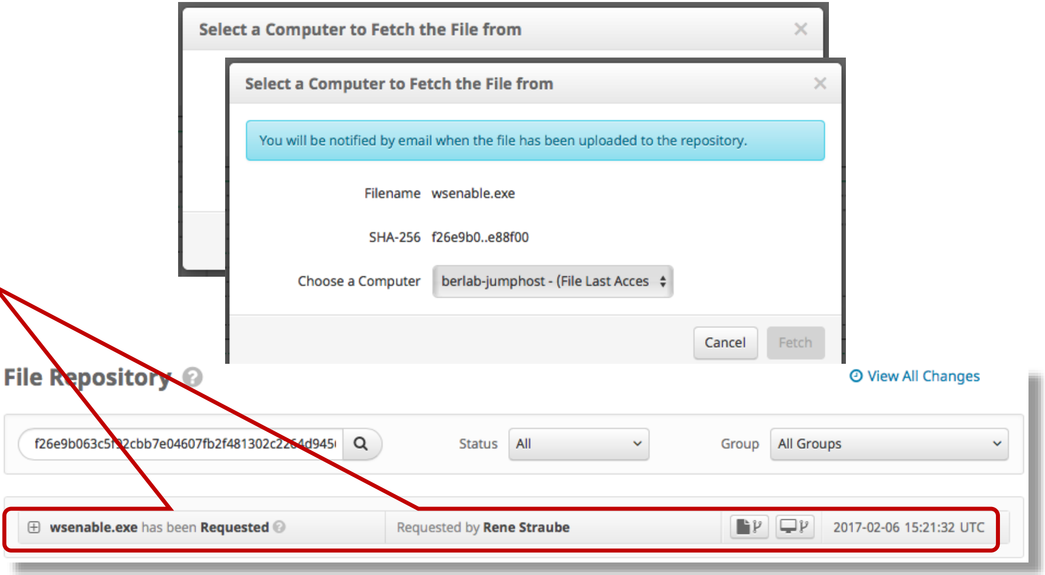
50 computers within the selected groups.

AMP for Endpoints File Analysis

Manual File Submissions

- Administrator selects File in File Trajectory to be fetched from an Endpoint

After file fetch is initiated, the file will show up in the file repository



Select a Computer to Fetch the File from

You will be notified by email when the file has been uploaded to the repository.

Filename wsenable.exe

SHA-256 f26e9b0..e88f00

Choose a Computer berlab-jumphost - (File Last Acces

f26e9b063c5f92cbb7e04607fb2f481302c2264d945

Status All

Group All Groups

wsenable.exe has been Requested | Requested by Rene Straube | 2017-02-06 15:21:32 UTC

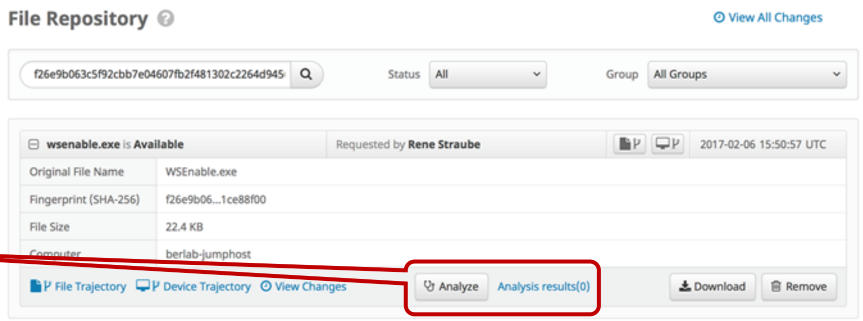
AMP for Endpoints File Analysis

Manual File Submissions

- After successful file fetch, the file will show up as “available”

File has not been analyzed, press the Analyze button to submit this file to Threat Grid

Threat Grid will analyze the file. If you have Threat Grid Cloud, you can interact with the sample during analysis and to view results after finishing in Threat Grid cloud, or the AMP Console



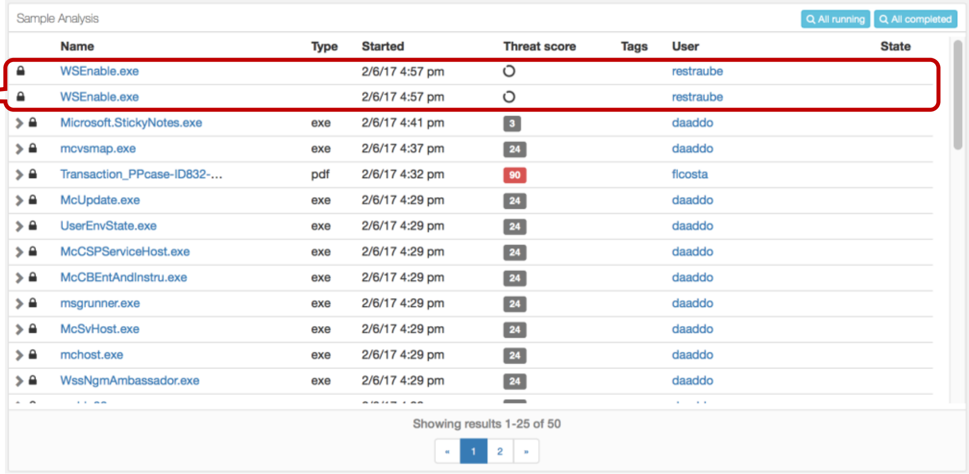
File Repository

View All Changes

f26e9b063c5f92cbb7e04607fb2f481302c2264d945 | Status: All | Group: All Groups

wsenable.exe is **Available** | Requested by **Rene Straube** | 2017-02-06 15:50:57 UTC

Original File Name	WSEnable.exe
Fingerprint (SHA-256)	f26e9b06...1ce88f00
File Size	22.4 KB
Computer	berlab-jumphost



Sample Analysis

Name	Type	Started	Threat score	Tags	User	State
WSEnable.exe		2/6/17 4:57 pm	○		restraube	
WSEnable.exe		2/6/17 4:57 pm	○		restraube	
Microsoft.StickyNotes.exe	exe	2/6/17 4:41 pm	3		daaddo	
mcvsmap.exe	exe	2/6/17 4:37 pm	24		daaddo	
Transaction_PPcase-ID832-...	pdf	2/6/17 4:32 pm	90		flcosta	
McUpdate.exe	exe	2/6/17 4:29 pm	24		daaddo	
UserEnvState.exe	exe	2/6/17 4:29 pm	24		daaddo	
McCSPServiceHost.exe	exe	2/6/17 4:29 pm	24		daaddo	
McCBEntAndInstru.exe	exe	2/6/17 4:29 pm	24		daaddo	
msgrunner.exe	exe	2/6/17 4:29 pm	24		daaddo	
McSvHost.exe	exe	2/6/17 4:29 pm	24		daaddo	
mchost.exe	exe	2/6/17 4:29 pm	24		daaddo	
WssNgmAmbassador.exe	exe	2/6/17 4:29 pm	24		daaddo	

Showing results 1-25 of 50

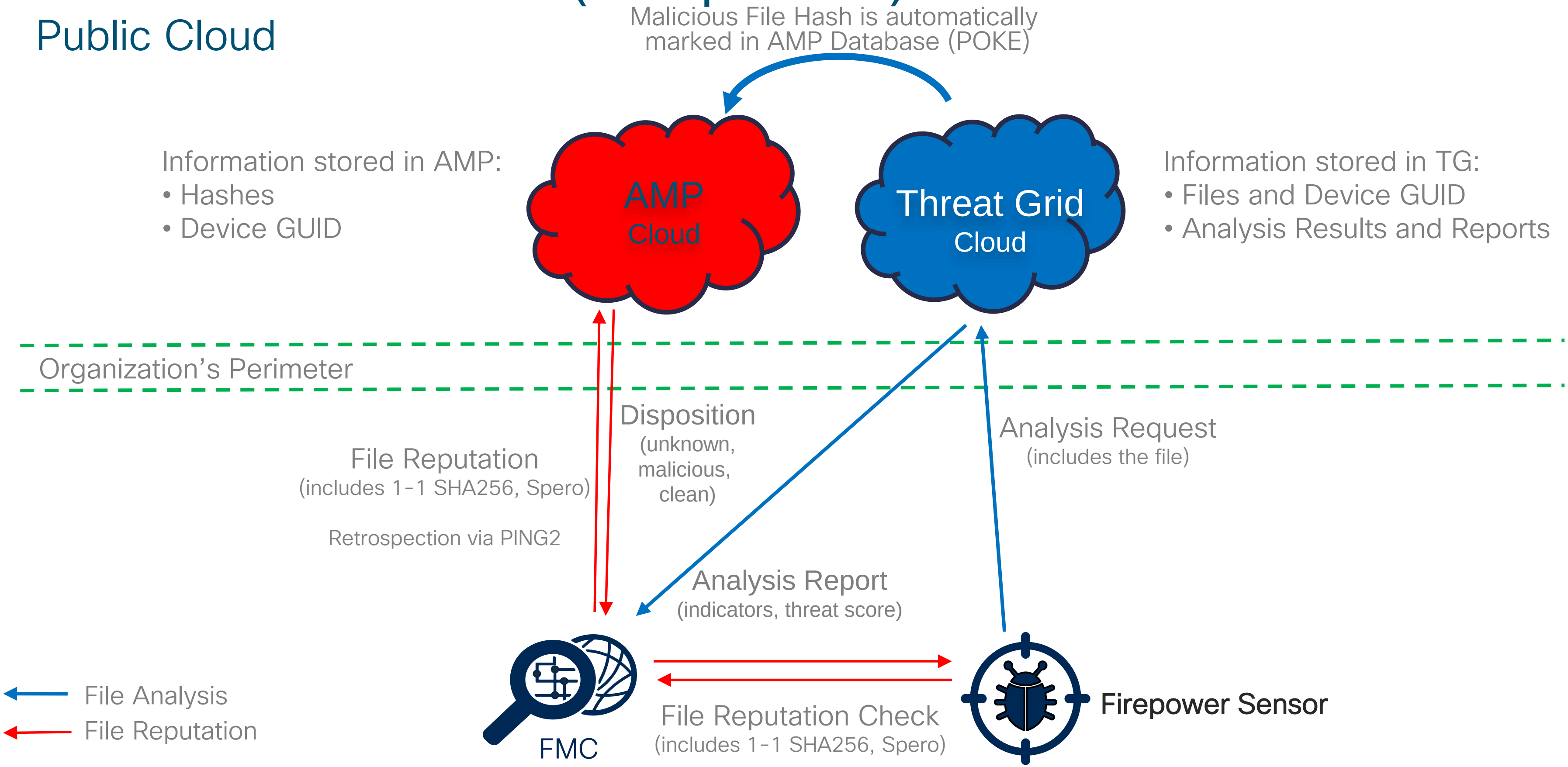
Cisco AMP and Threat Grid for Firepower

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

- More questions?!?
- How can I enable AMP on Firepower?

AMP for Network (Firepower)

Public Cloud



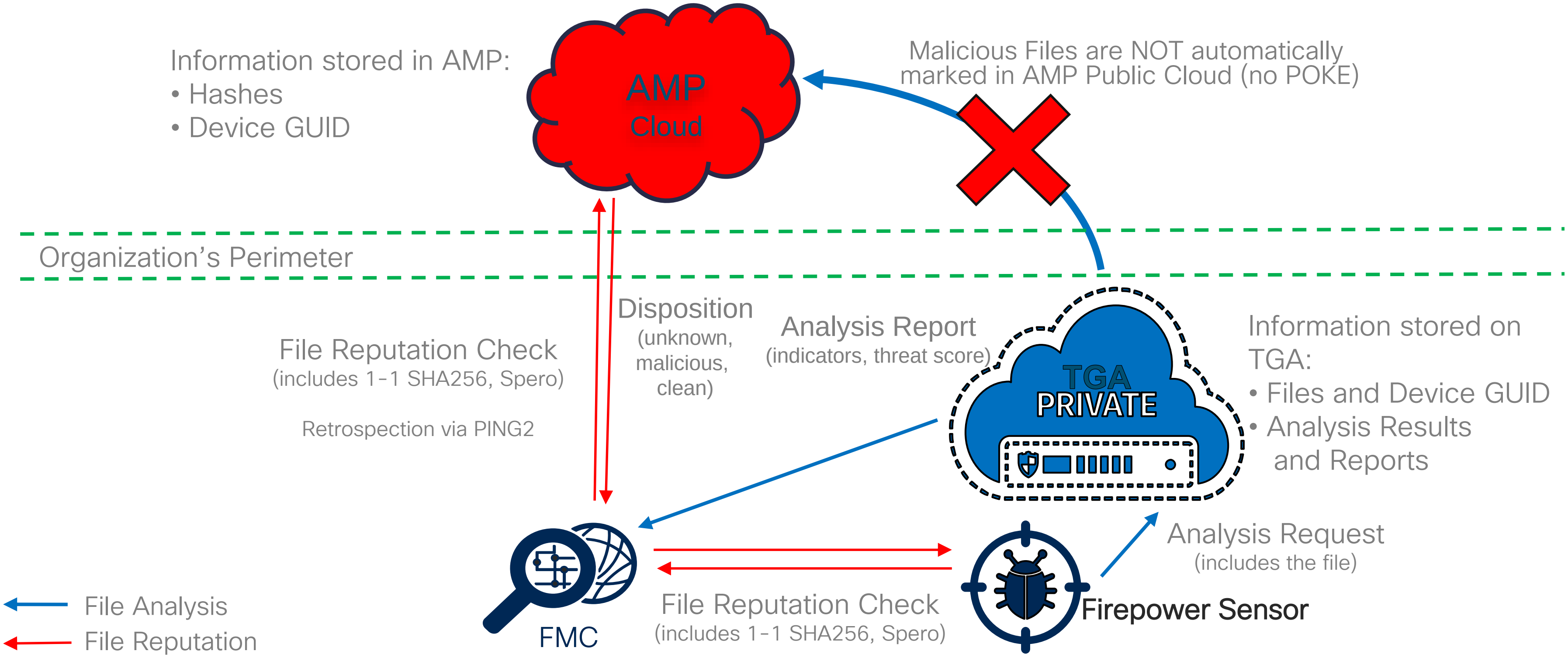
Malicious File Hash is automatically marked in AMP Database (POKE)

Information stored in AMP:
- Hashes
- Device GUID

Information stored in TG:
- Files and Device GUID
- Analysis Results and Reports

AMP for Networks (Firepower)

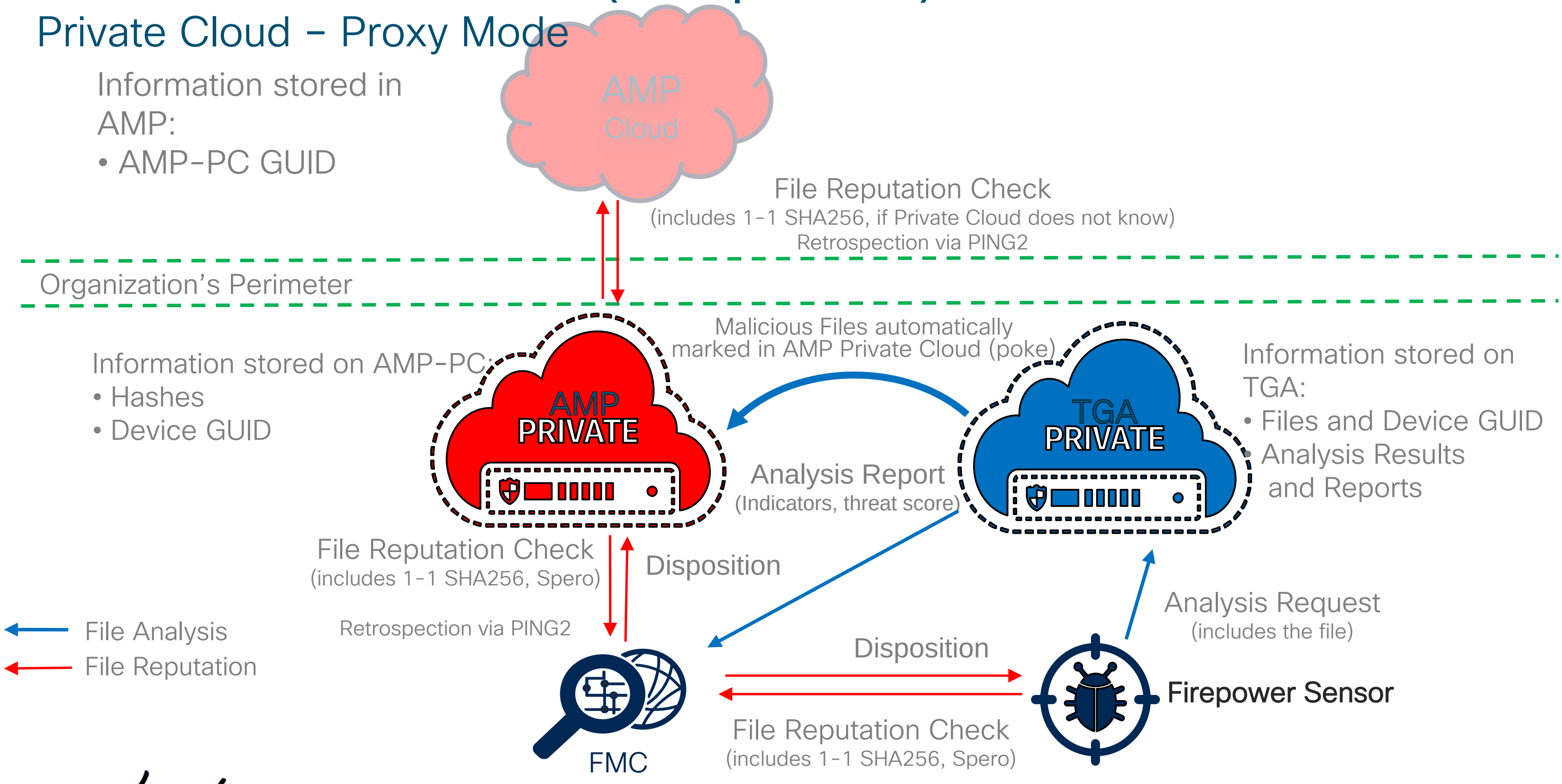
Hybrid Cloud



Information stored in AMP:
• Hashes
• Device GUID
AMP
Cloud
Malicious Files are NOT automatically marked in AMP Public Cloud (no POKE)
Organization's Perimeter
File Reputation Check
(includes 1-1 SHA256, Spero)
Retrospection via PING2
Disposition
(unknown, malicious, clean)
Analysis Report
(indicators, threat score)
TGA
PRIVATE
Information stored on TGA:
• Files and Device GUID
• Analysis Results and Reports
Analysis Request
(includes the file)
FMC
File Reputation Check
(includes 1-1 SHA256, Spero)
Firepower Sensor
File Analysis
File Reputation

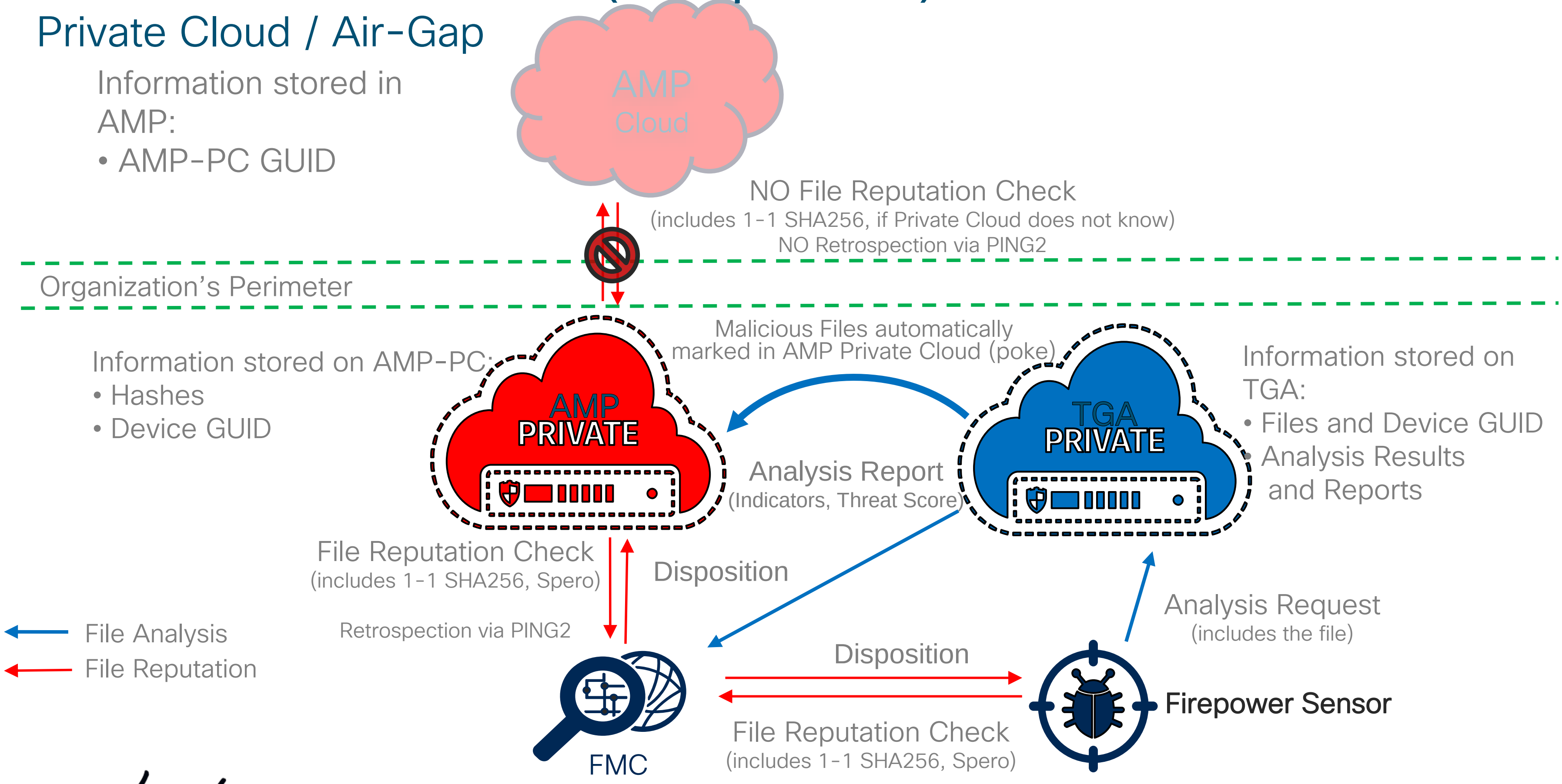
AMP for Networks (Firepower)

Private Cloud – Proxy Mode



AMP for Networks (Firepower)

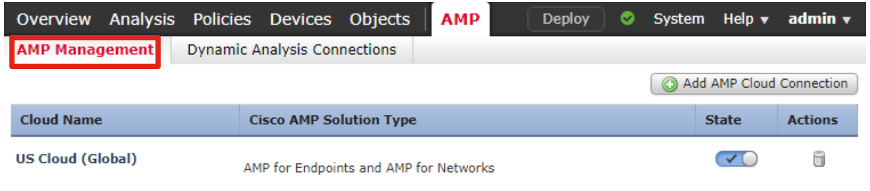
Private Cloud / Air-Gap


Information stored in AMP:
• AMP-PC GUID
AMP Cloud
NO File Reputation Check
(includes 1-1 SHA256, if Private Cloud does not know)
NO Retrospection via PING2
Organization’s Perimeter
Information stored on AMP-PC:
• Hashes
• Device GUID
AMP PRIVATE
Malicious Files automatically marked in AMP Private Cloud (poke)
TGA PRIVATE
Information stored on TGA:
• Files and Device GUID
• Analysis Results and Reports
Analysis Report
(Indicators, Threat Score)
File Reputation Check
(includes 1-1 SHA256, Spero)
Disposition
Retrospection via PING2
Analysis Request
(includes the file)
File Analysis
File Reputation
Disposition
File Reputation Check
(includes 1-1 SHA256, Spero)
FMC
Firepower Sensor

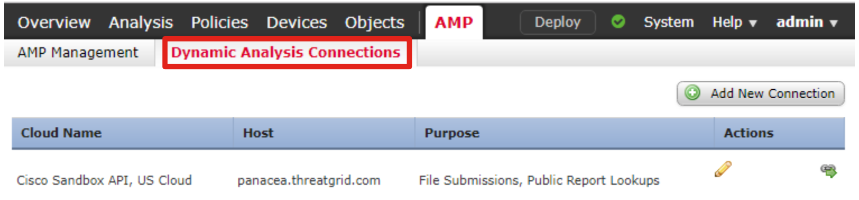
AMP for Networks (Firepower)

Tips & Tricks

- Confirm those firewall rules
  - File Reputation occurs from FMC
  - File Analysis occurs from Sensor
- Connect FMC to AMP Cloud and Threat Grid accounts



Cloud Name	Cisco AMP Solution Type	State	Actions
US Cloud (Global)	AMP for Endpoints and AMP for Networks	✓	

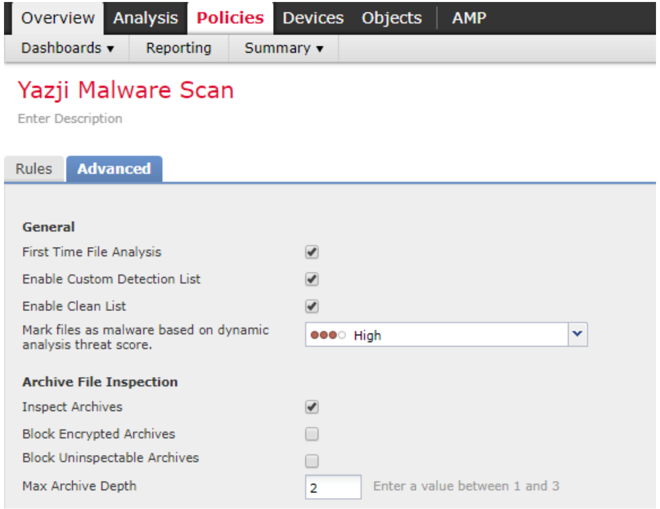


Cloud Name	Host	Purpose	Actions
Cisco Sandbox API, US Cloud	panacea.threatgrid.com	File Submissions, Public Report Lookups	

AMP for Networks (Firepower)

Configuration

- Malware & File Policy – Rule 1



Yazji Malware Scan

Enter Description

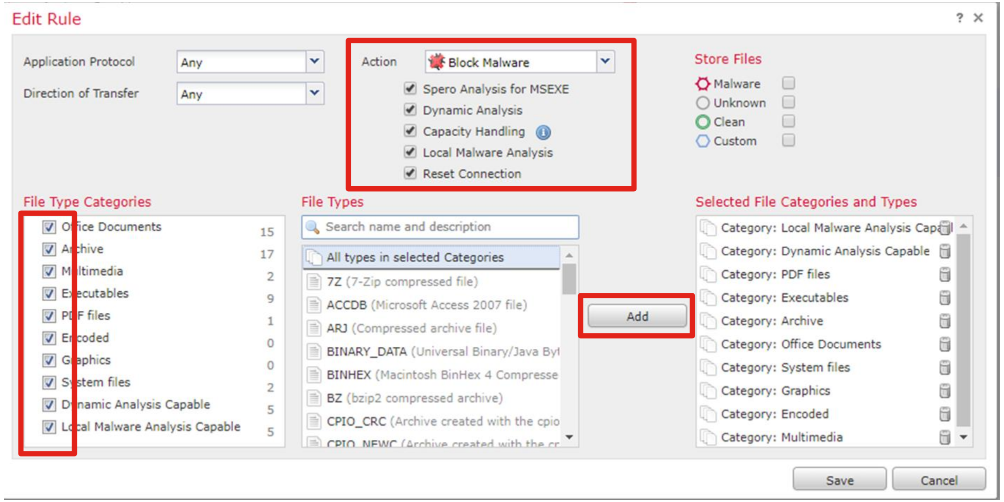
Rules | **Advanced**

General

- First Time File Analysis ☑
- Enable Custom Detection List ☑
- Enable Clean List ☑
- Mark files as malware based on dynamic analysis threat score: ●●●○ High

Archive File Inspection

- Inspect Archives ☑
- Block Encrypted Archives □
- Block Uninspectable Archives □
- Max Archive Depth: 2 — Enter a value between 1 and 3



Edit Rule

- Application Protocol: Any
- Direction of Transfer: Any
- Action: Block Malware
  - ☑ Spero Analysis for MSEXE
  - ☑ Dynamic Analysis
  - ☑ Capacity Handling
  - ☑ Local Malware Analysis
  - ☑ Reset Connection

Store Files

- Malware □
- Unknown □
- Clean □
- Custom □

File Type Categories

☑ Office Documents	15
☑ Archive	17
☑ Multimedia	2
☑ Executables	9
☑ PDF files	1
☑ Encoded	0
☑ Graphics	0
☑ System files	2
☑ Dynamic Analysis Capable	5
☑ Local Malware Analysis Capable	5

File Types

Search name and description

- All types in selected Categories
- 7Z (7-Zip compressed file)
- ACCDB (Microsoft Access 2007 file)
- ARJ (Compressed archive file)
- BINARY_DATA (Universal Binary/Java Byt
- BINHEX (Macintosh BinHex 4 Compresse
- BZ (bzip2 compressed archive)
- CPIO_CRC (Archive created with the cpio
- CPIO_NEWC (Archive created with the cr

Add

Selected File Categories and Types

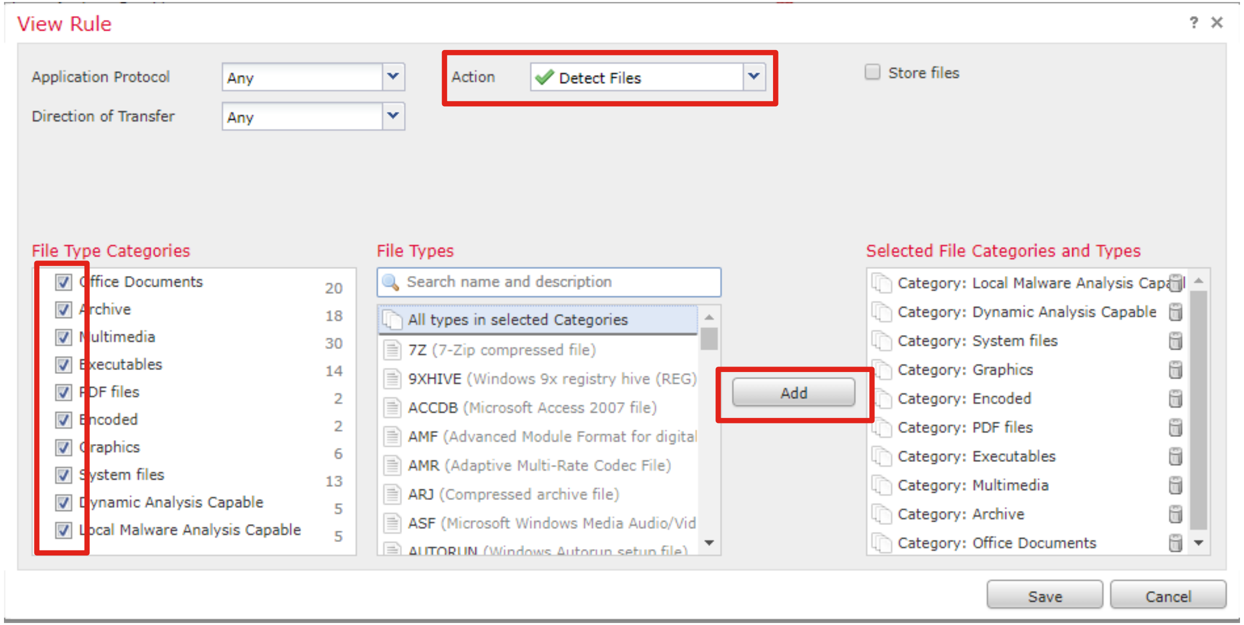
- Category: Local Malware Analysis Capa
- Category: Dynamic Analysis Capable
- Category: PDF files
- Category: Executables
- Category: Archive
- Category: Office Documents
- Category: System files
- Category: Graphics
- Category: Encoded
- Category: Multimedia

Save | Cancel

AMP for Networks (Firepower)

Configuration

- Malware & File Policy – Rule 2



View Rule

Application Protocol: Any

Direction of Transfer: Any

Action: Detect Files

□ Store files

File Type Categories

☑	Office Documents	20
☑	Archive	18
☑	Multimedia	30
☑	Executables	14
☑	PDF files	2
☑	Encoded	2
☑	Graphics	6
☑	System files	13
☑	Dynamic Analysis Capable	5
☑	Local Malware Analysis Capable	5

File Types

Search name and description

- All types in selected Categories
- 7Z (7-Zip compressed file)
- 9XHIVE (Windows 9x registry hive (REG)
- ACCDB (Microsoft Access 2007 file)
- AMF (Advanced Module Format for digital
- AMR (Adaptive Multi-Rate Codec File)
- ARJ (Compressed archive file)
- ASF (Microsoft Windows Media Audio/Vid
- AUTORUN (Windows Autorun setup file)

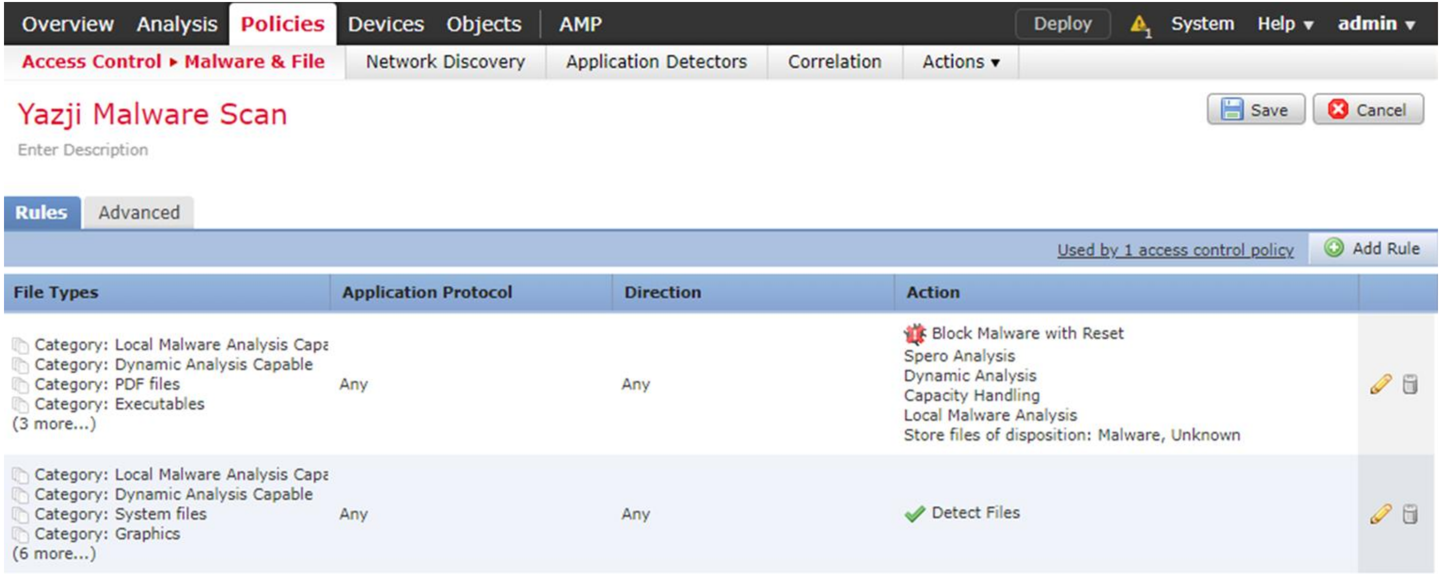
Selected File Categories and Types

- Category: Local Malware Analysis Capal
- Category: Dynamic Analysis Capable
- Category: System files
- Category: Graphics
- Category: Encoded
- Category: PDF files
- Category: Executables
- Category: Multimedia
- Category: Archive
- Category: Office Documents

AMP for Networks (Firepower)

Configuration

- Malware & File Policy



Yazji Malware Scan

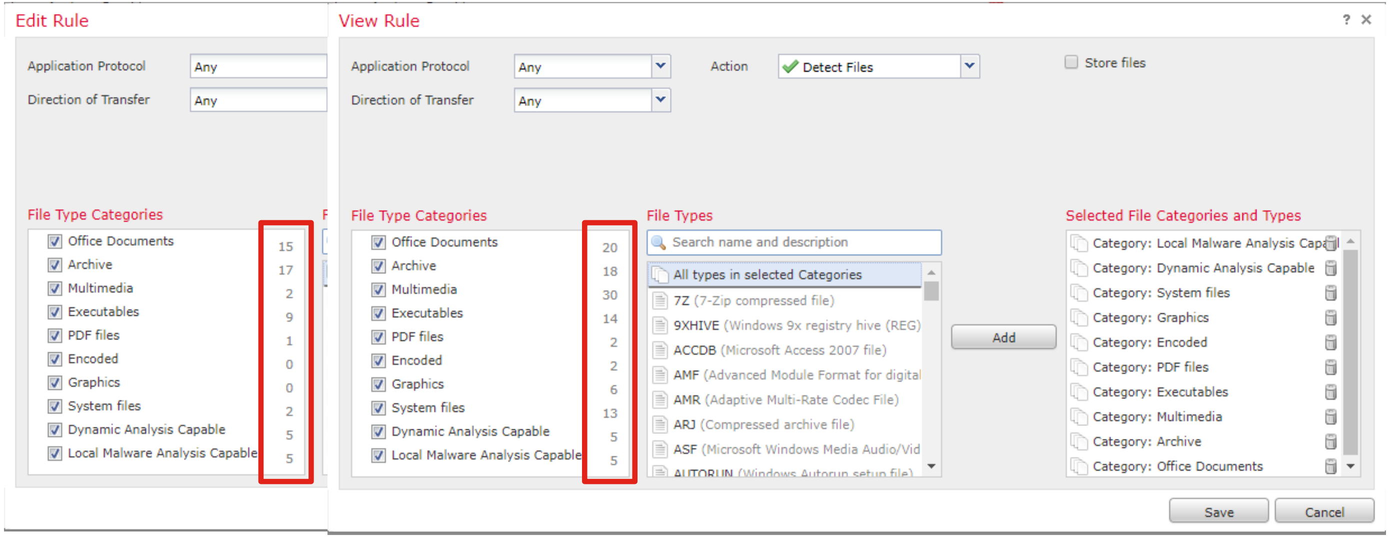
Enter Description

File Types	Application Protocol	Direction	Action
Category: Local Malware Analysis Capa Category: Dynamic Analysis Capable Category: PDF files Category: Executables (3 more...)	Any	Any	Block Malware with Reset Spero Analysis Dynamic Analysis Capacity Handling Local Malware Analysis Store files of disposition: Malware, Unknown
Category: Local Malware Analysis Capa Category: Dynamic Analysis Capable Category: System files Category: Graphics (6 more...)	Any	Any	✓ Detect Files

AMP for Networks (Firepower)

Configuration

- Malware & File Policy



Edit Rule

Application Protocol: Any

Direction of Transfer: Any

File Type Categories

☑ Office Documents	15
☑ Archive	17
☑ Multimedia	2
☑ Executables	9
☑ PDF files	1
☑ Encoded	0
☑ Graphics	0
☑ System files	2
☑ Dynamic Analysis Capable	5
☑ Local Malware Analysis Capable	5

View Rule

Application Protocol: Any

Direction of Transfer: Any

Action: ✓ Detect Files

□ Store files

File Type Categories

☑ Office Documents	20
☑ Archive	18
☑ Multimedia	30
☑ Executables	14
☑ PDF files	2
☑ Encoded	2
☑ Graphics	6
☑ System files	13
☑ Dynamic Analysis Capable	5
☑ Local Malware Analysis Capable	5

File Types

Search name and description

- All types in selected Categories
- 7Z (7-Zip compressed file)
- 9XHIVE (Windows 9x registry hive (REG)
- ACCDB (Microsoft Access 2007 file)
- AMF (Advanced Module Format for digital
- AMR (Adaptive Multi-Rate Codec File)
- ARJ (Compressed archive file)
- ASF (Microsoft Windows Media Audio/Vid
- AUTORUN (Windows Autorun setup file)

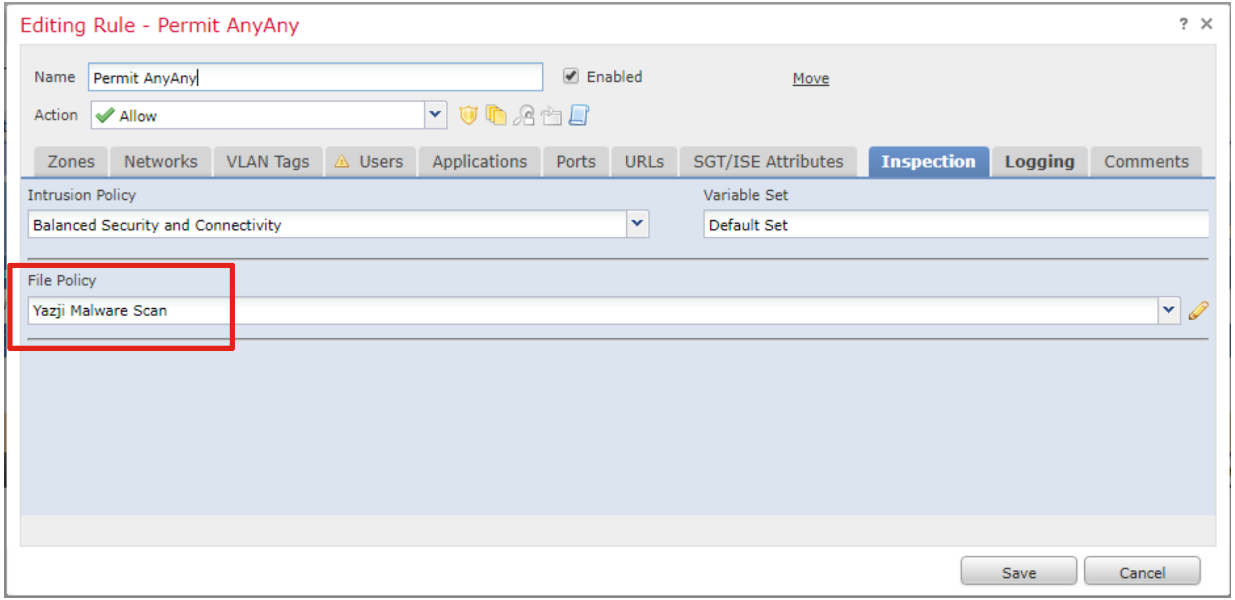
Selected File Categories and Types

- Category: Local Malware Analysis Capa
- Category: Dynamic Analysis Capable
- Category: System files
- Category: Graphics
- Category: Encoded
- Category: PDF files
- Category: Executables
- Category: Multimedia
- Category: Archive
- Category: Office Documents

AMP for Networks (Firepower)

Configuration

- Access Policy



Editing Rule - Permit AnyAny

Name: Permit AnyAny

☑ Enabled

Action: ✓ Allow

Intrusion Policy: Balanced Security and Connectivity

Variable Set: Default Set

File Policy: Yazji Malware Scan

Cisco AMP and Threat Grid for Umbrella and Meraki

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

- How do cloud services access AMP and Threat Grid?
- How do I configure AMP and Threat Grid on Umbrella Secure Web Gateway (SWG)
- What about Meraki config? Is it really that simple?

Why did I combine them…?

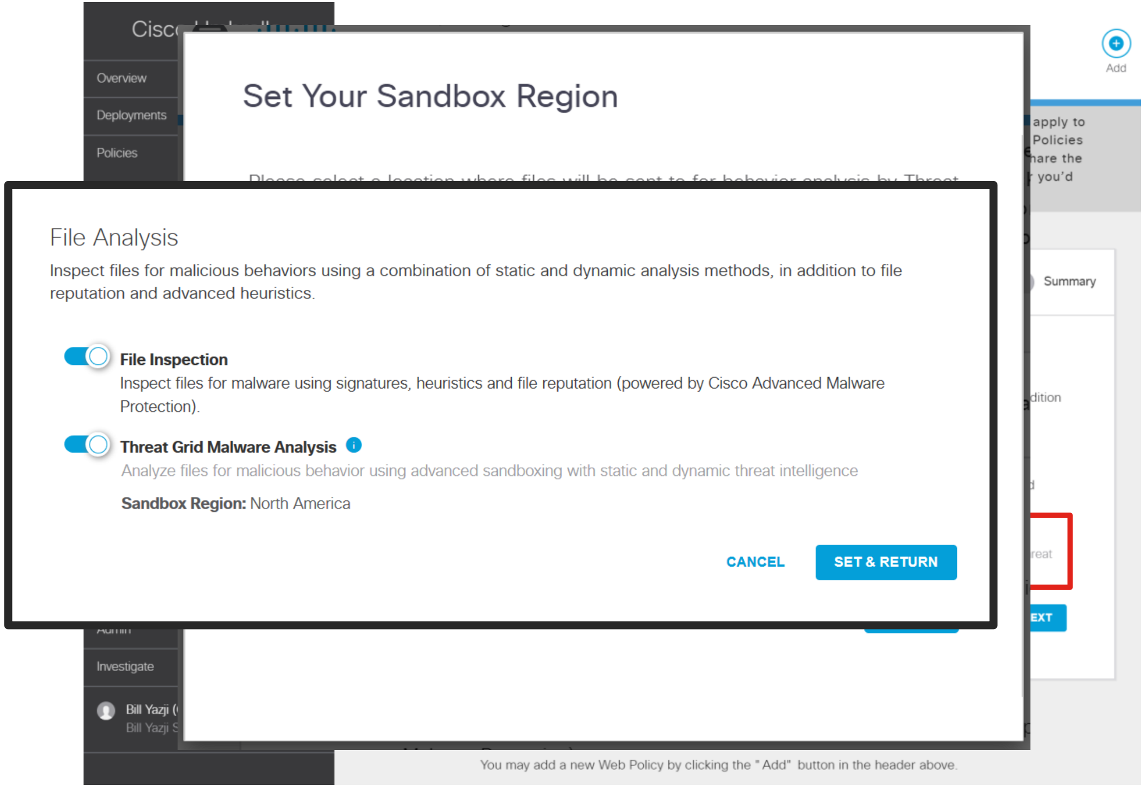
Not all that different!

- We have covered the flows….
  - Earlier slides show architecture & supported deployments
- We know the architecture…
  - AMP and Threat Grid
  - Cloud services only talk to AMP Public Cloud and Threat Grid Cloud

- So let’s talk configuration, best practices & differences…

Umbrella Web Policy Configuration

- File Inspection
  - AMP File Reputation
- Threat Grid Malware Analysis
  - Static and Dynamic Analysis
- North America or Europe



File Analysis

Inspect files for malicious behaviors using a combination of static and dynamic analysis methods, in addition to file reputation and advanced heuristics.

File Inspection
Inspect files for malware using signatures, heuristics and file reputation (powered by Cisco Advanced Malware Protection).

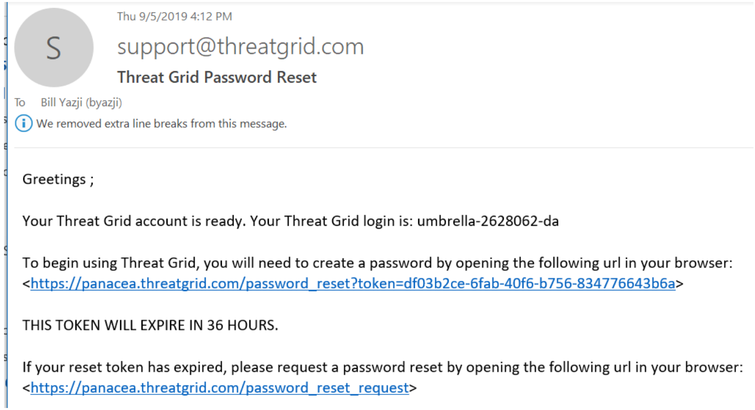
Threat Grid Malware Analysis
Analyze files for malicious behavior using advanced sandboxing with static and dynamic threat intelligence

Sandbox Region: North America

CANCEL SET & RETURN

Now what happens?

- Umbrella user receives password reset email for TG Entitlement org immediately – once complete will gain access to this TG Entitlement org
- At this point the Umbrella Service account and Device-Admin Entitlement org users are created automagically
- If the company has an existing TG Org or Entitlement org, request provisioning to move the accounts to existing org.



Thu 9/5/2019 4:12 PM

S support@threatgrid.com

Threat Grid Password Reset

To Bill Yazji (byazji)

ⓘ We removed extra line breaks from this message.

Greetings ;

Your Threat Grid account is ready. Your Threat Grid login is: umbrella-2628062-da

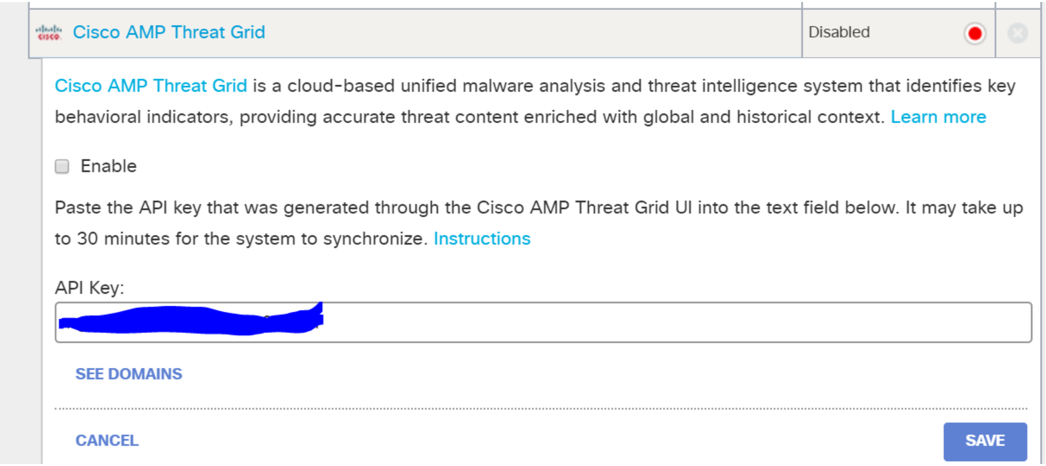
To begin using Threat Grid, you will need to create a password by opening the following url in your browser: <https://panacea.threatgrid.com/password_reset?token=df03b2ce-6fab-40f6-b756-834776643b6a>

THIS TOKEN WILL EXPIRE IN 36 HOURS.

If your reset token has expired, please request a password reset by opening the following url in your browser: <https://panacea.threatgrid.com/password_reset_request>

Umbrella Integration Tips (1)

- The legacy “Policies/Integrations: Threat Grid” config just pulls a Threat Grid domain feed into an Umbrella policy. This has proven to be false positive ridden and not suggested to be used for blocking – not suggested to be used when running Threat Grid with SWG.
- https://support.umbrella.com/hc/en-us/articles/231248768-Cisco-Umbrella-Cisco-AMP-Threat-Grid-Cloud-Integration-Setup-Guide



Cisco AMP Threat Grid — Disabled ●

Cisco AMP Threat Grid is a cloud-based unified malware analysis and threat intelligence system that identifies key behavioral indicators, providing accurate threat content enriched with global and historical context. Learn more

□ Enable

Paste the API key that was generated through the Cisco AMP Threat Grid UI into the text field below. It may take up to 30 minutes for the system to synchronize. Instructions

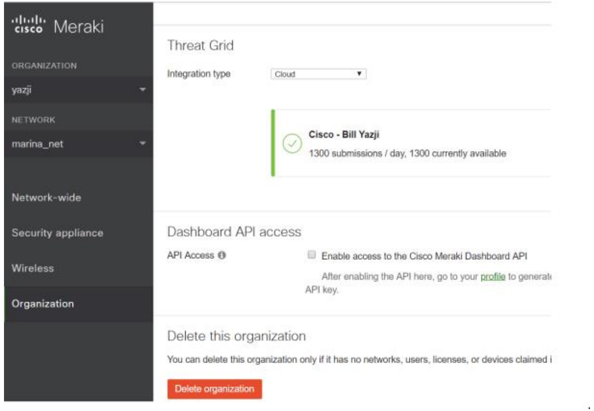
API Key: [redacted]

Umbrella Integration Tips (2)

- Configuration is simple – and one time
- File Analysis is only for SWG Full Proxy, not Selective Proxy
- Sandbox region selected is permanent – region is per org. All orgs in a multi-org must be in the same region as well.

AMP & Threat Grid for Meraki MX

- Setup TG under Organization/Settings/Threat Grid
- Configure AMP under Security & SD-WAN/Threat Protection
- HTTP Traffic, HTTPS in v15.15+ in beta
- MX Supports AMP Cloud (US), and Cloud Threat Grid (US & EU)



Threat Grid

Integration type: Cloud

Cisco - Bill Yazji

1300 submissions / day, 1300 currently available

Dashboard API access

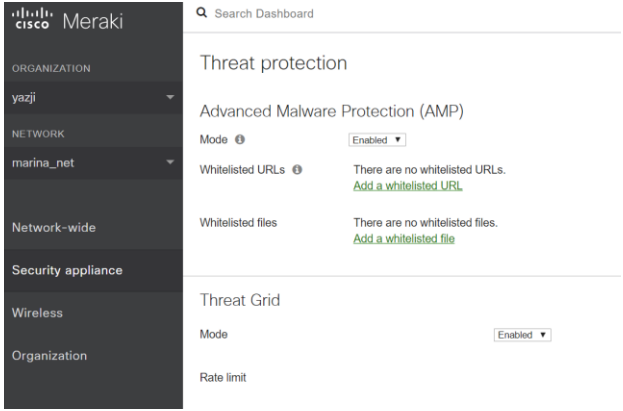
API Access: ☐ Enable access to the Cisco Meraki Dashboard API

After enabling the API here, go to your profile to generat

API key.

Delete this organization

You can delete this organization only if it has no networks, users, licenses, or devices claimed i



Threat protection

Advanced Malware Protection (AMP)

Mode: Enabled

Whitelisted URLs: There are no whitelisted URLs. Add a whitelisted URL

Whitelisted files: There are no whitelisted files. Add a whitelisted file

Threat Grid

Mode: Enabled

Rate limit

AMP & Threat Grid for Meraki MX

- Meraki MX file type support:
  - File Reputation: SWF, MSOLE2 (.doc, .xls, .ppt), MSCAB, PDF, EXE, ELF, MACHO, MACHO UNIBIN, JAVA, XML based MS Office files
  - File Analysis: PE32, DLL, PDF and MS Office files
- Maximum file size is 10 MB
- Meraki does not include any submissions to Threat Grid by default
  - The number of available sample submissions to Threat Grid Cloud determined by Threat Grid Advanced File Analysis license purchase
  - Threat Grid Cloud Portal licensed separately

Threat Grid Cloud Portal vs. AMP-Enabled Integration

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

- What Threat Grid is 'included' with just an AMP-Enabled integration?
- What does the Threat Grid Cloud portal offer to a customer that can not be done with an AMP-Enabled integration?
- Can I integrate with 3rd party products? How?
- Threat Grid offers different types of portal views?!?
- How do I integrate my AMP-Enabled devices to Threat Grid Cloud?

Threat Grid Offering Comparison

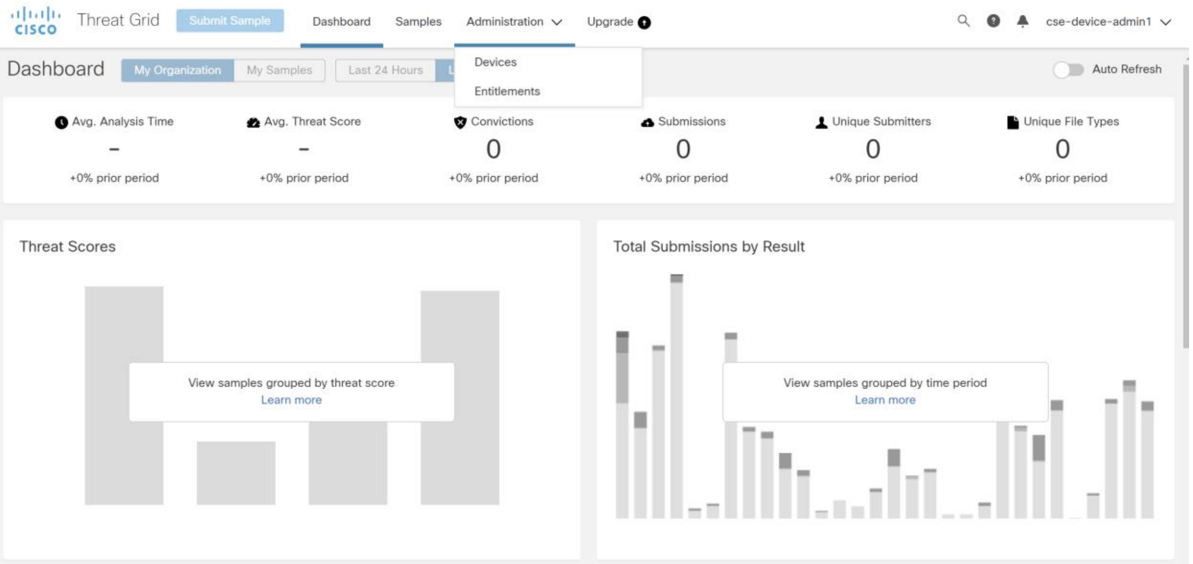
AMP-Enabled Threat Grid, Entitlement Portal and Threat Grid Cloud Portal

	AMP-Enabled Threat Grid	Threat Grid Entitlement Portal	Threat Grid Cloud Portal
Automatic submission from Cisco AMP-Enabled Device	✓ *	✓ *	✓ *
Access to “Device/Entitlements” section of TG Cloud		✓	✓
Manual file & 3rd party API submissions			✓ *
Search and pivot on Global Data			✓
Cisco Threat Response 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

Threat Grid Entitlement Portal

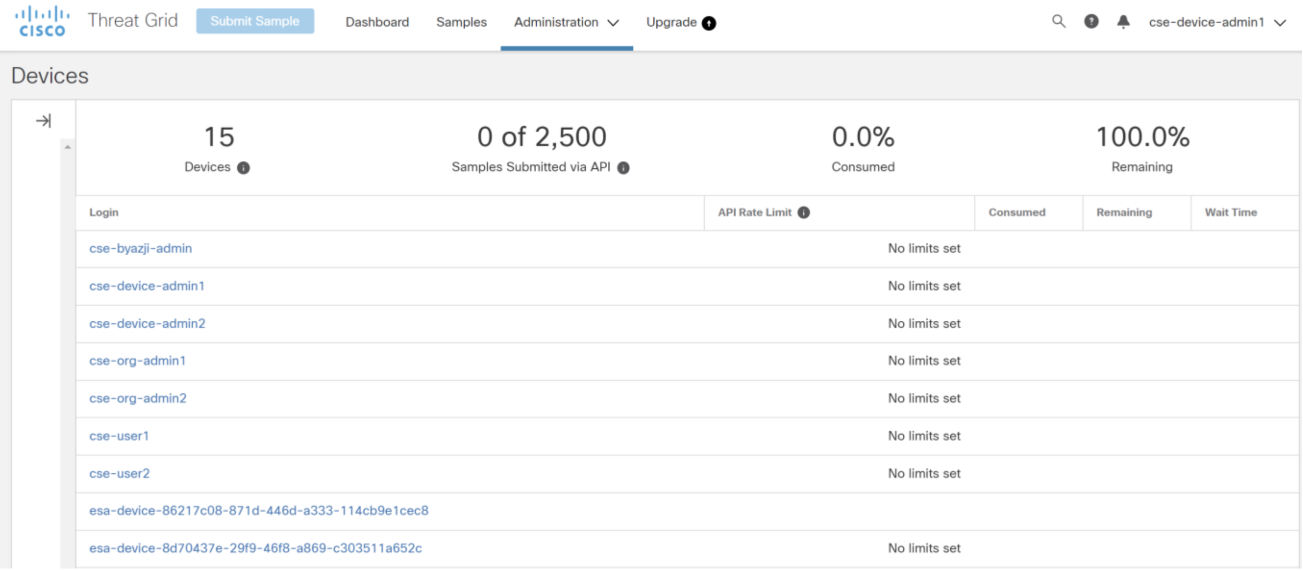
- No-cost access for all AMP-Enabled customers who do not have Threat Grid Cloud
- Special 'Device_Admin' account that provides a **limited view** of the Threat Grid Cloud portal
  - Sample Consumption per 24 hours
  - Basic Dashboard – Avg. Analysis Time, Avg. Threat Score, Convictions, etc.
- Ability to view device information and organizational entitlements



Threat Grid Entitlement Portal

Devices View

- Access for all Threat Grid and AMP-Enabled customers
- View all devices in an organization
  - API Limits
  - Amount Consumed
  - Remaining
- Ability to self-configure device limits from organizational total



Devices

15 Devices

0 of 2,500 Samples Submitted via API

0.0% Consumed

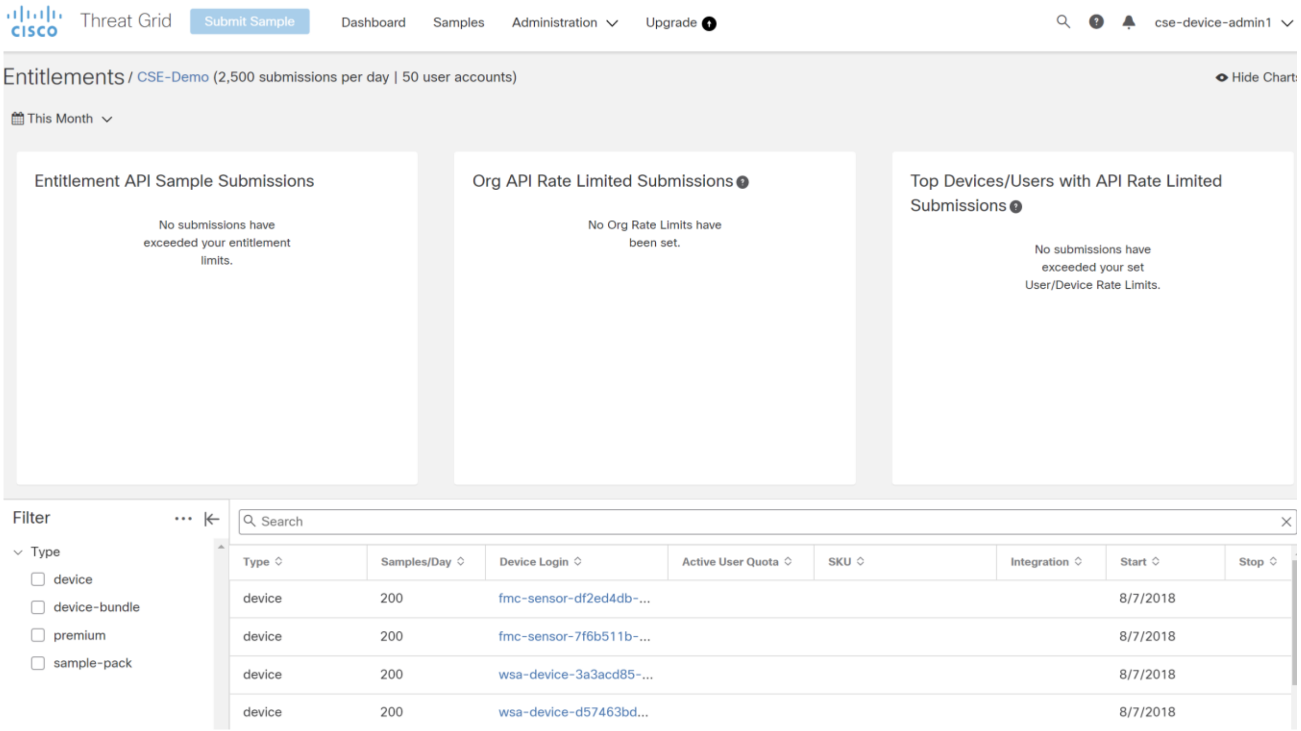
100.0% Remaining

Login	API Rate Limit	Consumed	Remaining	Wait Time
cse-byazji-admin	No limits set			
cse-device-admin1	No limits set			
cse-device-admin2	No limits set			
cse-org-admin1	No limits set			
cse-org-admin2	No limits set			
cse-user1	No limits set			
cse-user2	No limits set			
esa-device-86217c08-871d-446d-a333-114cb9e1cec8				
esa-device-8d70437e-29f9-46f8-a869-c303511a652c	No limits set			

Threat Grid Entitlement Portal

Entitlement View

- Access for all Threat Grid and AMP-Enabled customers
- View all Entitlements in an organization
    - TypeSamples/Day
    - Login
    - Users (if applicable)
    - Re-order SKU
    - Start/End date - subscription



Entitlements / CSE-Demo (2,500 submissions per day | 50 user accounts)

Entitlement API Sample Submissions

No submissions have exceeded your entitlement limits.

Org API Rate Limited Submissions

No Org Rate Limits have been set.

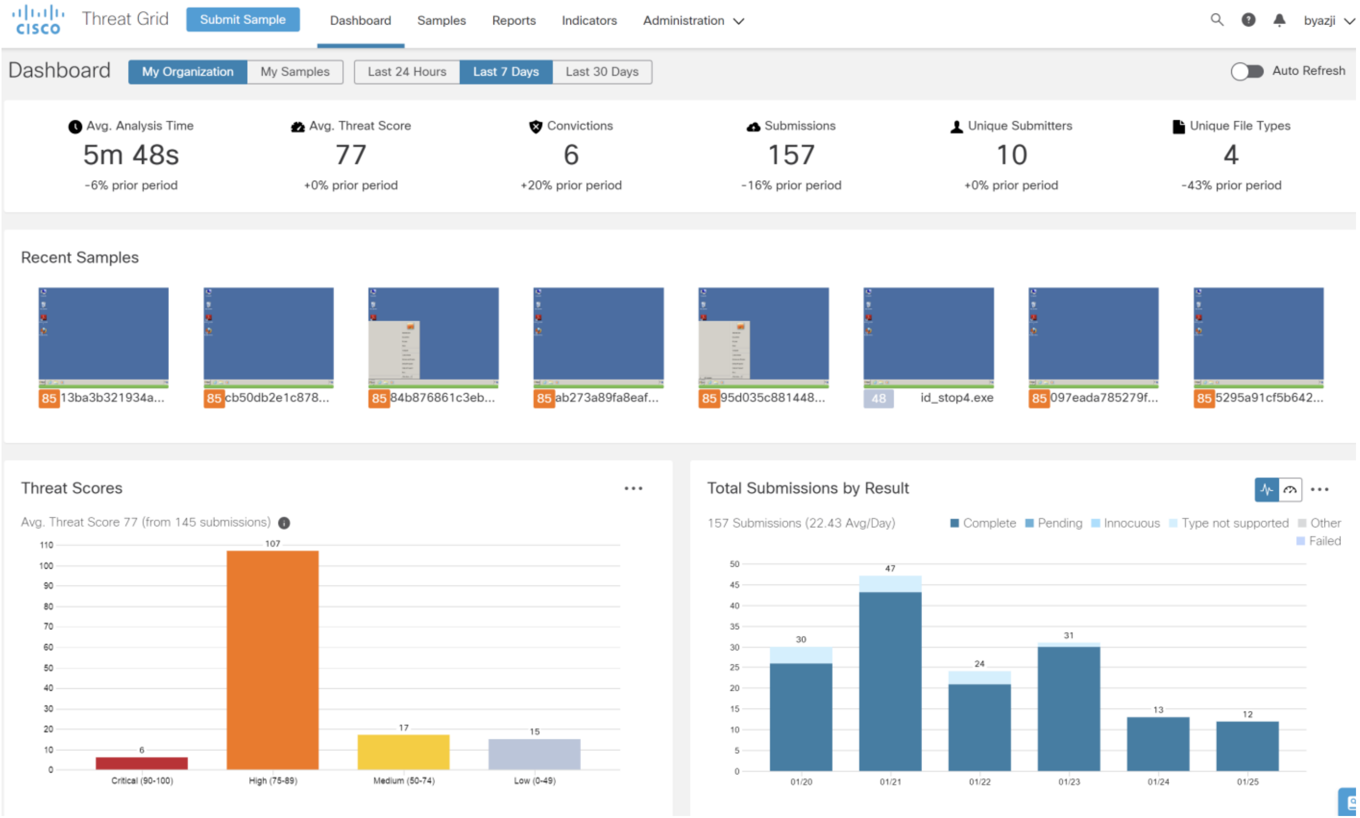
Top Devices/Users with API Rate Limited Submissions

No submissions have exceeded your set User/Device Rate Limits.

Type	Samples/Day	Device Login	Active User Quota	SKU	Integration	Start	Stop
device	200	fmc-sensor-df2ed4db-...				8/7/2018	
device	200	fmc-sensor-7f6b511b-...				8/7/2018	
device	200	wsa-device-3a3acd85-...				8/7/2018	
device	200	wsa-device-d57463bd...				8/7/2018	

Threat Grid Cloud

Full access portal



Avg. Analysis Time 5m 48s -6% prior period

Avg. Threat Score 77 +0% prior period

Convictions 6 +20% prior period

Submissions 157 -16% prior period

Unique Submitters 10 +0% prior period

Unique File Types 4 -43% prior period

Recent Samples

85 13ba3b321934a...

85 cb50db2e1c878...

85 84b876861c3eb...

85 ab273a89fa8eaf...

85 95d035c881448...

48 id_stop4.exe

85 097eada785279f...

85 5295a91cf5b642...

Threat Scores

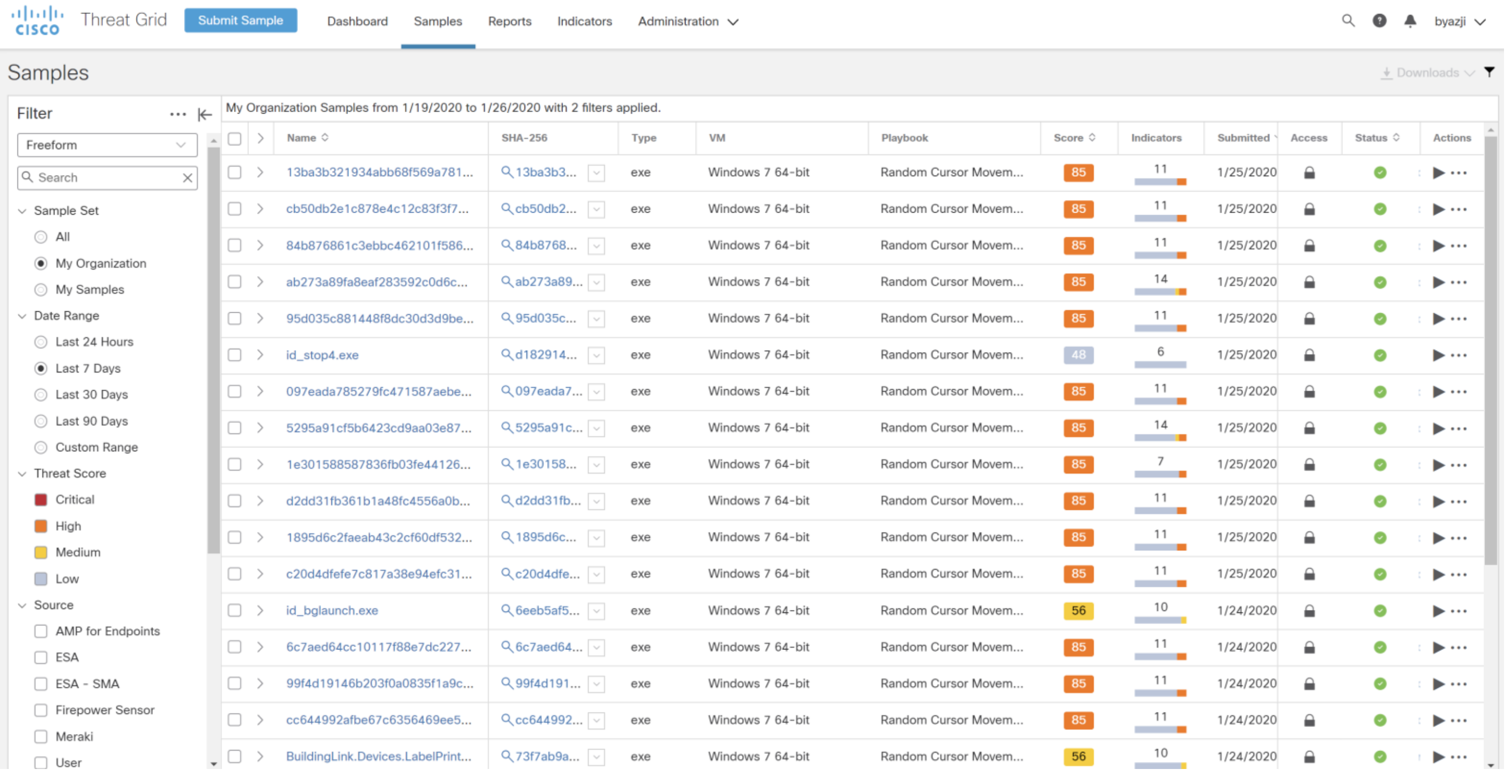
Avg. Threat Score 77 (from 145 submissions)

Total Submissions by Result

157 Submissions (22.43 Avg/Day)

File Analysis Visibility

Threat Grid Sample Manager



Threat Grid | Submit Sample | Dashboard | Samples | Reports | Indicators | Administration | byazji

Samples

Downloads

Filter

Freeform

Search

Sample Set
- ○ 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

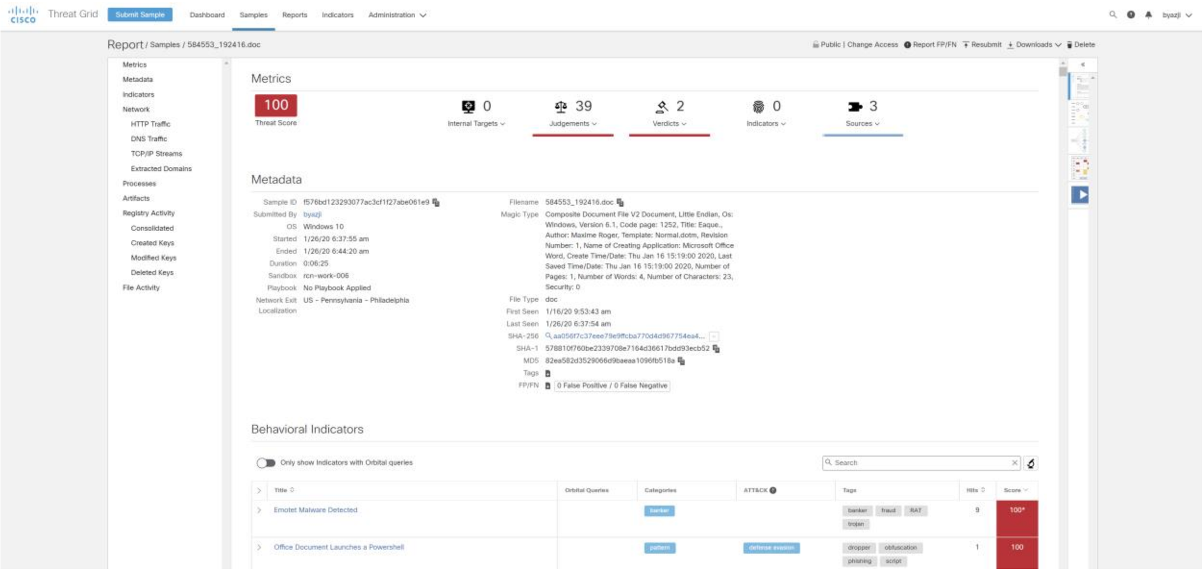
Source
- □ AMP for Endpoints
- □ ESA
- □ ESA - SMA
- □ Firepower Sensor
- □ Meraki
- □ User

My Organization Samples from 1/19/2020 to 1/26/2020 with 2 filters applied.

□	Name	SHA-256	Type	VM	Playbook	Score	Indicators	Submitted	Access	Status	Actions
□	13ba3b321934abb68f569a781...	13ba3b3...	exe	Windows 7 64-bit	Random Cursor Movem...	85	11	1/25/2020	🔒	✓	▶ ⋯
□	cb50db2e1c878e4c12c83f3f7...	cb50db2...	exe	Windows 7 64-bit	Random Cursor Movem...	85	11	1/25/2020	🔒	✓	▶ ⋯
□	84b876861c3ebbc462101f586...	84b8768...	exe	Windows 7 64-bit	Random Cursor Movem...	85	11	1/25/2020	🔒	✓	▶ ⋯
□	ab273a89fa8eaf283592c0d6c...	ab273a89...	exe	Windows 7 64-bit	Random Cursor Movem...	85	14	1/25/2020	🔒	✓	▶ ⋯
□	95d035c881448f8dc30d3d9be...	95d035c...	exe	Windows 7 64-bit	Random Cursor Movem...	85	11	1/25/2020	🔒	✓	▶ ⋯
□	id_stop4.exe	d182914...	exe	Windows 7 64-bit	Random Cursor Movem...	48	6	1/25/2020	🔒	✓	▶ ⋯
□	097eada785279fc471587aebe...	097eada7...	exe	Windows 7 64-bit	Random Cursor Movem...	85	11	1/25/2020	🔒	✓	▶ ⋯
□	5295a91cf5b6423cd9aa03e87...	5295a91c...	exe	Windows 7 64-bit	Random Cursor Movem...	85	14	1/25/2020	🔒	✓	▶ ⋯
□	1e301588587836fb03fe44126...	1e30158...	exe	Windows 7 64-bit	Random Cursor Movem...	85	7	1/25/2020	🔒	✓	▶ ⋯
□	d2dd31fb361b1a48fc4556a0b...	d2dd31fb...	exe	Windows 7 64-bit	Random Cursor Movem...	85	11	1/25/2020	🔒	✓	▶ ⋯
□	1895d6c2faeab43c2cf60df532...	1895d6c...	exe	Windows 7 64-bit	Random Cursor Movem...	85	11	1/25/2020	🔒	✓	▶ ⋯
□	c20d4dfefe7c817a38e94efc31...	c20d4dfe...	exe	Windows 7 64-bit	Random Cursor Movem...	85	11	1/25/2020	🔒	✓	▶ ⋯
□	id_bglaunch.exe	6eeb5af5...	exe	Windows 7 64-bit	Random Cursor Movem...	56	10	1/24/2020	🔒	✓	▶ ⋯
□	6c7aed64cc10117f88e7dc227...	6c7aed64...	exe	Windows 7 64-bit	Random Cursor Movem...	85	11	1/24/2020	🔒	✓	▶ ⋯
□	99f4d19146b203f0a0835f1a9c...	99f4d191...	exe	Windows 7 64-bit	Random Cursor Movem...	85	11	1/24/2020	🔒	✓	▶ ⋯
□	cc644992afbe67c6356469ee5...	cc644992...	exe	Windows 7 64-bit	Random Cursor Movem...	85	11	1/24/2020	🔒	✓	▶ ⋯
□	BuildingLink.Devices.LabelPrint...	73f7ab9a...	exe	Windows 7 64-bit	Random Cursor Movem...	56	10	1/24/2020	🔒	✓	▶ ⋯

Threat Grid Analysis Results

- The Threat Grid Analysis Report provides a detailed view to:
  - Meta Data
  - Behavioral Indicators
  - Network Activity
  - Processes
  - Artifacts
  - Registry Activities
  - File Activities
  - Threat Response Bar
- Threat Grid also provides:
  - 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



Metrics

100 Threat Score

0 Internal Targets

39 Judgements

2 Verdicts

0 Indicators

3 Sources

Metadata

Sample ID f576bd123293077ac3cf1f27abe061e9
Submitted By byazji
OS Windows 10
Started 1/26/20 6:37:55 am
Ended 1/26/20 6:44:20 am
Duration 0:06:25
Sandbox rcn-work-006
Playbook No Playbook Applied
Network Exit Localization US - Pennsylvania - Philadelphia

Filename 584553_192416.doc
Magic Type Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, Code page: 1252, Title: Eaque., Author: Maxime Roger, Template: Normal.dotm, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Create Time/Date: Thu Jan 16 15:19:00 2020, Last Saved Time/Date: Thu Jan 16 15:19:00 2020, Number of Pages: 1, Number of Words: 4, Number of Characters: 23, Security: 0
File Type doc
First Seen 1/16/20 9:53:43 am
Last Seen 1/26/20 6:37:54 am
SHA-256 aa056f7c37eee79e9ffcba770d4d967754ea4...
SHA-1 578810f760be2339708e7164d36617bdd93ecb52
MD5 82ea582d3529066d9baeaa1096fb518a
Tags
FP/FN 0 False Positive / 0 False Negative

Behavioral Indicators

Only show Indicators with Orbital queries

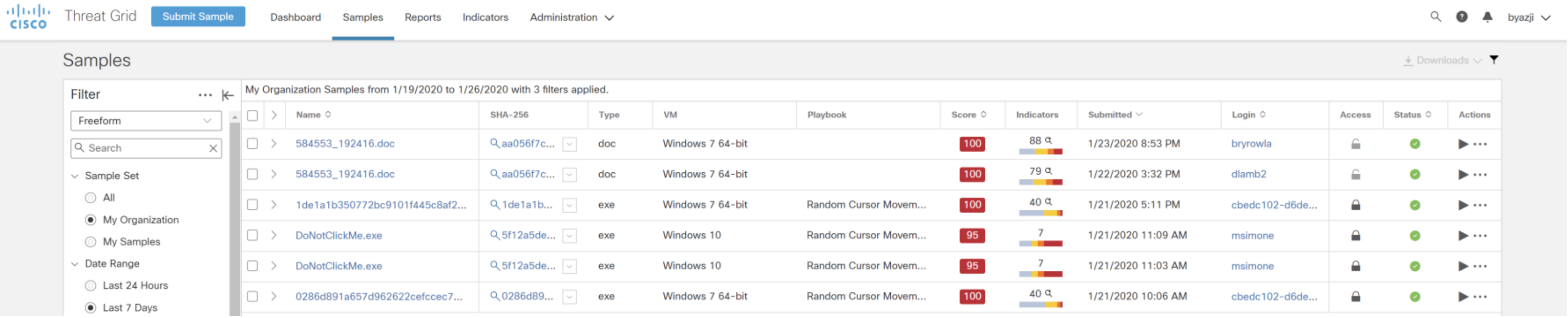
Search

Title	Orbital Queries	Categories	ATT&CK	Tags	Hits	Score
Emotet Malware Detected		banker		banker fraud RAT trojan	9	100*
Office Document Launches a Powershell		pattern	defense evasion	dropper obfuscation phishing script	1	100

Threat Grid Public Cloud Submissions

Public and Private Tagging

- Every Sample submitted to Threat Grid Cloud gets tagged:
  - Public – Sample will be visible globally (each user can access all the details of the report)
  - Private – Sample is <u>only</u> visible to the submitting Organization
- Automated Submissions from an AMP-Enabled Integration are **<u>always</u>** marked private



Samples

Filter

Freeform

Search

Sample Set

○ All

● My Organization

○ My Samples

Date Range

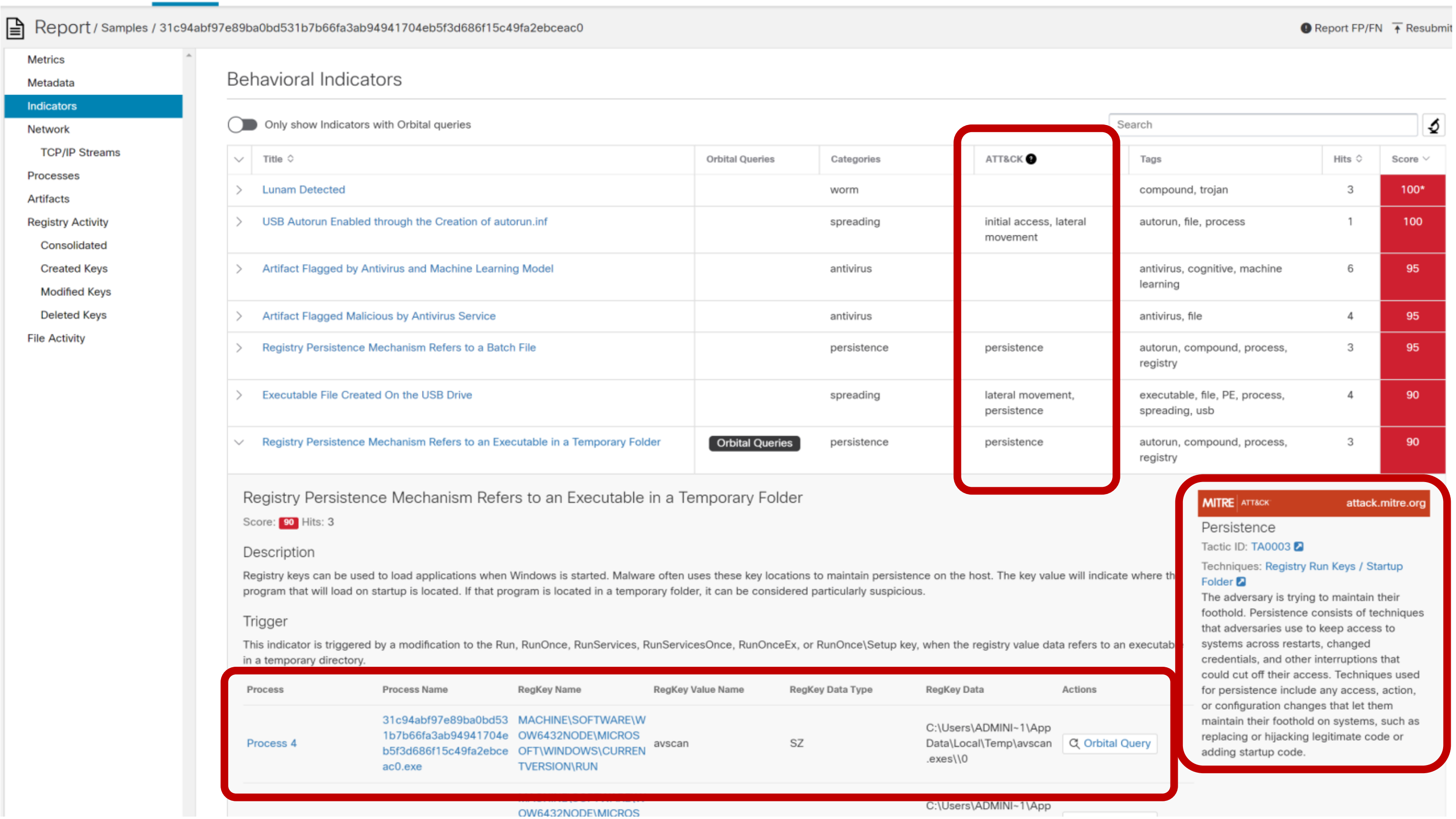
○ Last 24 Hours

● Last 7 Days

My Organization Samples from 1/19/2020 to 1/26/2020 with 3 filters applied.

□	Name	SHA-256	Type	VM	Playbook	Score	Indicators	Submitted	Login	Access	Status	Actions
□	584553_192416.doc	aa056f7c...	doc	Windows 7 64-bit		100	88	1/23/2020 8:53 PM	bryrowla	🔓	✓	▶ ···
□	584553_192416.doc	aa056f7c...	doc	Windows 7 64-bit		100	79	1/22/2020 3:32 PM	dlamb2	🔓	✓	▶ ···
□	1de1a1b350772bc9101f445c8af2...	1de1a1b...	exe	Windows 7 64-bit	Random Cursor Movem...	100	40	1/21/2020 5:11 PM	cbedc102-d6de...	🔒	✓	▶ ···
□	DoNotClickMe.exe	5f12a5de...	exe	Windows 10	Random Cursor Movem...	95	7	1/21/2020 11:09 AM	msimone	🔒	✓	▶ ···
□	DoNotClickMe.exe	5f12a5de...	exe	Windows 10	Random Cursor Movem...	95	7	1/21/2020 11:03 AM	msimone	🔒	✓	▶ ···
□	0286d891a657d962622cefccec7...	0286d89...	exe	Windows 7 64-bit	Random Cursor Movem...	100	40	1/21/2020 10:06 AM	cbedc102-d6de...	🔒	✓	▶ ···

Orbital & MITRE ATT&CK



Report / Samples / 31c94abf97e89ba0bd531b7b66fa3ab94941704eb5f3d686f15c49fa2ebceac0

Behavioral Indicators

○ Only show Indicators with Orbital queries

Search

Title	Orbital Queries	Categories	ATT&CK	Tags	Hits	Score
Lunam Detected		worm		compound, trojan	3	100*
USB Autorun Enabled through the Creation of autorun.inf		spreading	initial access, lateral movement	autorun, file, process	1	100
Artifact Flagged by Antivirus and Machine Learning Model		antivirus		antivirus, cognitive, machine learning	6	95
Artifact Flagged Malicious by Antivirus Service		antivirus		antivirus, file	4	95
Registry Persistence Mechanism Refers to a Batch File		persistence	persistence	autorun, compound, process, registry	3	95
Executable File Created On the USB Drive		spreading	lateral movement, persistence	executable, file, PE, process, spreading, usb	4	90
Registry Persistence Mechanism Refers to an Executable in a Temporary Folder	Orbital Queries	persistence	persistence	autorun, compound, process, registry	3	90

Registry Persistence Mechanism Refers to an Executable in a Temporary Folder

Score: 90 Hits: 3

Description

Registry keys can be used to load applications when Windows is started. Malware often uses these key locations to maintain persistence on the host. The key value will indicate where th program that will load on startup is located. If that program is located in a temporary folder, it can be considered particularly suspicious.

Trigger

This indicator is triggered by a modification to the Run, RunOnce, RunServices, RunServicesOnce, RunOnceEx, or RunOnce\Setup key, when the registry value data refers to an executab in a temporary directory.

Process	Process Name	RegKey Name	RegKey Value Name	RegKey Data Type	RegKey Data	Actions
Process 4	31c94abf97e89ba0bd531b7b66fa3ab94941704eb5f3d686f15c49fa2ebceac0.exe	MACHINE\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN	avscan	SZ	C:\Users\ADMINI~1\AppData\Local\Temp\avscan.exes\\0	Orbital Query
		OW6432NODE\MICROS			C:\Users\ADMINI~1\App	

MITRE ATT&CK attack.mitre.org

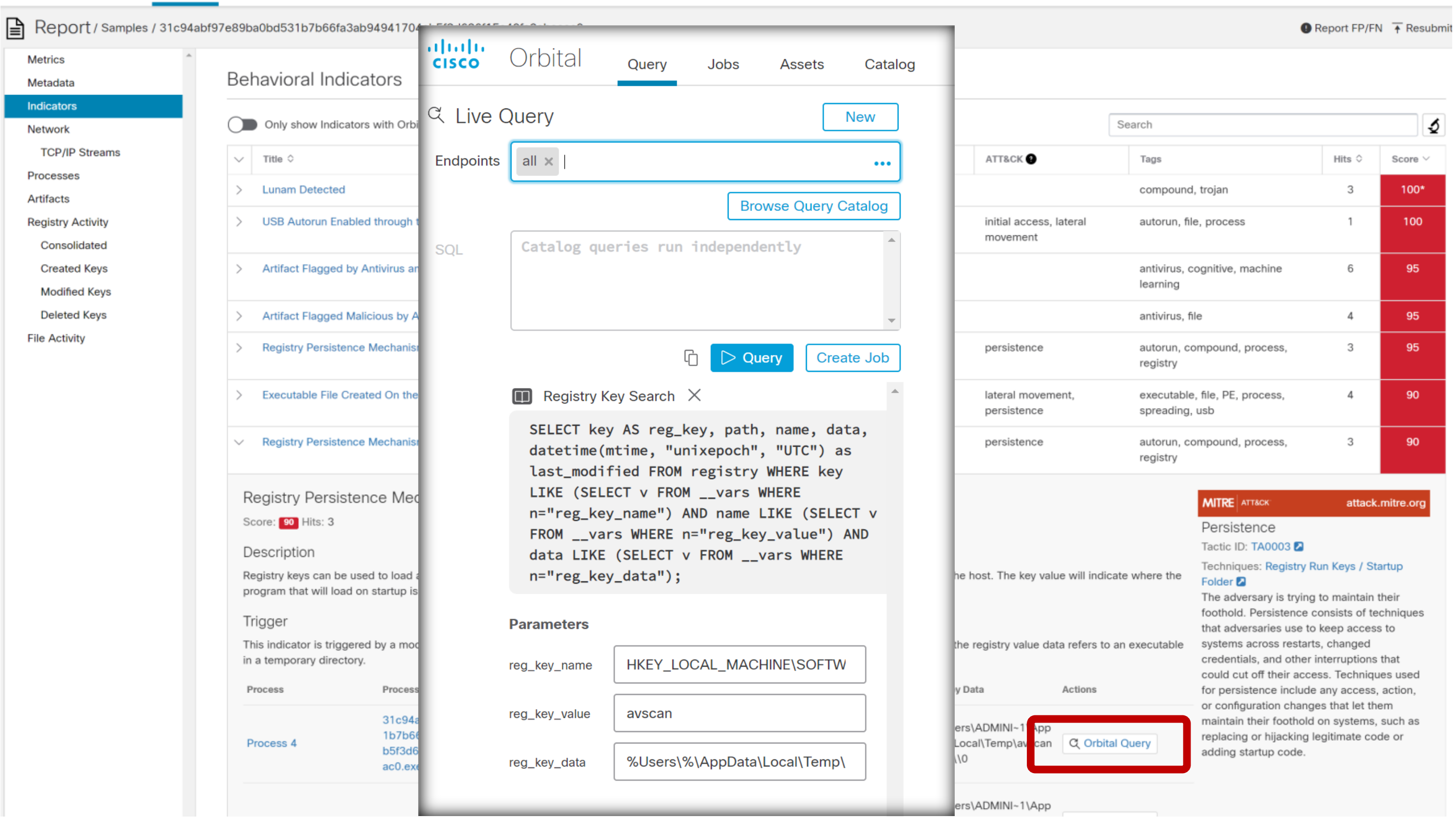
Persistence

Tactic ID: TA0003

Techniques: Registry Run Keys / Startup Folder

The adversary is trying to maintain their foothold. Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access. Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code.

Orbital & MITRE ATT&CK



Report / Samples / 31c94abf97e89ba0bd531b7b66fa3ab94941704

Report FP/FN   Resubmit

- Metrics
- Metadata
- Indicators
- Network
  - TCP/IP Streams
- Processes
- Artifacts
- Registry Activity
  - Consolidated
  - Created Keys
  - Modified Keys
  - Deleted Keys
- File Activity

Behavioral Indicators

Only show Indicators with Orbi

Search

Title	ATT&CK	Tags	Hits	Score
Lunam Detected		compound, trojan	3	100*
USB Autorun Enabled through t	initial access, lateral movement	autorun, file, process	1	100
Artifact Flagged by Antivirus ar		antivirus, cognitive, machine learning	6	95
Artifact Flagged Malicious by A		antivirus, file	4	95
Registry Persistence Mechanis	persistence	autorun, compound, process, registry	3	95
Executable File Created On the	lateral movement, persistence	executable, file, PE, process, spreading, usb	4	90
Registry Persistence Mechanis	persistence	autorun, compound, process, registry	3	90

Registry Persistence Mec

Score: 90 Hits: 3

Description

Registry keys can be used to load a ... he host. The key value will indicate where the program that will load on startup is

Trigger

This indicator is triggered by a mod ... the registry value data refers to an executable in a temporary directory.

Process	Process	y Data	Actions
Process 4	31c94a 1b7b66 b5f3d6 ac0.exe	ers\ADMINI~1\App Local\Temp\av can \\0	Orbital Query
		ers\ADMINI~1\App	

MITRE ATT&CK attack.mitre.org

Persistence

Tactic ID: TA0003

Techniques: Registry Run Keys / Startup Folder

The adversary is trying to maintain their foothold. Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access. Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code.

Live Query   New

Endpoints: all ×

Browse Query Catalog

SQL: Catalog queries run independently

Query   Create Job

Registry Key Search

```
SELECT key AS reg_key, path, name, data,
datetime(mtime, "unixepoch", "UTC") as
last_modified FROM registry WHERE key
LIKE (SELECT v FROM __vars WHERE
n="reg_key_name") AND name LIKE (SELECT v
FROM __vars WHERE n="reg_key_value") AND
data LIKE (SELECT v FROM __vars WHERE
n="reg_key_data");
```

Parameters

reg_key_name: HKEY_LOCAL_MACHINE\SOFTW

reg_key_value: avscan

reg_key_data: %Users\%\AppData\Local\Temp\

Integrations feeding Threat Grid Cloud

- CES, ESA, WSA, Firepower
  - File Analysis (FA) Client ID identifies individual device to Threat Grid. Devices register with Threat Grid Cloud using their individual FA Client ID
- Umbrella, AMP for Endpoints, Meraki
  - Business/Service name identifies a service to Threat Grid
- FA Client ID and Service Name are used to bind submissions to a TG Organization
  - Provides access to view in TG Cloud Portal if purchased
  - Provides the ability to see samples submitted by AMP-Enabled devices
  - Provides manual submissions, analysis and sample interactions (Glovebox)
  - Note: Threat Grid Entitlement Portal released for device management
- **Appliance Note**: These are also used to register devices on a TG Appliance
  - Device registers a new User at TGA with TG Client ID as the Username
  - This new User must be activated, otherwise TGA will not accept submissions

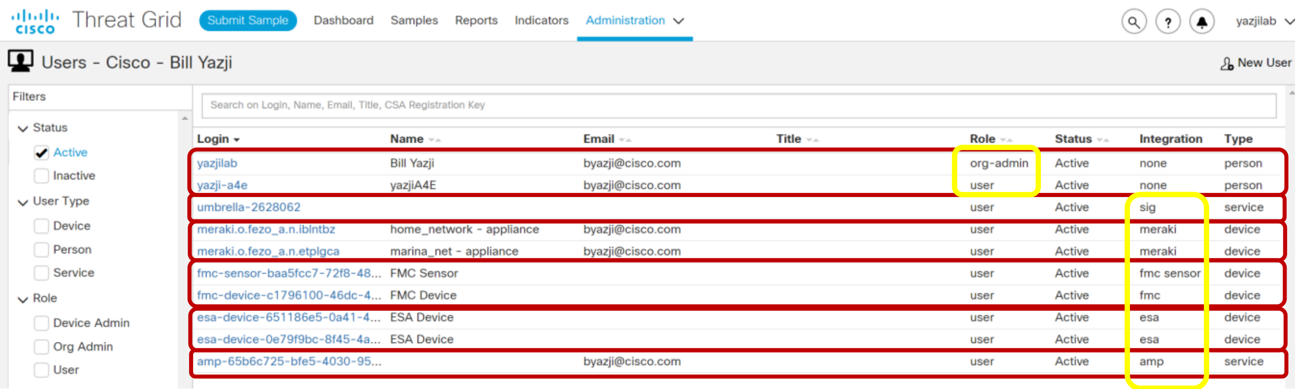
Integrated Connector Registration

AMP-Enabled Integration Registration to Threat Grid

- 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-secur.html
- Best to work with your Advanced Threat or Security account teams
  - Gather FA-IDs and Service Names
  - Group in Threat Grid Cloud organization (subscription) or Threat Grid Entitlement Portal organization (complimentary)
- tg-provisioning@cisco.com can also provide grouping assistance

Integrated Connector Registration

- Threat Grid
- Organizational view into AMP-Enabled devices and cloud users



Login	Name	Email	Title	Role	Status	Integration	Type
yazjilab	Bill Yazji	byazji@cisco.com		org-admin	Active	none	person
yazji-a4e	yazjiA4E	byazji@cisco.com		user	Active	none	person
umbrella-2628062				user	Active	sig	service
meraki.o.fezo_a.n.iblntbz	home_network - appliance	byazji@cisco.com		user	Active	meraki	device
meraki.o.fezo_a.n.etplgca	marina_net - appliance	byazji@cisco.com		user	Active	meraki	device
fmc-sensor-baa5fcc7-72f8-48...	FMC Sensor			user	Active	fmc sensor	device
fmc-device-c1796100-46dc-4...	FMC Device			user	Active	fmc	device
esa-device-651186e5-0a41-4...	ESA Device			user	Active	esa	device
esa-device-0e79f9bc-8f45-4a...	ESA Device			user	Active	esa	device
amp-65b6c725-bfe5-4030-95...		byazji@cisco.com		user	Active	amp	service

Integrated Connector Registration

Things to keep in mind

- Firewall rules can interfere with your device registering
- If a device is exchanged (hardware upgrade/return, etc) – you will need to add that back to Threat Grid and your organization manually
- Firepower Sensors 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 Threat Grid Portal
- Consider Threat Grid Cloud upgrade for full visibility
- Consider Threat Grid Entitlement Portal for device visibility vs. Group Reporting feature of WSA/ESA/CES

Recent Enhancements for AMP-Enabled Integrations

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

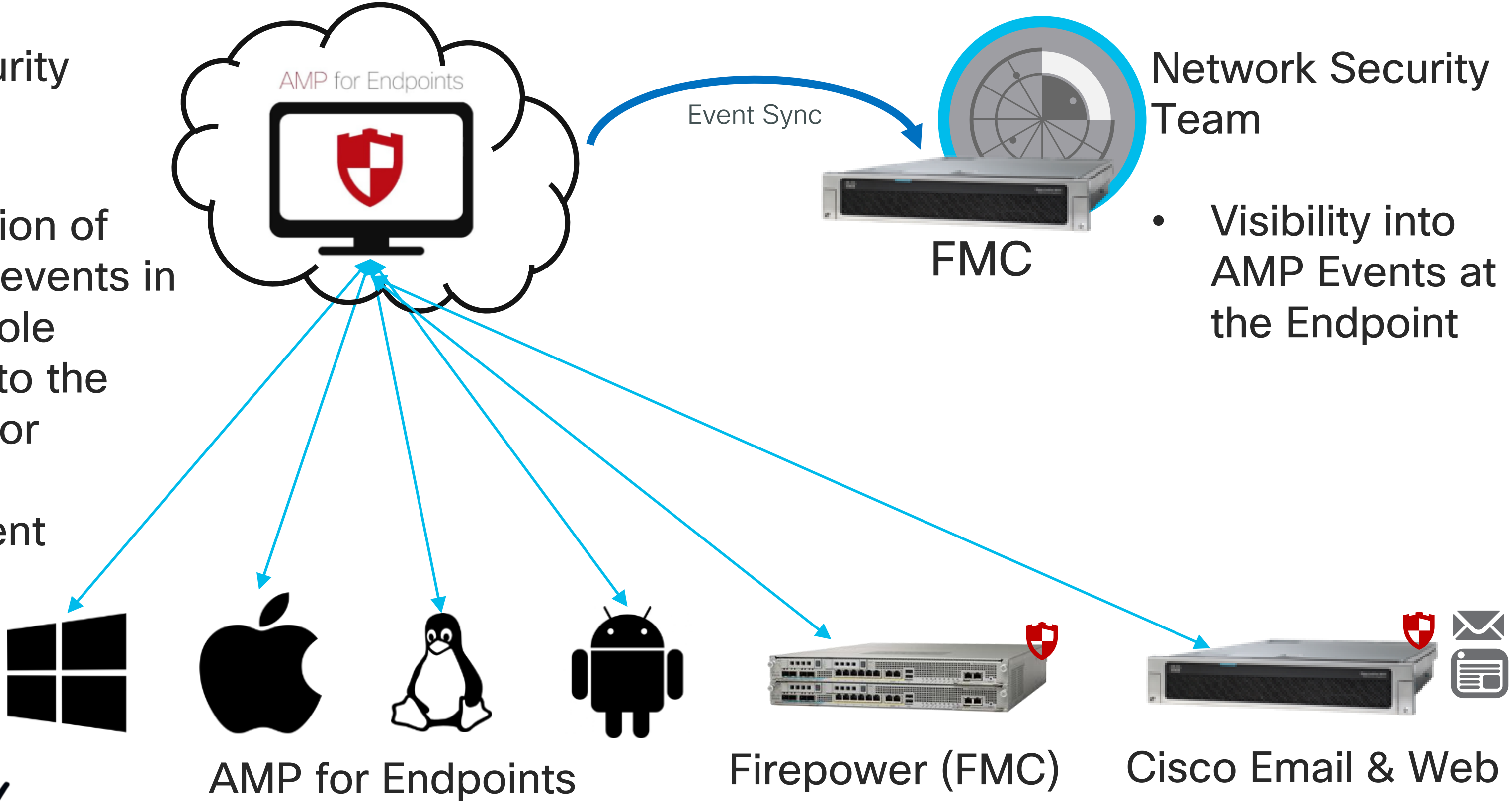
- I have a few of these products, how do they integrate?
- Wait, I can click once and block everywhere?

AMP Unity

Enhanced Operational Visibility and Control

Systems Security Team

- Consolidation of connector events in AMP Console
- Visibility into the threat vector
- A4E Policy Management



Network Security Team

- Visibility into AMP Events at the Endpoint

AMP Unity

Manages for Endpoints:
- Endpoint Policies
- Black & White Lists
- Exclusions

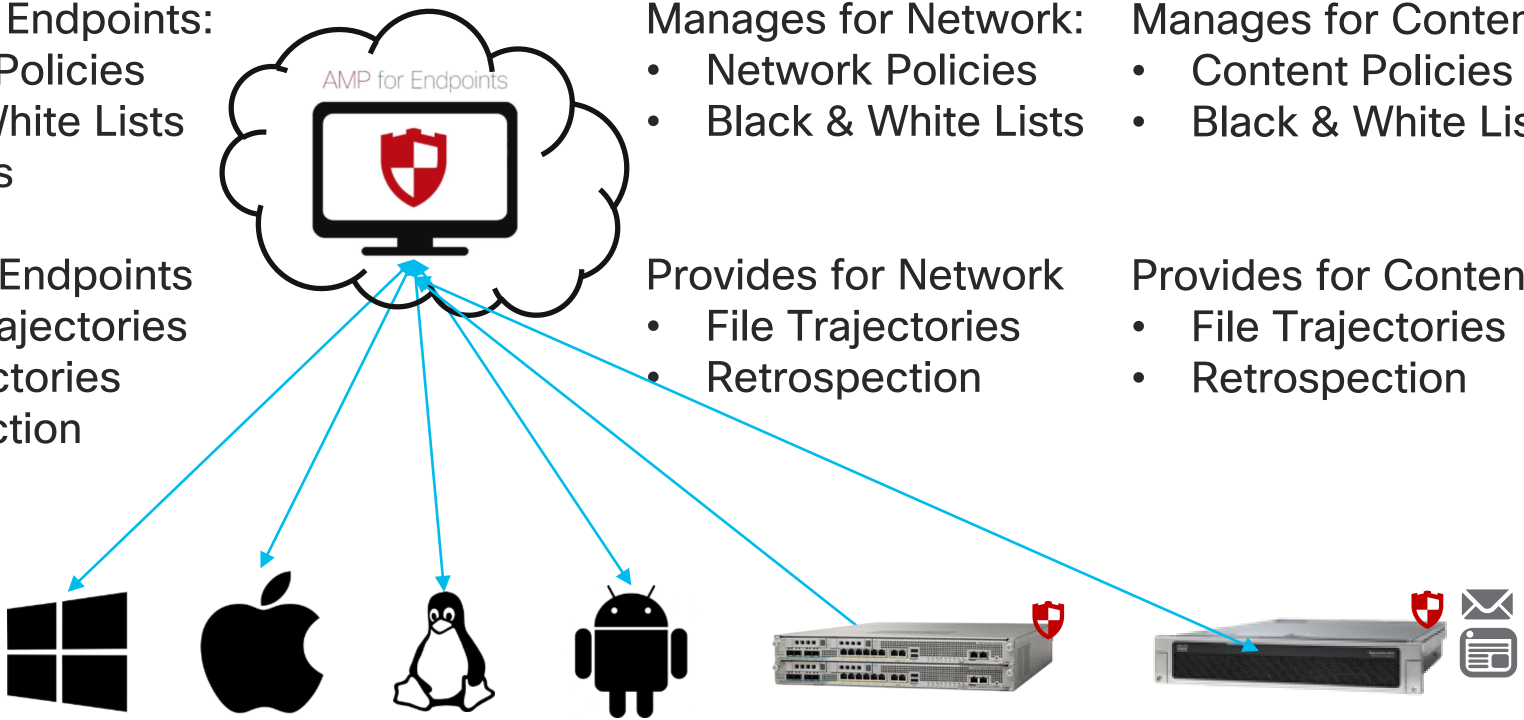
Provides for Endpoints
- Device Trajectories
- File Trajectories
- Retrospection

Manages for Network:
- Network Policies
- Black & White Lists

Provides for Network
- File Trajectories
- Retrospection

Manages for Content:
- Content Policies
- Black & White Lists

Provides for Content
- File Trajectories
- Retrospection

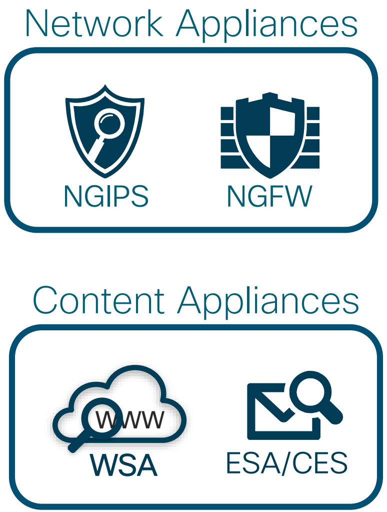


AMP for Endpoints

Firepower (FMC)

Cisco Email & Web

AMP Unity Functionality with Releases



Unity Support as of...	
AMP & Firepower Appliances	FMC 6.2
Email Security	AsyncOS 11.1
Web Security	AsyncOS 11.5

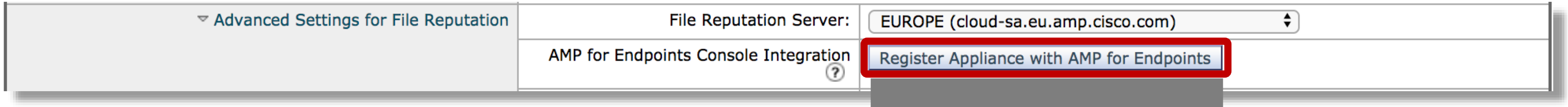
Global Outbreak Control
Simple Custom Detection (Blacklisting)
Whitelisting
Trajectories
File
Device

* See File & Device trajectory from all your AMP-enabled devices

Integrating Connectors into AMP Cloud

CES/ESA and WSA

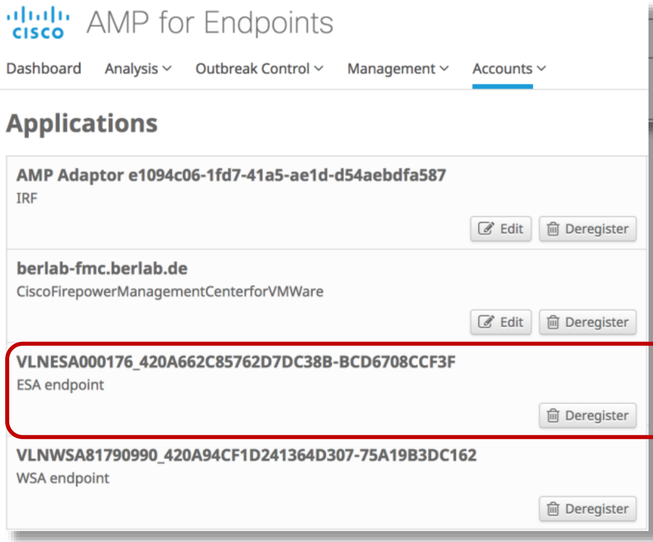
- AMP Client ID identifies individual file reputation checks per device
- Devices register with AMP Cloud using their individual AMP Client ID



▽ Advanced Settings for File Reputation

File Reputation Server: EUROPE (cloud-sa.eu.amp.cisco.com)

AMP for Endpoints Console Integration ⓘ



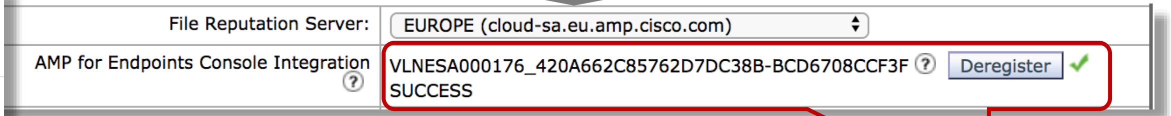
Applications

AMP Adaptor e1094c06-1fd7-41a5-ae1d-d54aebdfa587
IRF

berlab-fmc.berlab.de
CiscoFirepowerManagementCenterforVMWare

VLNESA000176_420A662C85762D7DC38B-BCD6708CCF3F
ESA endpoint

VLNWSA81790990_420A94CF1D241364D307-75A19B3DC162
WSA endpoint



File Reputation Server: EUROPE (cloud-sa.eu.amp.cisco.com)

AMP for Endpoints Console Integration ⓘ VLNESA000176_420A662C85762D7DC38B-BCD6708CCF3F ⓘ ✓
SUCCESS

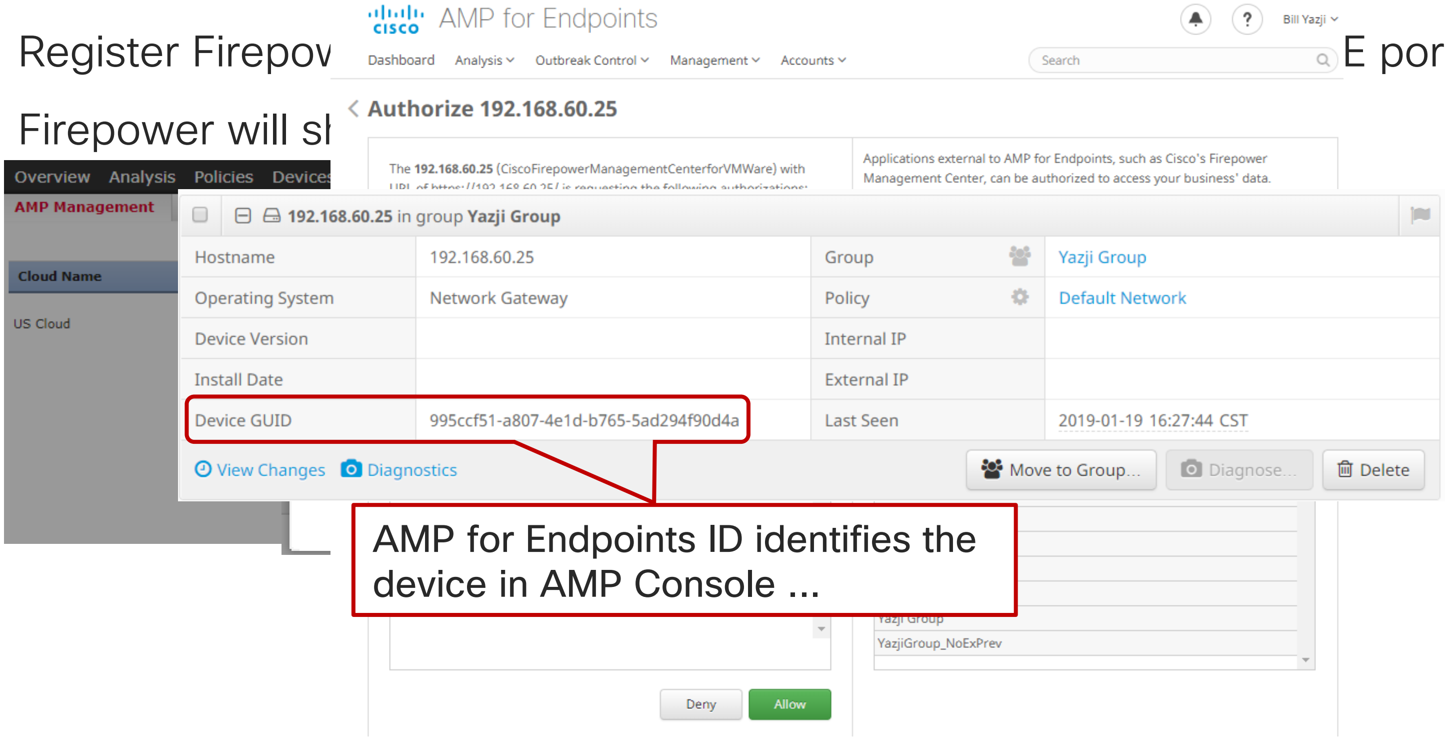
AMP for Endpoints ID identifies the device in AMP Console ...

... and shows up as an integrated application

Integrating Connectors into AMP Cloud

Firepower via FMC

- Register Firepov E portal)
- Firepower will sl



Authorize 192.168.60.25

The **192.168.60.25** (CiscoFirepowerManagementCenterforVMWare) with URL of https://192.168.60.25/ is requesting the following authorizations:

Applications external to AMP for Endpoints, such as Cisco's Firepower Management Center, can be authorized to access your business' data.

192.168.60.25 in group **Yazji Group**

Hostname	192.168.60.25	Group	Yazji Group
Operating System	Network Gateway	Policy	Default Network
Device Version		Internal IP	
Install Date		External IP	
Device GUID	995ccf51-a807-4e1d-b765-5ad294f90d4a	Last Seen	2019-01-19 16:27:44 CST

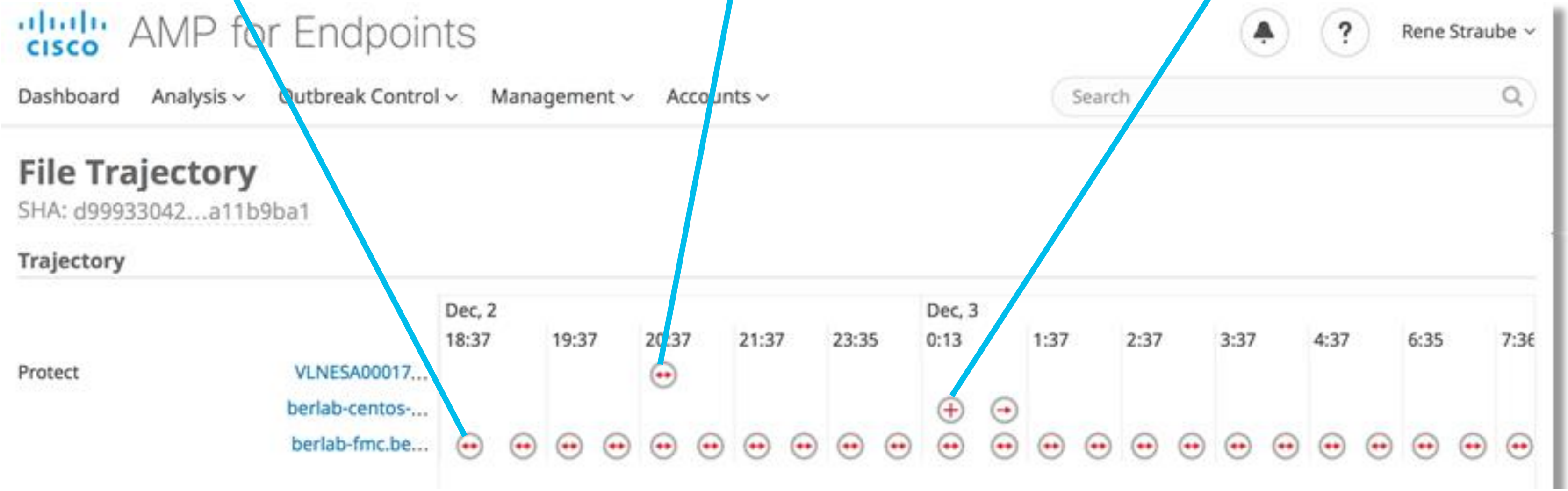
AMP for Endpoints ID identifies the device in AMP Console ...

AMP Unity – Full Visibility into the Threat Vector

First, it traversed the Firepower NGFW

Then it was observed on the Email Security Solution

And finally stored on the Endpoint



File Trajectory

SHA: d99933042...a11b9ba1

Trajectory

Dec, 2 18:37 | 19:37 | 20:37 | 21:37 | 23:35 | Dec, 3 0:13 | 1:37 | 2:37 | 3:37 | 4:37 | 6:35 | 7:36

Protect
- VLNESA00017...
- berlab-centos-...
- berlab-fmc.be...

Cisco Threat Response: Enhancing Incident Research & Response Capabilities

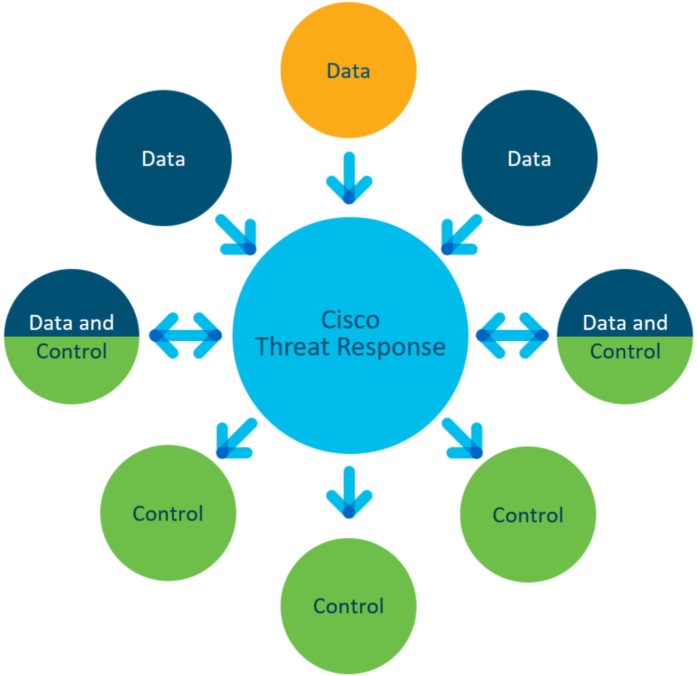
Questions you'll be able to answer after this section:

- Is Cisco protecting my company from the latest threats?
- Have we seen this threat in our environment yet?
- How do I access Cisco Threat Response?

Introducing Threat Response

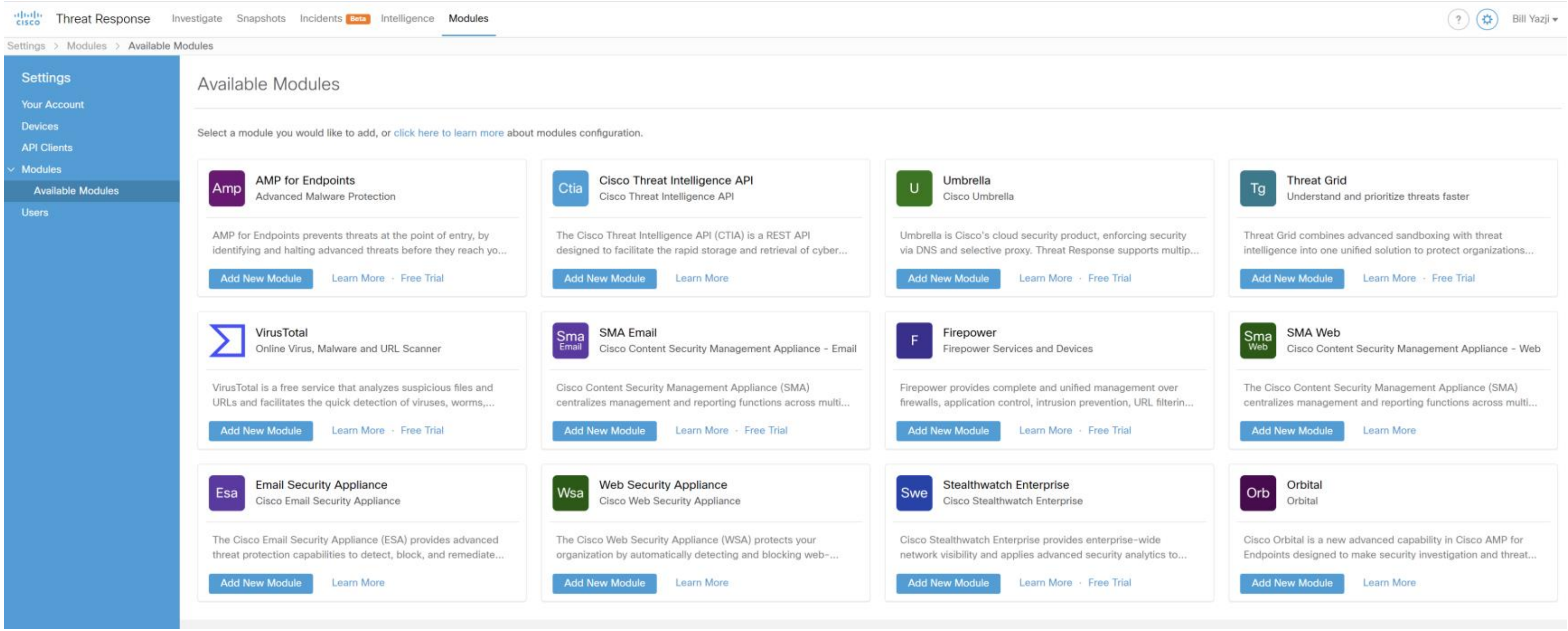
A new integrated Security Orchestration Enhancement

- Included with AMP for Endpoints, Threat Grid Cloud, ESA/CES (via SMA v12.1+), WSA, Umbrella, Firepower v6.4, Stealth Watch Enterprise
- Single Pane of Glass across multiple IR Tools
- Combines external Threat Intelligence and internal Log Data via Enrichment Modules
- External Threat Intelligence is integrated from Cisco and 3rd Party Sources
- Reduces Incident triage and Mitigation time by integrating various remediation actions



Threat Response

Enrichment Modules



Available Modules

Select a module you would like to add, or click here to learn more about modules configuration.

AMP for Endpoints – Advanced Malware Protection
AMP for Endpoints prevents threats at the point of entry, by identifying and halting advanced threats before they reach yo...
Add New Module · Learn More · Free Trial

Cisco Threat Intelligence API – Cisco Threat Intelligence API
The Cisco Threat Intelligence API (CTIA) is a REST API designed to facilitate the rapid storage and retrieval of cyber...
Add New Module · Learn More

Umbrella – Cisco Umbrella
Umbrella is Cisco's cloud security product, enforcing security via DNS and selective proxy. Threat Response supports multip...
Add New Module · Learn More · Free Trial

Threat Grid – Understand and prioritize threats faster
Threat Grid combines advanced sandboxing with threat intelligence into one unified solution to protect organizations...
Add New Module · Learn More · Free Trial

VirusTotal – Online Virus, Malware and URL Scanner
VirusTotal is a free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms,...
Add New Module · Learn More · Free Trial

SMA Email – Cisco Content Security Management Appliance - Email
Cisco Content Security Management Appliance (SMA) centralizes management and reporting functions across multi...
Add New Module · Learn More · Free Trial

Firepower – Firepower Services and Devices
Firepower provides complete and unified management over firewalls, application control, intrusion prevention, URL filterin...
Add New Module · Learn More · Free Trial

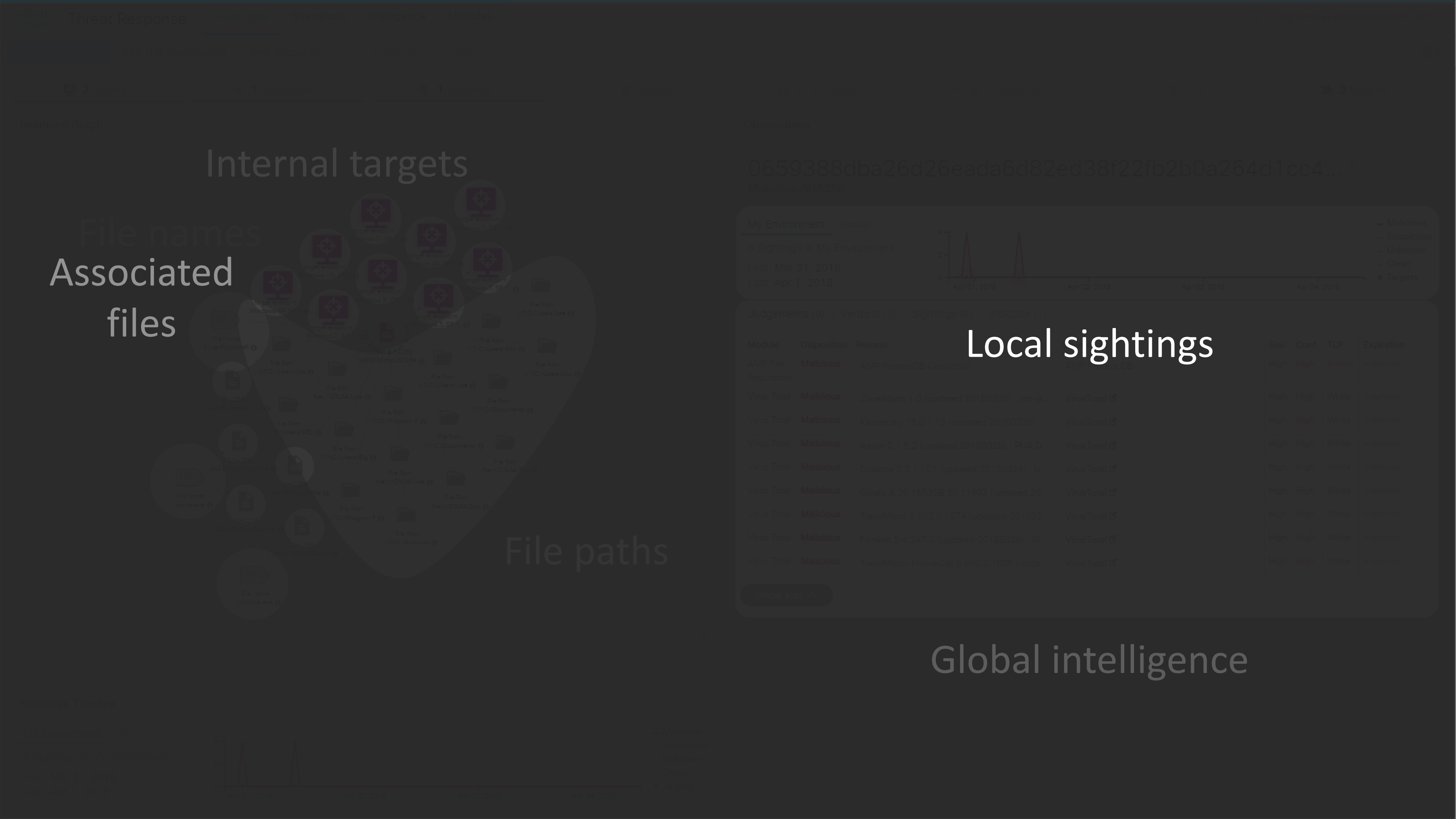
SMA Web – Cisco Content Security Management Appliance - Web
The Cisco Content Security Management Appliance (SMA) centralizes management and reporting functions across multi...
Add New Module · Learn More

Email Security Appliance – Cisco Email Security Appliance
The Cisco Email Security Appliance (ESA) provides advanced threat protection capabilities to detect, block, and remediate...
Add New Module · Learn More

Web Security Appliance – Cisco Web Security Appliance
The Cisco Web Security Appliance (WSA) protects your organization by automatically detecting and blocking web-...
Add New Module · Learn More

Stealthwatch Enterprise – Cisco Stealthwatch Enterprise
Cisco Stealthwatch Enterprise provides enterprise-wide network visibility and applies advanced security analytics to...
Add New Module · Learn More · Free Trial

Orbital – Orbital
Cisco Orbital is a new advanced capability in Cisco AMP for Endpoints designed to make security investigation and threat...
Add New Module · Learn More



Internal targets

File names

Associated files

File paths

Local sightings

Global intelligence

Observables

0659388dba26d26eada6d82ed38f22fb2b0a264d1cc4...

Malicious SHA256

My Environment Global

8 Sightings in My Environment

First: Mar 31, 2018

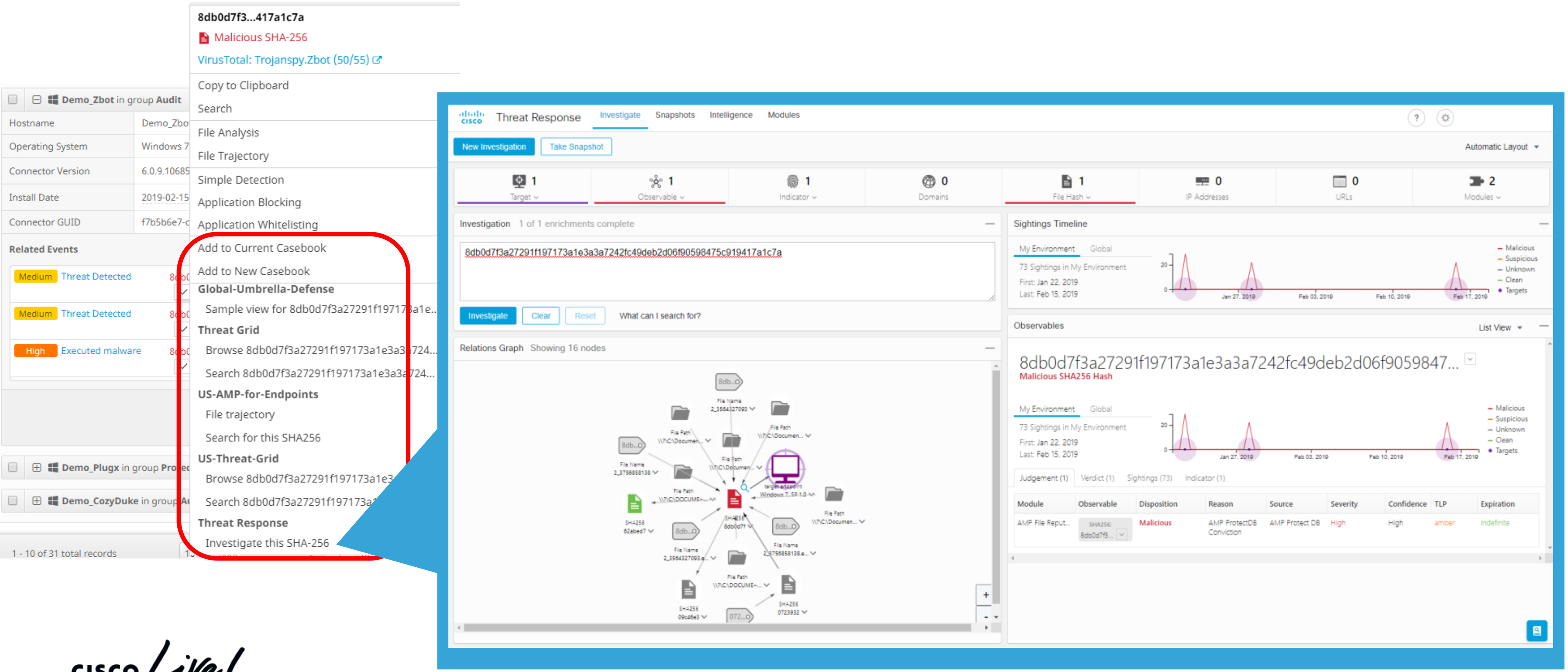
Last: Apr 1, 2018

Judgements (9) Verdicts (2) Sightings (8) Indicator (1)

Module	Disposition	Reason		Sev.	Conf.	TLP	Expiration
AMP File Reputation	Malicious	AMP ProtectDB Conviction	AMP Protect DB	High	High	Amber	Indefinite
Virus Total	Malicious	ZoneAlarm 1.0 (updated 20180329) - not-a...	VirusTotal	High	High	White	Indefinite
Virus Total	Malicious	Kaspersky 15.0.1.13 (updated 20180329) ...	VirusTotal	High	High	White	Indefinite
Virus Total	Malicious	Ikarus 0.1.5.2 (updated 20180328) - PUA.O...	VirusTotal	High	High	White	Indefinite
Virus Total	Malicious	Cylance 2.3.1.101 (updated 20180329) - U...	VirusTotal	High	High	White	Indefinite
Virus Total	Malicious	GData A:25.16535B:25.11903 (updated 20...	VirusTotal	High	High	White	Indefinite
Virus Total	Malicious	TrendMicro 9.862.0.1074 (updated 201803...	VirusTotal	High	High	White	Indefinite
Virus Total	Malicious	Fortinet 5.4.247.0 (updated 20180329) - Ri...	VirusTotal	High	High	White	Indefinite
Virus Total	Malicious	TrendMicro-HouseCall 9.950.0.1006 (upda...	VirusTotal	High	High	White	Indefinite

Threat Response Integration

AMP for Endpoints



Hostname	Demo_Zbo
Operating System	Windows 7
Connector Version	6.0.9.10685
Install Date	2019-02-15
Connector GUID	f7b5b6e7-c

8db0d7f3a27291f197173a1e3a3a7242fc49deb2d06f90598475c919417a1c7a

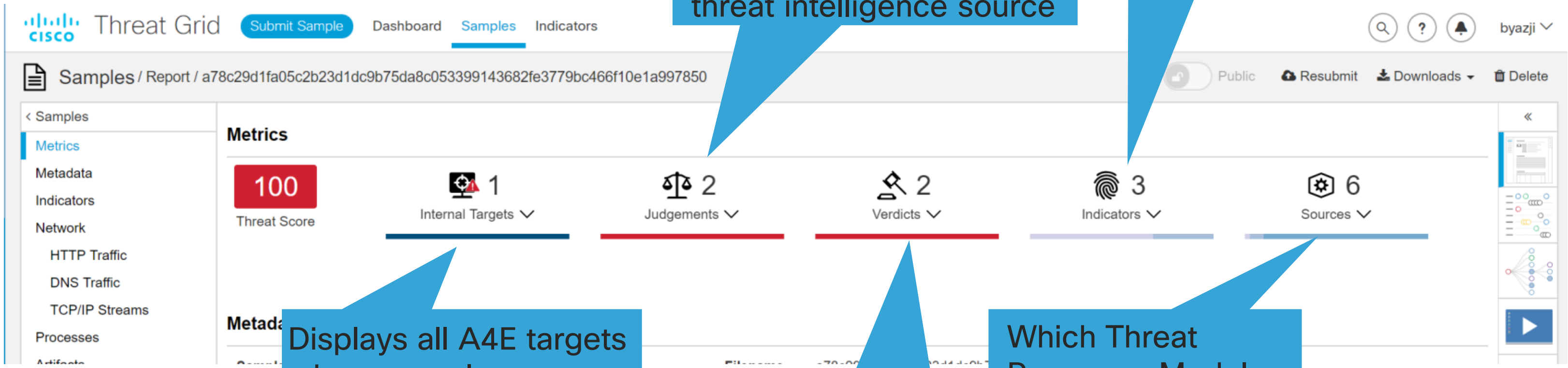
73 Sightings in My Environment
First: Jan 22, 2019
Last: Feb 15, 2019

8db0d7f3a27291f197173a1e3a3a7242fc49deb2d06f9059847...

Module	Observable	Disposition	Reason	Source	Severity	Confidence	TLP	Expiration
AMP File Reput...	SHA256: 8db0d7f3...	Malicious	AMP ProtectDB Conviction	AMP Protect DB	High	High	amber	Indefinite

Threat Response Integration

Threat Grid “info bar”



Patterns of behavior or a set of conditions which indicate malicious behavior

Single ruling of an observable from one threat intelligence source

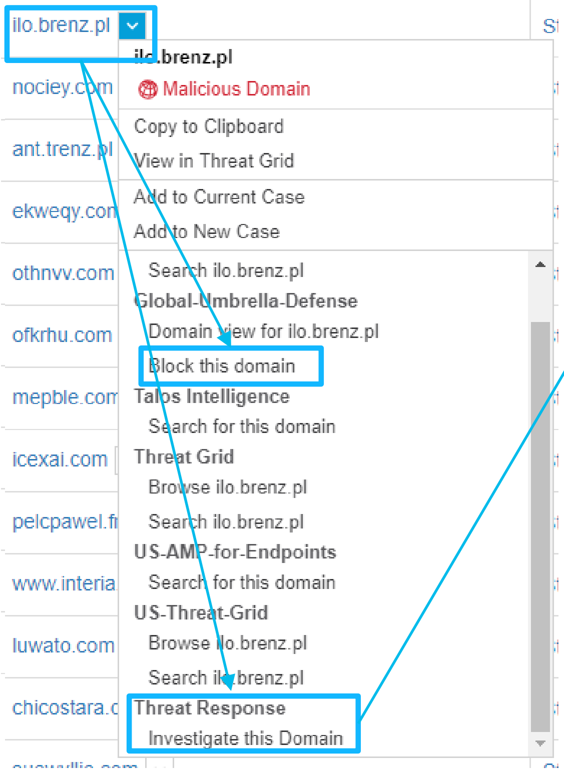
Displays all A4E targets where sample was seen

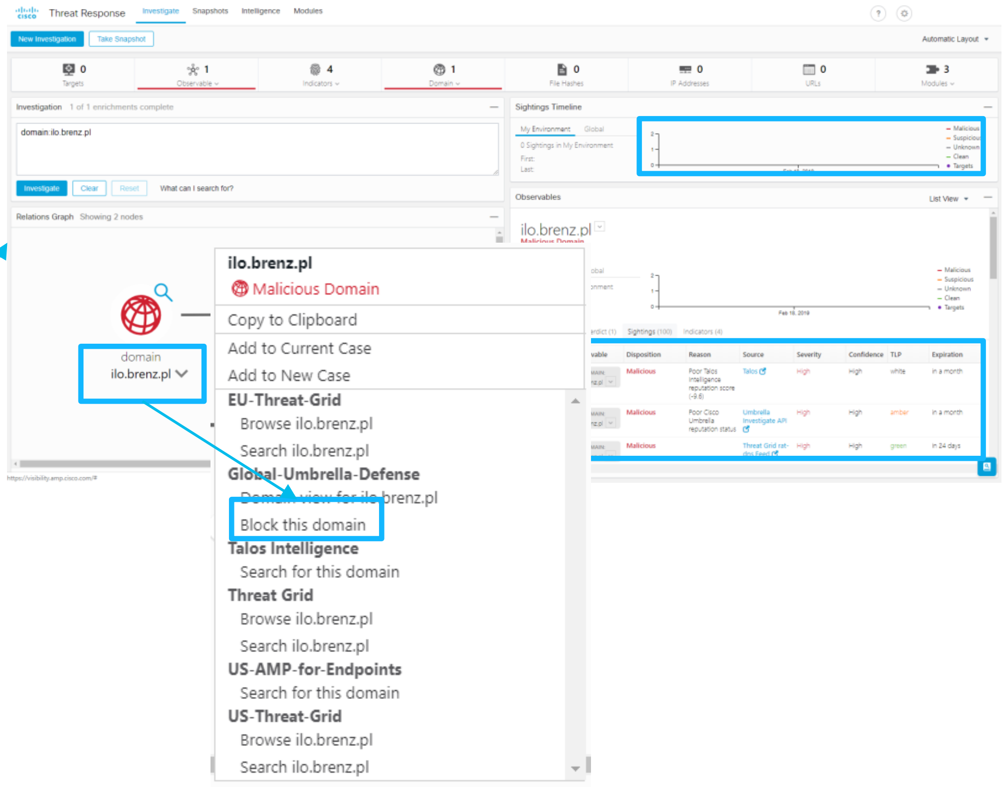
Which Threat Response Module contributed

Highest-priority judgement on that observable from that source

Threat Response Integration

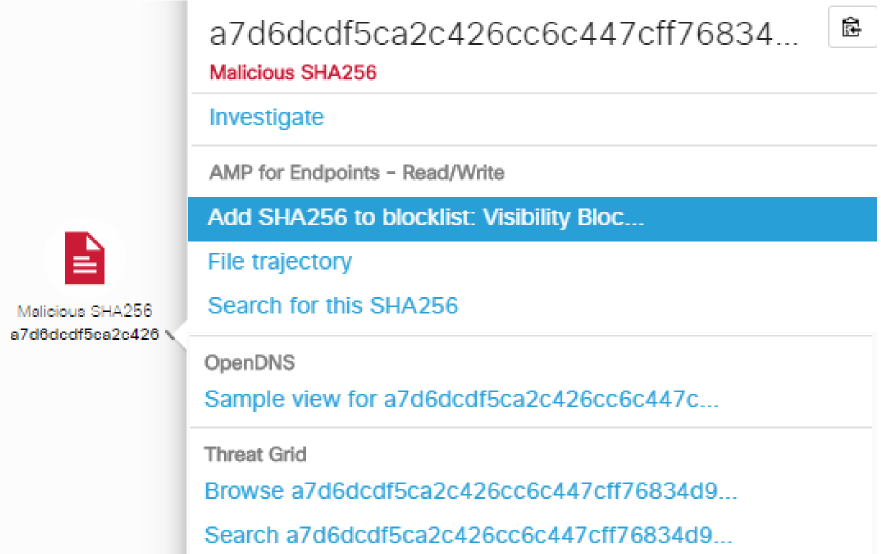
Threat Grid Observables





Disposition	Reason	Source	Severity	Confidence	TLP	Expiration
Malicious	Poor Talos Intelligence reputation score (-9.6)	Talos	High	High	white	in a month
Malicious	Poor Cisco Umbrella reputation status	Umbrella Investigate API	High	High	amber	in a month
Malicious		Threat Grid rat-dns Feed	High	High	green	in 24 days

Immediately take mitigating action from pivot menu



Malicious SHA256
a7d6dcdf5ca2c426

a7d6dcdf5ca2c426cc6c447cff76834...

Malicious SHA256

Investigate

AMP for Endpoints - Read/Write

Add SHA256 to blocklist: Visibility Bloc...

File trajectory

Search for this SHA256

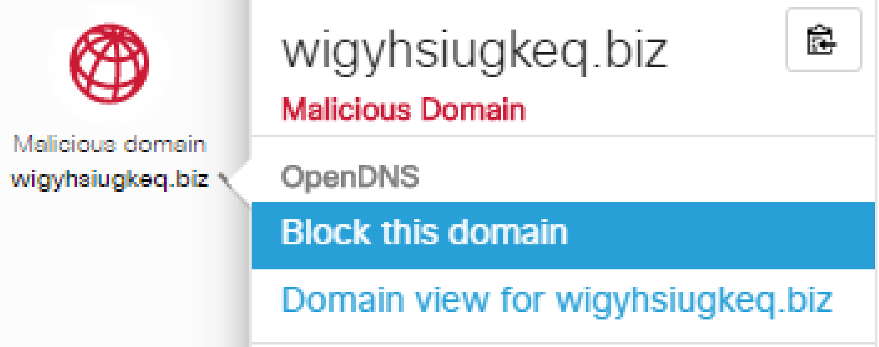
OpenDNS

Sample view for a7d6dcdf5ca2c426cc6c447c...

Threat Grid

Browse a7d6dcdf5ca2c426cc6c447cff76834d9...

Search a7d6dcdf5ca2c426cc6c447cff76834d9...



Malicious domain
wigyhsiugkeq.biz

wigyhsiugkeq.biz

Malicious Domain

OpenDNS

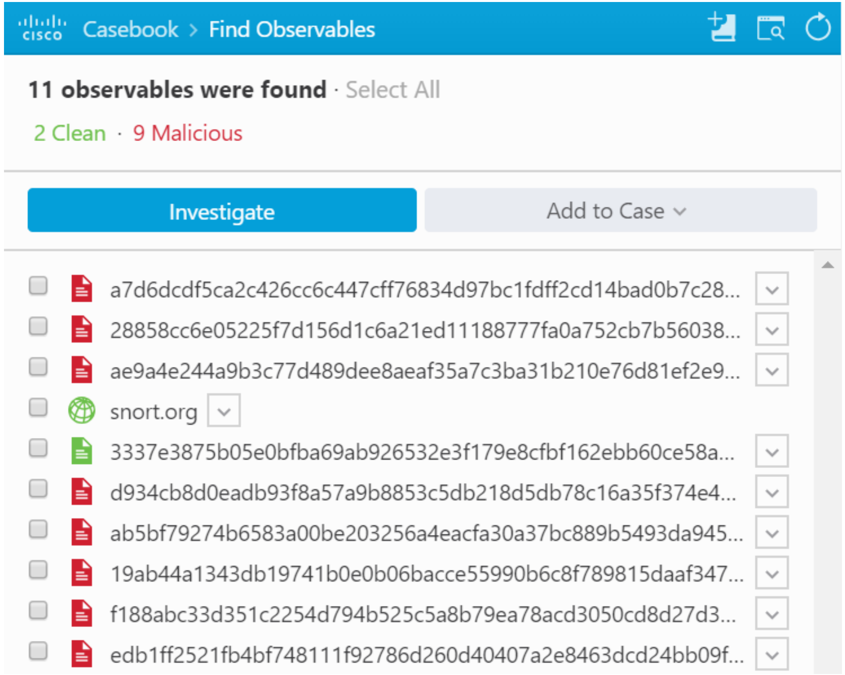
Block this domain

Domain view for wigyhsiugkeq.biz

Browser plugin for Cisco Threat Response

Overview

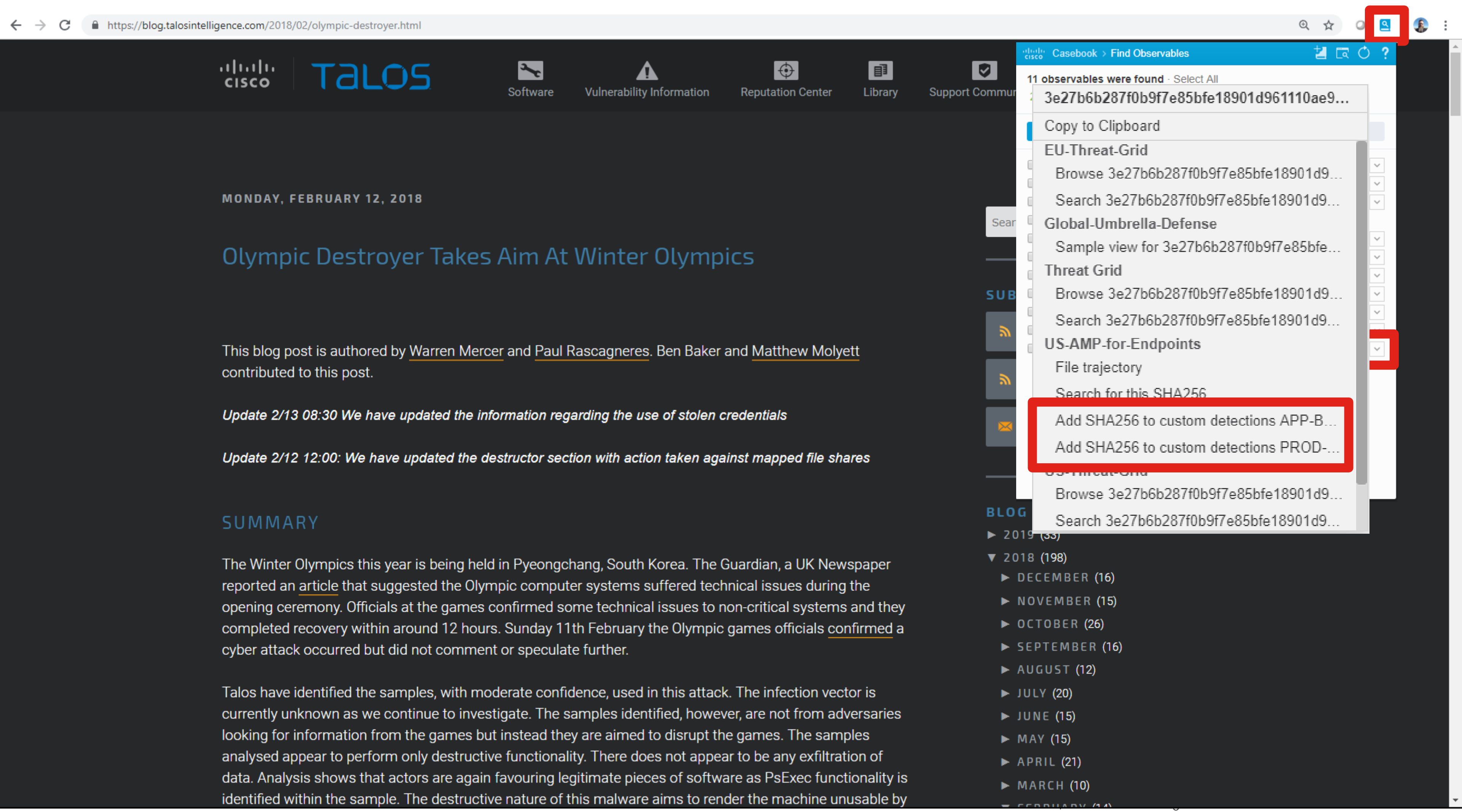
1. Pull observables from the contents of any web page, Cisco or 3rd party web-based console
2. Immediately gives you the current verdicts on each observable
3. Access the Threat Response pivot menu, where you can block a SHA or domain, without ever leaving the page
4. Pivot into the Threat Response investigate UI with the set of selected observables



11 observables were found · Select All

2 Clean · 9 Malicious

- □ a7d6dcdf5ca2c426cc6c447cff76834d97bc1fdff2cd14bad0b7c28...
- □ 28858cc6e05225f7d156d1c6a21ed11188777fa0a752cb7b56038...
- □ ae9a4e244a9b3c77d489dee8aeaf35a7c3ba31b210e76d81ef2e9...
- □ snort.org
- □ 3337e3875b05e0bfba69ab926532e3f179e8cfbf162ebb60ce58a...
- □ d934cb8d0eadb93f8a57a9b8853c5db218d5db78c16a35f374e4...
- □ ab5bf79274b6583a00be203256a4eacfa30a37bc889b5493da945...
- □ 19ab44a1343db19741b0e0b06bacce55990b6c8f789815daaf347...
- □ f188abc33d351c2254d794b525c5a8b79ea78acd3050cd8d27d3...
- □ edb1ff2521fb4bf748111f92786d260d40407a2e8463dcd24bb09f...


https://blog.talosintelligence.com/2018/02/olympic-destroyer.html
cisco
Talos
Software
Vulnerability Information
Reputation Center
Library
Support Commu
Casebook > Find Observables
11 observables were found · Select All
3e27b6b287f0b9f7e85bfe18901d961110ae9...
Copy to Clipboard
EU-Threat-Grid
Browse 3e27b6b287f0b9f7e85bfe18901d9...
Search 3e27b6b287f0b9f7e85bfe18901d9...
Global-Umbrella-Defense
Sample view for 3e27b6b287f0b9f7e85bfe...
Threat Grid
Browse 3e27b6b287f0b9f7e85bfe18901d9...
Search 3e27b6b287f0b9f7e85bfe18901d9...
US-AMP-for-Endpoints
File trajectory
Search for this SHA256
Add SHA256 to custom detections APP-B...
Add SHA256 to custom detections PROD-...
US-Threat-Grid
Browse 3e27b6b287f0b9f7e85bfe18901d9...
Search 3e27b6b287f0b9f7e85bfe18901d9...
Sear
SUB
BLOG
▶ 2019 (33)
▼ 2018 (198)
▶ DECEMBER (16)
▶ NOVEMBER (15)
▶ OCTOBER (26)
▶ SEPTEMBER (16)
▶ AUGUST (12)
▶ JULY (20)
▶ JUNE (15)
▶ MAY (15)
▶ APRIL (21)
▶ MARCH (10)

MONDAY, FEBRUARY 12, 2018

Olympic Destroyer Takes Aim At Winter Olympics

This blog post is authored by Warren Mercer and Paul Rascagneres. Ben Baker and Matthew Molyett contributed to this post.

Update 2/13 08:30 We have updated the information regarding the use of stolen credentials

Update 2/12 12:00: We have updated the destructor section with action taken against mapped file shares

SUMMARY

The Winter Olympics this year is being held in Pyeongchang, South Korea. The Guardian, a UK Newspaper reported an article that suggested the Olympic computer systems suffered technical issues during the opening ceremony. Officials at the games confirmed some technical issues to non-critical systems and they completed recovery within around 12 hours. Sunday 11th February the Olympic games officials confirmed a cyber attack occurred but did not comment or speculate further.

Talos have identified the samples, with moderate confidence, used in this attack. The infection vector is currently unknown as we continue to investigate. The samples identified, however, are not from adversaries looking for information from the games but instead they are aimed to disrupt the games. The samples analysed appear to perform only destructive functionality. There does not appear to be any exfiltration of data. Analysis shows that actors are again favouring legitimate pieces of software as PsExec functionality is identified within the sample. The destructive nature of this malware aims to render the machine unusable by

For your viewing pleasure...

- Cisco Security APIs and Scripts
  - https://github.com/CiscoSecurity
- Cisco Threat Response Plugins
  - http://cs.co/CTR4Chrome & http://cs.co/CTR4Firefox
- Cisco Threat Response Supported Modules
  - http://cs.co/ctr_modules
- AMP Cloud and Threat Grid 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/

Threat Grid Cloud Demo if time permits

(warning: a live demo at Cisco Live…)

Questions?

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

Continue your education

Demos in the Cisco campus

Walk-in self-paced labs

Meet the engineer 1:1 meetings

Related sessions

Thank you

You make **possible**