



Possibilities

#CiscoLive

Endpoint Security

Your Last Line of Defense

Brian McMahon

Technical Marketing Engineer, Advanced Threat Solutions

DGTL-BRKSEC-3446

CISCO *Live!*

June 2-3, 2020 | ciscolive.com/us

#CiscoLive



#whoami

Brian McMahon

brmcmaho@cisco.com

Technical Marketing Engineer,
Advanced Threat Solutions team

Currently working with AMP,
Threat Grid, SecureX, security
integrations, with a focus on
improved incident response
workflows.

First Cisco job: TAC 1996-1999

First incident response: circa
1993 on a VAXcluster



Agenda

- Why endpoint security?
 - Protecting the human
- AnyConnect
 - It's not just for VPN
- AMP for Endpoints
 - The nuts and bolts
- Endpoint security in context
 - What about the rest of your network?



Why Endpoint Security?



Agenda

- Why endpoint security?
 - Protecting the human
- AnyConnect
 - It's not just for VPN
- AMP for Endpoints
 - The nuts and bolts
- Endpoint security in context
 - What about the rest of your network?

Why Endpoint Security?

Why focus on endpoint security, when everyone is talking about “new” identity and trust-based approaches to security like *Zero Trust Architecture (ZTA)* or Google’s *BeyondCorp*?

Why Zero Trust?

- “Don’t worry, we’re secure – we’re behind the firewall!”
- It never really worked that way, and **definitely** doesn’t any more.
- We’ve accumulated years (or decades) of implicit assumptions about trust.

Trust-centric security models

- Turn the security model inside-out.
 - Establishing micro-perimeters
 - Provide the RIGHT access to the RIGHT data at the RIGHT time, only:
 - Validate User is Trusted
 - **Validate Endpoint is Trusted**
- Endpoint Security is critical to Threat-Centric & Trust-Centric approaches alike.

Complementary security approaches

Not one or the other



Threat-Centric

Basic level of security maturity to prevent attacks via an intelligence-based policy – then detect, investigate, and remediate

Dynamic Context



Trust-Centric

Good security practice to verify before granting access via a identity-based policy – for any user, any device, any app, in any location

The Goal of Any Attacker
Is to **Gain Access**



- More than 80% of data breaches result from an attacker logging into a customer's applications using stolen passwords—often due to phishing.

Protect the Business



Our #1 Responsibility Is to Protect the Business

- A business is comprised of the **people** who make it happen.
- Those people use **devices** to interact with our business.
- Ergo: we must protect our people and the devices they use.

Infrastructure

Network



Firepower
ASA



Stealthwatch

Corporate Assets

Desktops, Servers



AMP for
Endpoints



AnyConnect

Employees

People



Umbrella



Duo

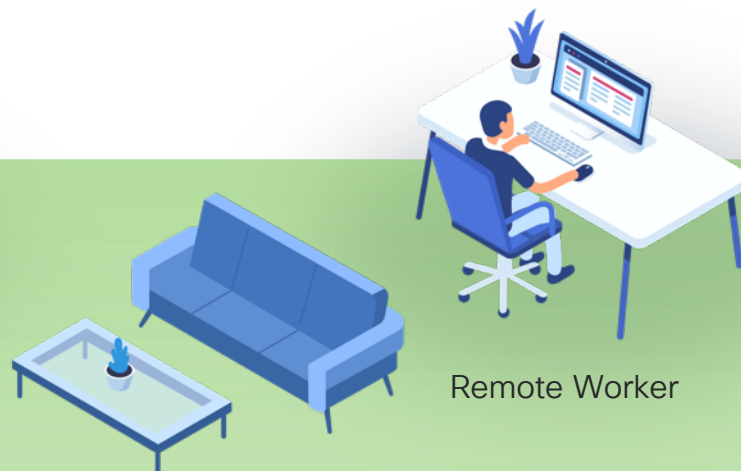
The Endpoint Is the Last Line of Defense



Image source: https://commons.wikimedia.org/wiki/File:Soccer_goalkeeper.jpg (public domain)

The Endpoint Is the Last Line of Defense, and the Last Chance to See or Stop Anything

- Encryption is becoming pervasive.
- We cannot decrypt everything.
 - We must be on the endpoint to have visibility.
- The endpoint is often the target of the attack.
- The endpoint is where the attacker can best exploit the human.



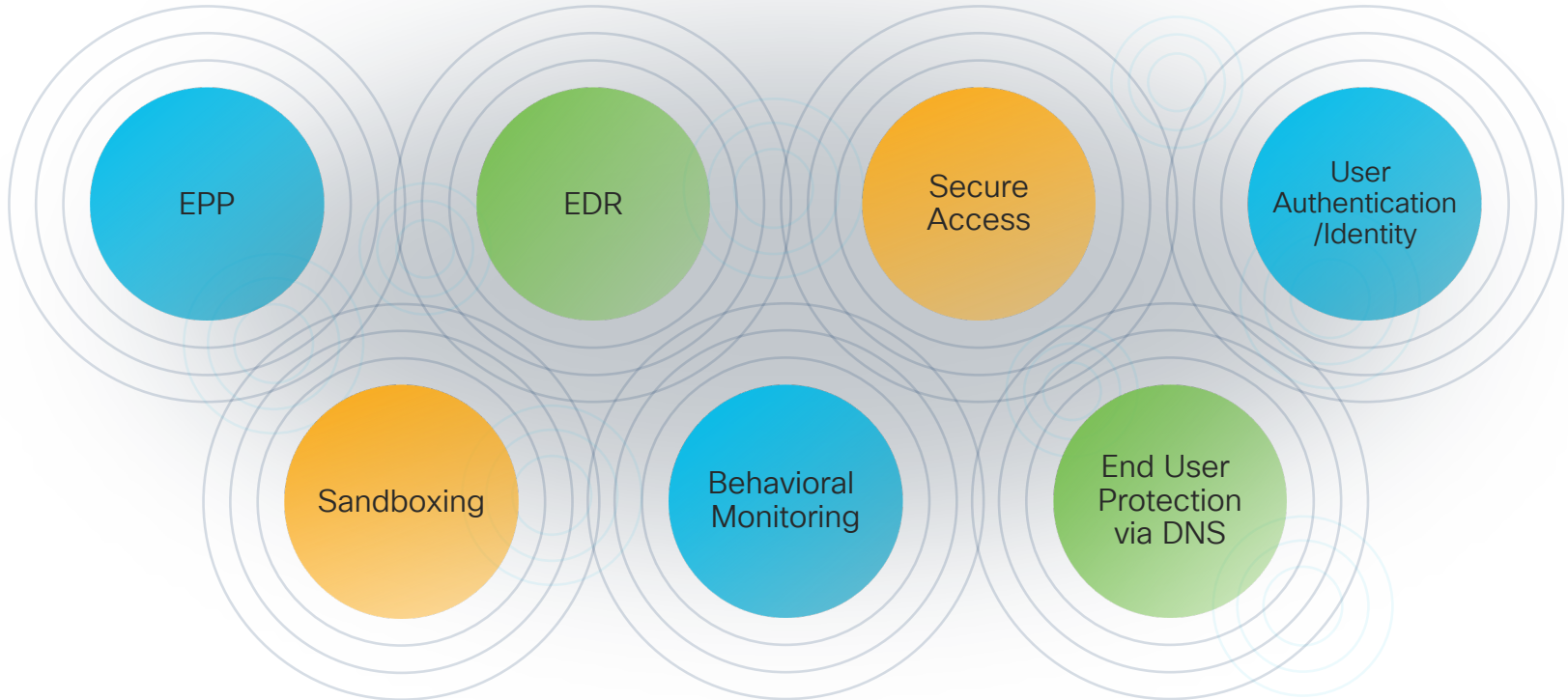
Example: Ransomware Is Still Prevalent

- Endpoint focused malware, such as Ransomware, is still in the wild and a major problem.
- Ransomware continues to evolve, both in its techniques and in its business model.
- We still see “SQL Slammer” once in a while, if you can believe that!

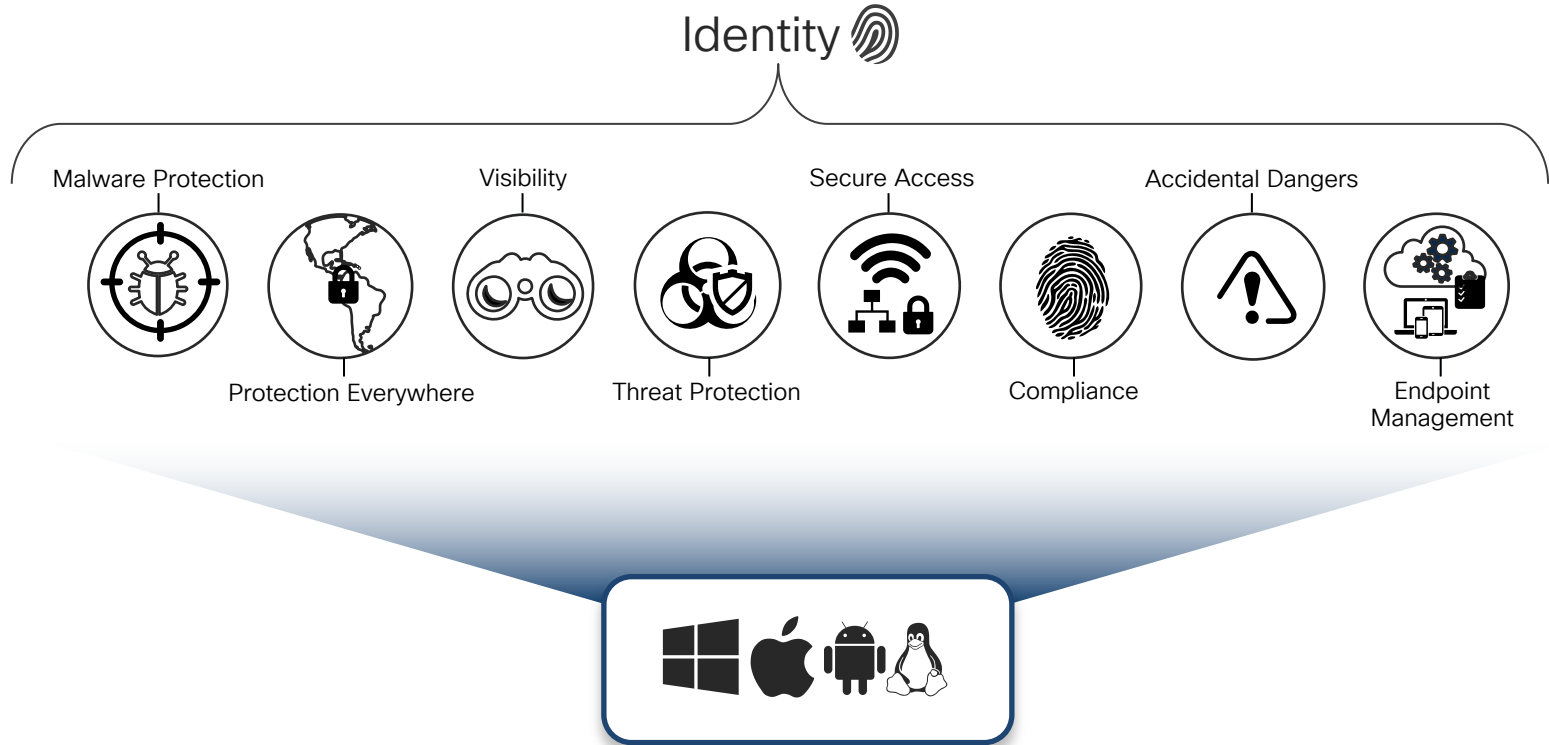


Endpoint Security:

A Broad & Fragmented Market



Generalized endpoint security strategy






AnyConnect

CISCO *Live!*



Agenda

- Why endpoint security?
 - Protecting the human
- AnyConnect
 - It's not just for VPN
- AMP for Endpoints
 - The nuts and bolts
- Endpoint security in context
 - What about the rest of your network?



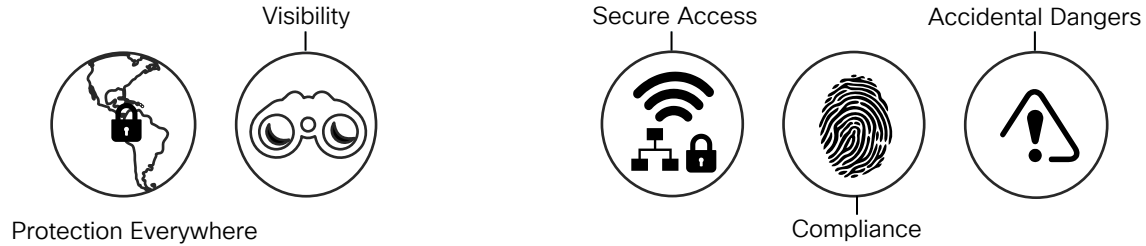
180+ million endpoints delivering the most
comprehensive set of security services to more than
80,000+ customers worldwide



*is
more
than*



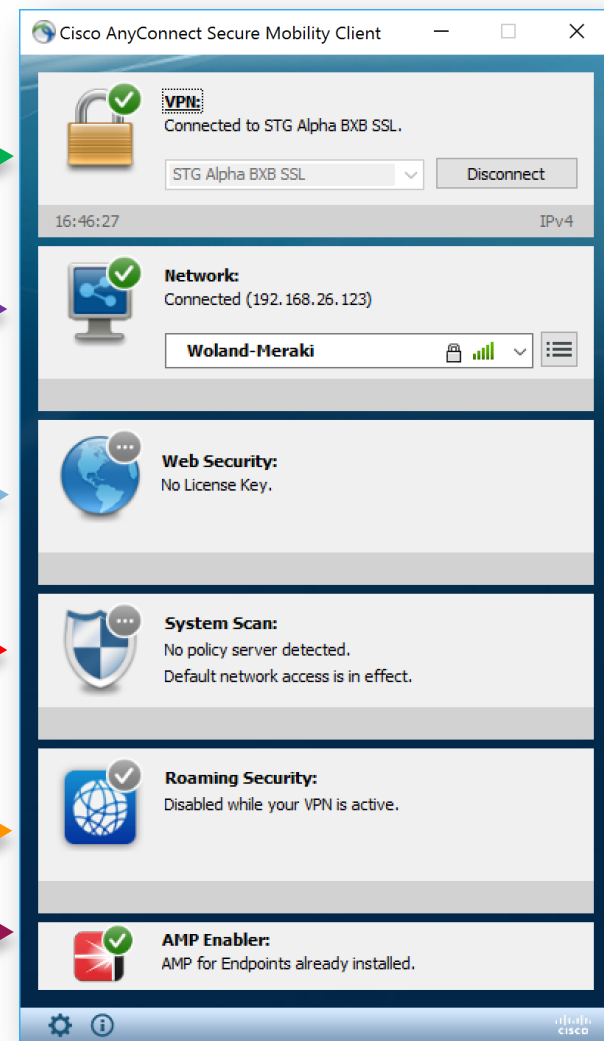
Yes, AnyConnect can do that!



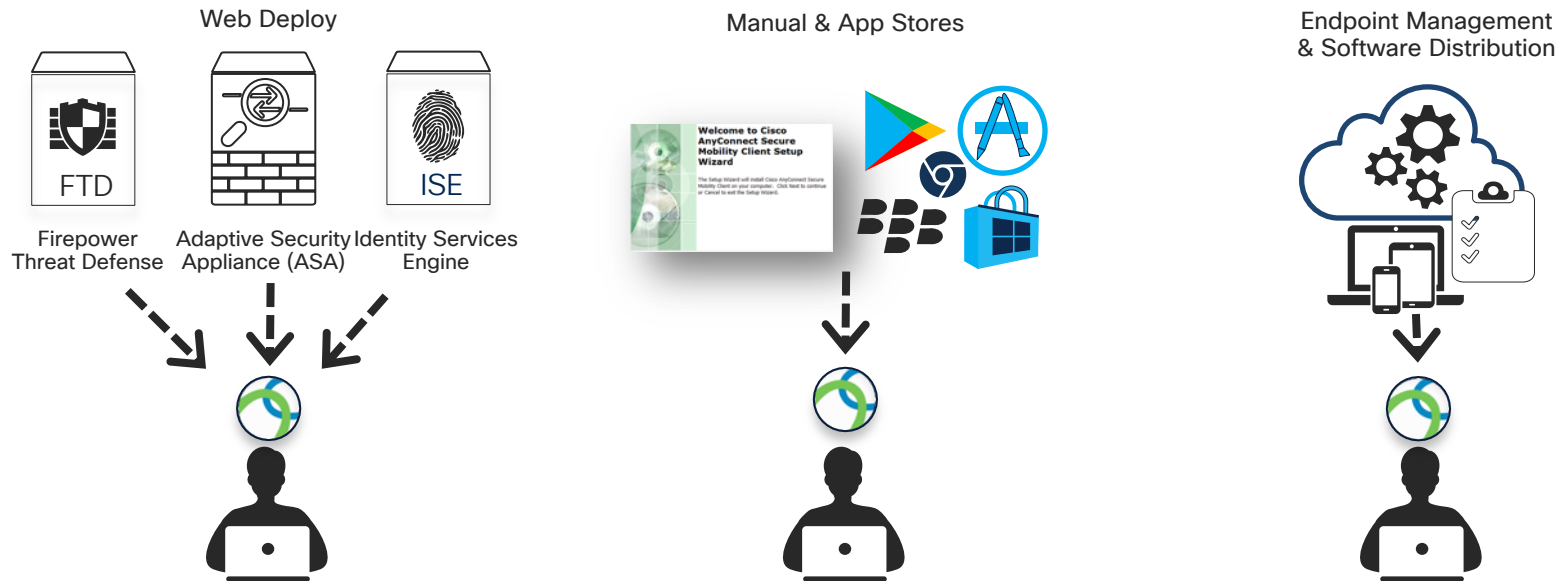
Cisco AnyConnect

suite of security service enablement modules

- VPN Module (Core)
- Network Access Manager (NAM)
- ~~Web Security (GWS) (Umbrella SIG)~~
- Posture
- Umbrella Module
- HostScan (aka: ASA posture) (No UI)
- Network Visibility Module (NVM) (No UI)
- AMP Enabler Module
- Diagnostics and Reporting Tool (DART)



Deploying, Distributing Policy & Updating AnyConnect



Benefits

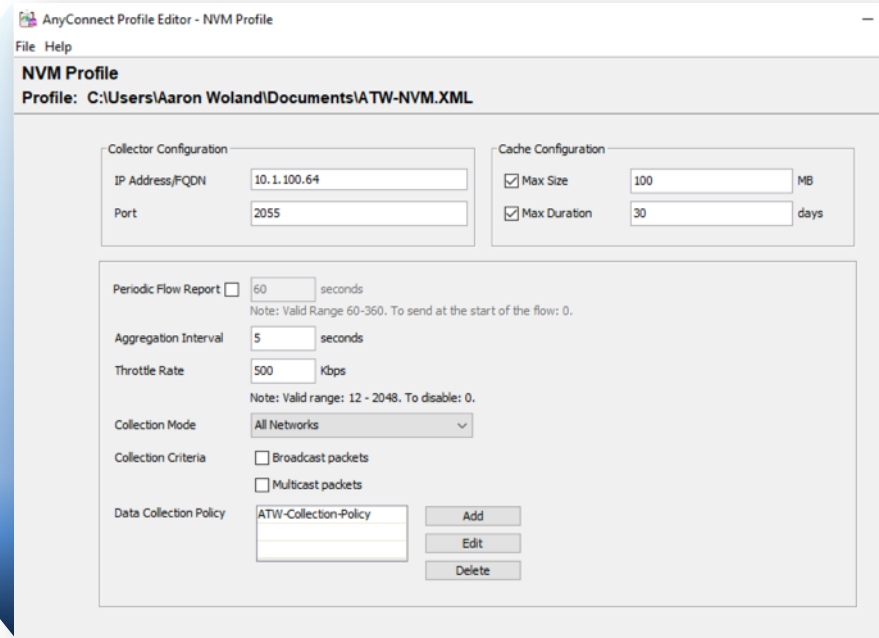
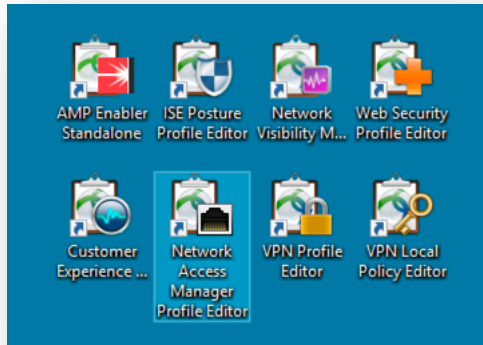
- Flexible Options for Deployments
- Greater Control over Correct Versions
- Dynamically Update Policies on Endpoint
- Simple to add / remove / change AC Modules

Capabilities

- Headend Deployment from ASA, FTN and/or ISE
- AC Installed with Software Managers (SMS/SCCM)
- Manual Install per OS
- Mobile Users can install from App Stores

Cisco AnyConnect

Profiles for the modules – standalone profile editors



Cisco AnyConnect

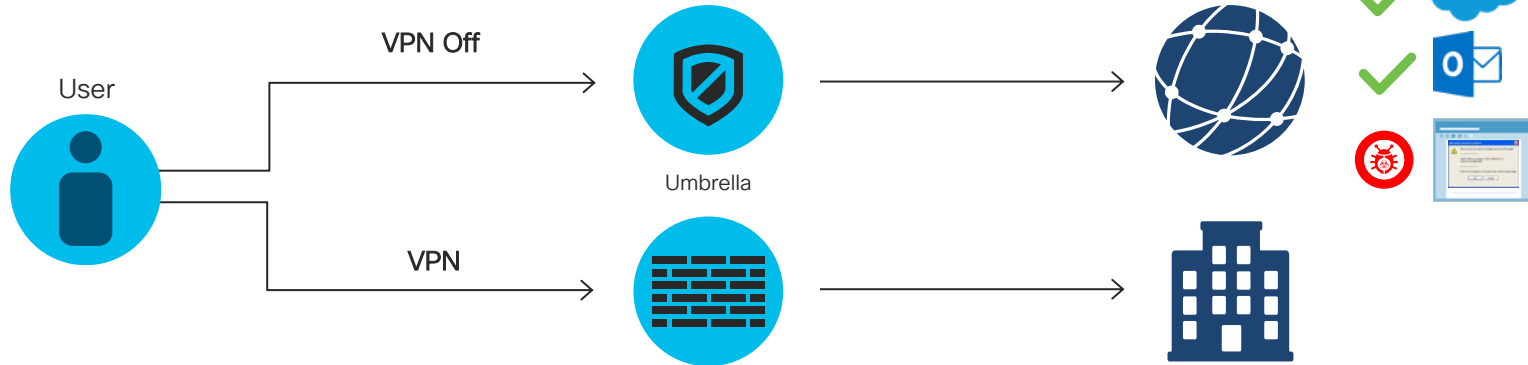
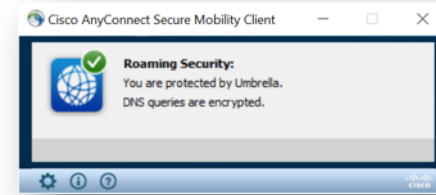
Profiles for the modules – ASDM

The screenshot displays the Cisco ASDM 7.9(1) interface for configuring an AnyConnect Client Profile. The main window is titled "Profile: atw-core-asa-profile" and is divided into several sections:

- Navigation Pane (Left):** Shows the configuration tree with "Remote Access VPN" expanded to "AnyConnect Client Profile".
- Configuration Area (Center):** Contains a "Profile Name" field set to "atw-core-asa-profile" and an "EnrollmentProfile" field.
- Preferences (Part 1) (Right):** A list of settings for the profile, including:
 - Use Start Before Logon
 - Show Pre-Connect Message
 - Certificate Store:** Set to "All".
 - Certificate Store Override
 - Auto Connect On Start
 - Minimize On Connect
 - Local Lan Access
 - Disable Captive Portal Dete...
 - Auto Reconnect
 - Auto Reconnect Behavior:** Set to "ReconnectAfter..."
 - Auto Update
 - RSA Secure ID Integration:** Set to "Automatic".
 - Windows Logon Enforcement:** Set to "SingleLocalLo..."
 - Windows VPN Establishment:** Set to "LocalUsersOnly".
 - Clear SmartCard PIN
 - IP Protocol Supported

Better roaming security

Pair Cisco AnyConnect and Umbrella



Capabilities

Intercepts DNS / IP / Web traffic and redirects to cloud proxies

Options for on premises or VPN connected

Benefits

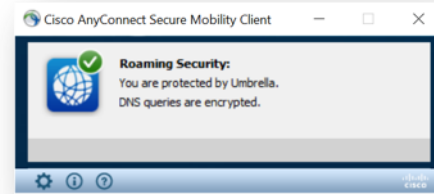
Extend security to roaming users

Defend against malware

Safeguard web usage

Roaming Security Module

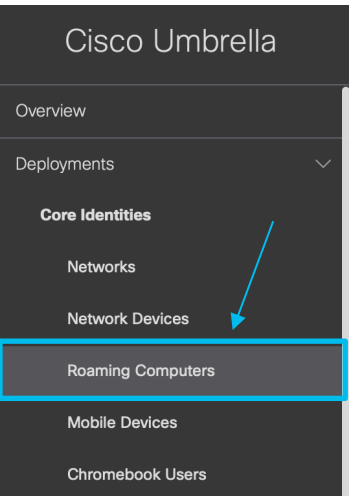
- Umbrella Client
 - Also known as Endpoint Roaming Client (ERC)
 - DNS layer security
 - Leverages DNSCrypt (UDP 443 / TCP 443)
 - <https://github.com/jedisct1/dnscrypt-proxy/blob/master/DNSCRYPT-V2-PROTOCOL.txt>
 - Next-gen web security
 - No Profile Editor for Roaming Module.
 - Download the orginfo.json from OpenDNS and upload to ASDM / Client Profiles.
 - Or place directly in the directory



```
{  
  "organizationId" : "XXXXXXXX",  
  "fingerprint" : "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",  
  "userId" : "XXXXXXXX"  
}
```

Roaming Security (Umbrella) Profile

Obtaining the orginfo.json



The screenshot shows the Cisco Umbrella dashboard with a modal window titled 'Download Roaming Client'. The modal contains the following text:

Download Roaming Client

The roaming client protects laptops and desktops, on and off the network. Before installing the roaming client, read through the [documentation and prerequisites](#).

⚠ For your [internal domains](#) to resolve, you must add them to the [internal domains list](#). It's important to add them before you deploy!

Cisco Umbrella Roaming Client

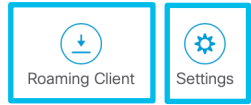
- Download Windows Client**
Supported Versions: Windows Vista, 7, 8, 10
- Download macOS Client**
Supported Versions: macOS 10.11+

AnyConnect Umbrella Roaming Security Module

Cisco AnyConnect can be configured to enable an Umbrella Roaming Security module which provides similar functionality to the roaming client. There are many deployment options, and each requires the customized profile downloaded below. [For full documentation, read here.](#)

Download Module Profile
The Umbrella module requires AnyConnect for Windows or macOS, version 4.3 MR1 minimum. 4.3 MR4+ is recommended.

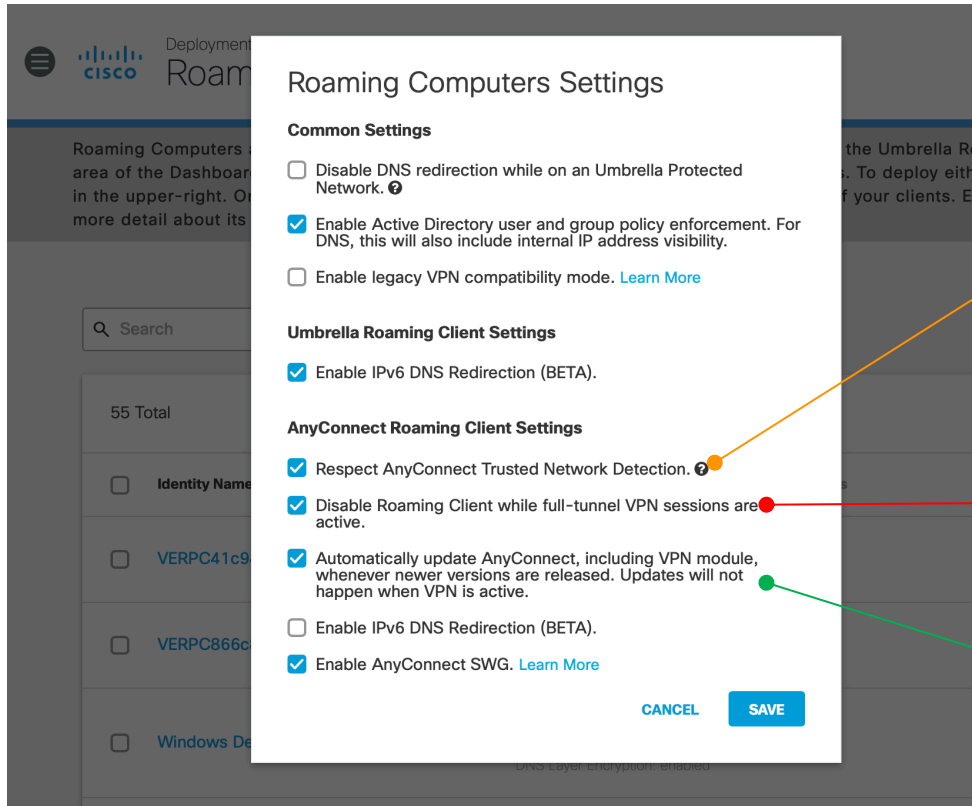
The AnyConnect 4.x client download can be found [here](#) (requires contract).



For the Umbrella Roaming Security module for AnyConnect. This... To deploy either agent type, click the "Download" button of your clients. Each Roaming Computer can be expanded for

Roaming Security (Umbrella) Profile

Obtaining the orginfo.json



Use TND

- Turns the connector off when on trusted network
- Enables Umbrella when not on Trusted Network

Disable when VPN

- If a full tunnel VPN is active, disable Umbrella

Update AC Client

- Use Umbrella connection to upgrade AC software



Network Visibility Module (NVM)

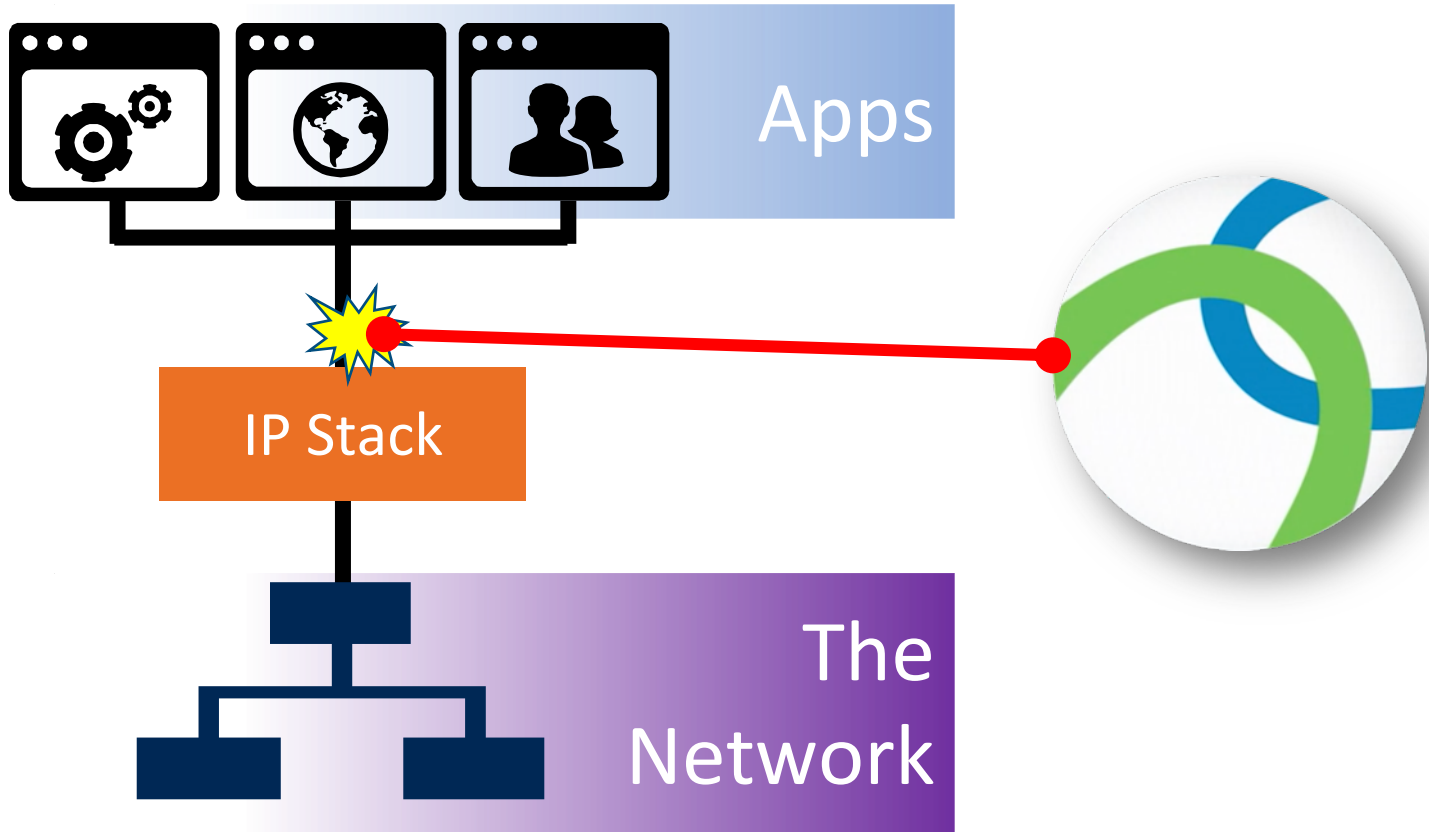
Summary of Features

- Completes the Visibility Story by Augmenting Network Flows with Details from the Endpoint
 - Visibility into All Network Traffic From Endpoint
 - Works On and Off Prem
 - Sends Data in IPFIX (NetFlow) based “nvzFlow”.

*“NVM says: not just this IP is talking to this IP on these ports[...] It actually has **this application is opening this connection**”.*

-Michael Scheck, Director Cisco CSIRT

Network Visibility Module



NVM Settings

nvzFlow Collector

- Stealthwatch Endpoint Concentrator, Splunk, etc.

Timed Summaries

- Sends summaries at timed intervals; helps with long-lived sessions

Protect the Collector

- Only Send During Interval
- Throttle Kbps of Flow Data

Offline Storage

Could be Unlimited
Oldest Removed First
If ! Configured, 50MB Default

The screenshot shows the configuration interface for the nvzFlow Collector. It is divided into several sections:

- Collector Configuration:** IP Address/FQDN: 10.1.100.63, Port: 3055.
- Cache Configuration:** Max Size: 100 MB, Max Duration: 30 days.
- Periodic Flow Report:** 60 seconds. Note: Valid Range: 60-360. To send at the start of the flow: 0.
- Aggregation Interval:** 5 seconds.
- Throttle Rate:** 500 Kbps. Note: Valid range: 12 - 2048. To disable: 0.
- Collection Mode:** All Networks (dropdown menu).
- Collection Criteria:** Broadcast packets (checkbox), Multicast packets (checkbox).
- Data Collection Policy:** ATW-Collection-Policy (text field), Add, Edit, Delete buttons.

Callouts from the text on the left point to these sections: a green line points to Collector Configuration, a blue line points to Periodic Flow Report, and an orange line points to the Collection Mode dropdown and its menu options.

The Collection Mode dropdown menu is open, showing the following options: All Networks (selected), Off, Trusted Network Only, Untrusted Network Only, and All Networks.

NVM Settings Continued

Collection Policy

- Define when to collect (VPN, Trusted, Untrusted)
- What Fields to Collect
- What Fields to Anonymize:
 - LoggedInUser
 - ProcessName
 - ProcessAccount
 - ParentProcessName
 - ParentProcessAccount
 - DestinationHostname
 - DNSSuffix
 - VirtualStationName
 - OSName
 - OSVersion
 - SystemManufacturer
 - SystemType
 - OSEdition
 - InterfaceName
 - SSID

Data Collection Policy

Name:

Network Type Vpn Trusted Untrusted

Include/Exclude

Type: Include Exclude

Fields

- LoggedInUser
- ProcessName
- ProcessAccount
- ProcessHash
- ParentProcessName
- ParentProcessAccount

Optional Anonymization More

Fields

- LoggedInUser
- ProcessName
- ProcessAccount
- ParentProcessName
- ParentProcessAccount
- DestinationHostname

Collector Configuration

IP Address/FQDN:

Port:

Periodic Flow Report seconds
Note: Valid Range: 60-360. To send a

Aggregation Interval: seconds

Throttle Rate: Kbps
Note: Valid range: 12 - 2048. To disa

Collection Mode:

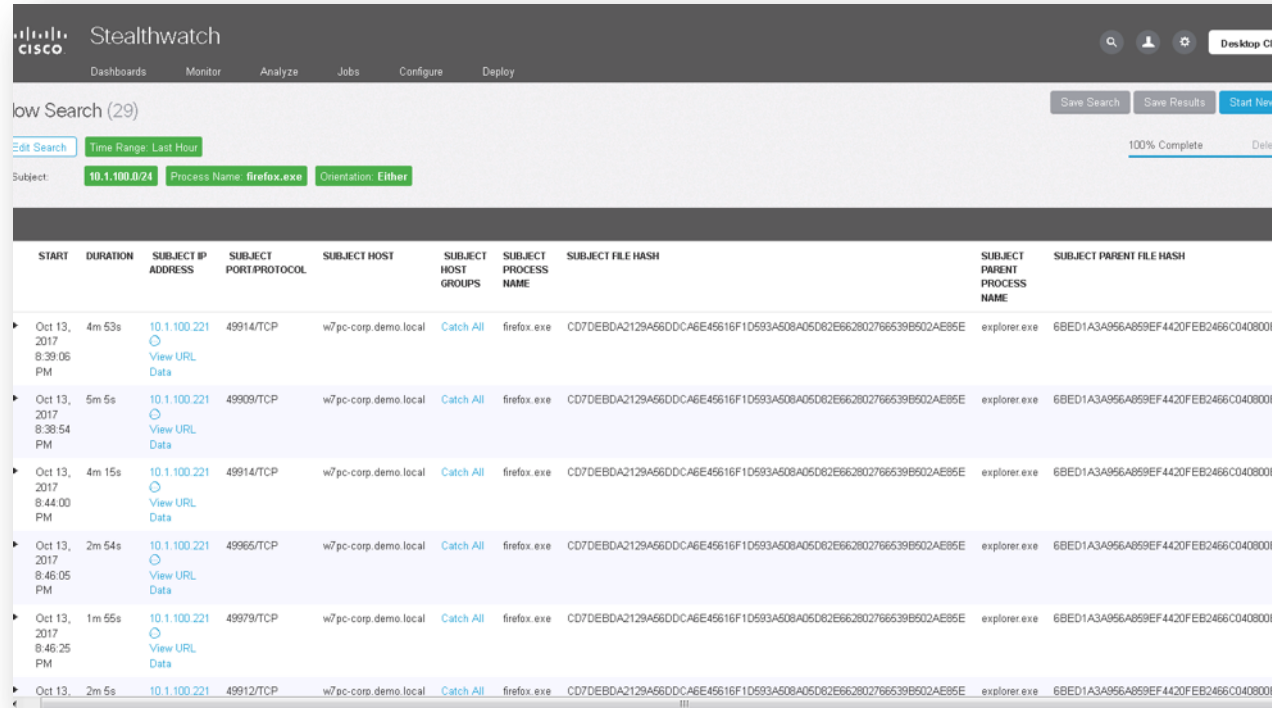
Collection Criteria: Broadcast packets Multicast packets

Data Collection Policy:

Use Stealthwatch for On-Premise Added Value

Stealthwatch Enterprise

- Adds tremendous value and situational awareness to the incident responder
- Provides so much more context to the enterprise flows



The screenshot displays the Cisco Stealthwatch Enterprise web interface. At the top, there are navigation tabs: Dashboards, Monitor, Analyze, Jobs, Configure, and Deploy. A search bar is visible with the text "low Search (29)". Below the search bar, there are filters for "Subject: 10.1.100.0/24", "Process Name: firefox.exe", and "Orientation: Either". The main content is a table with the following columns: START, DURATION, SUBJECT IP ADDRESS, SUBJECT PORT/PROTOCOL, SUBJECT HOST, SUBJECT HOST GROUPS, SUBJECT PROCESS NAME, SUBJECT FILE HASH, SUBJECT PARENT PROCESS NAME, and SUBJECT PARENT FILE HASH. The table contains five rows of data, all showing Firefox processes running on hosts in the w7pc-corp.demo.local network.

START	DURATION	SUBJECT IP ADDRESS	SUBJECT PORT/PROTOCOL	SUBJECT HOST	SUBJECT HOST GROUPS	SUBJECT PROCESS NAME	SUBJECT FILE HASH	SUBJECT PARENT PROCESS NAME	SUBJECT PARENT FILE HASH
Oct 13, 2017 8:39:06 PM	4m 53s	10.1.100.221	49914/TCP	w7pc-corp.demo.local	Catch All	firefox.exe	CD7DEBDA2129A56DDCA6E45616F1D593A508A05D62E662802766539B502AE85E	explorer.exe	6BED1A3A956A859EF4420FEB2466C0408001
Oct 13, 2017 8:39:54 PM	5m 5s	10.1.100.221	49909/TCP	w7pc-corp.demo.local	Catch All	firefox.exe	CD7DEBDA2129A56DDCA6E45616F1D593A508A05D62E662802766539B502AE85E	explorer.exe	6BED1A3A956A859EF4420FEB2466C0408001
Oct 13, 2017 8:44:00 PM	4m 15s	10.1.100.221	49914/TCP	w7pc-corp.demo.local	Catch All	firefox.exe	CD7DEBDA2129A56DDCA6E45616F1D593A508A05D62E662802766539B502AE85E	explorer.exe	6BED1A3A956A859EF4420FEB2466C0408001
Oct 13, 2017 8:46:05 PM	2m 54s	10.1.100.221	49965/TCP	w7pc-corp.demo.local	Catch All	firefox.exe	CD7DEBDA2129A56DDCA6E45616F1D593A508A05D62E662802766539B502AE85E	explorer.exe	6BED1A3A956A859EF4420FEB2466C0408001
Oct 13, 2017 8:46:25 PM	1m 55s	10.1.100.221	49979/TCP	w7pc-corp.demo.local	Catch All	firefox.exe	CD7DEBDA2129A56DDCA6E45616F1D593A508A05D62E662802766539B502AE85E	explorer.exe	6BED1A3A956A859EF4420FEB2466C0408001
Oct 13, 2017 8:46:25 PM	2m 5s	10.1.100.221	49912/TCP	w7pc-corp.demo.local	Catch All	firefox.exe	CD7DEBDA2129A56DDCA6E45616F1D593A508A05D62E662802766539B502AE85E	explorer.exe	6BED1A3A956A859EF4420FEB2466C0408001

NVM – The Endpoint Visibility it Provides...

Netflow/IPFIX

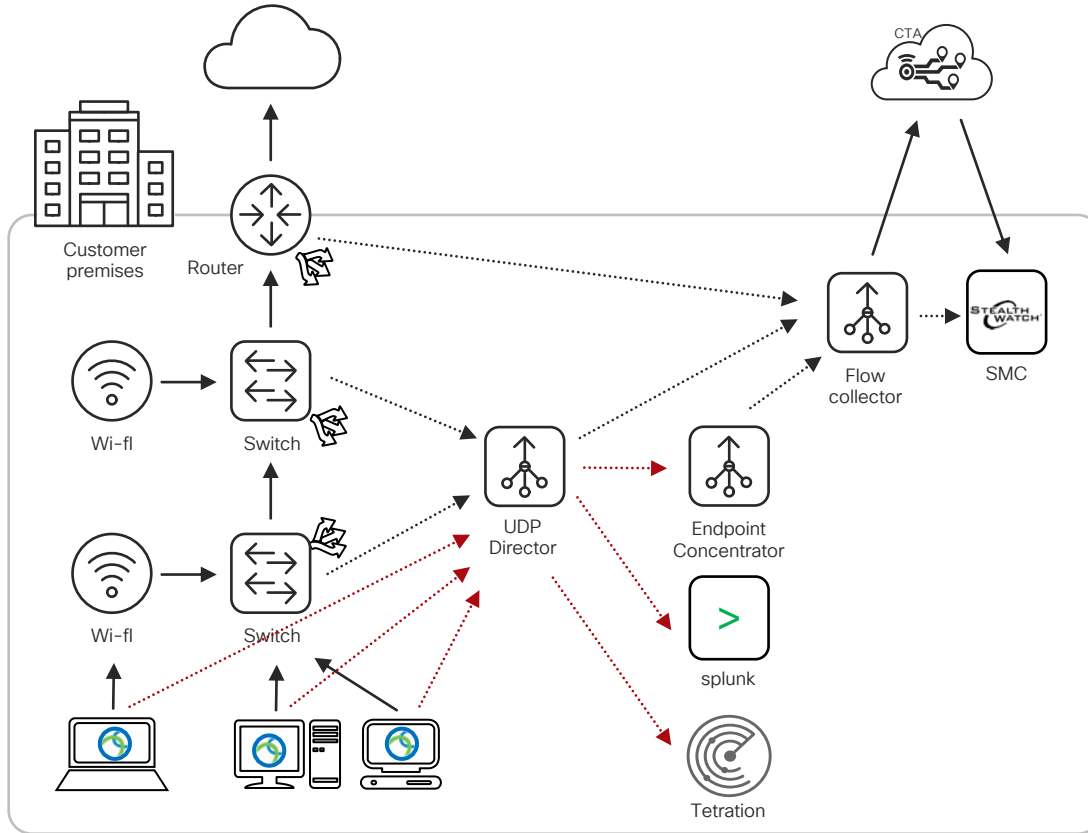
Source IP	Source IP
Destination IP	Destination IP
Source Port	Source Port
Destination Port	Destination Port
Bytes Sent	Bytes Sent
Bytes Received	Bytes Received

NVM (IPFIX Formatted)

OS Version
OS Edition
UDID
Host Name
Logged In User
Process Name
Process Hash
Process Account
Parent Process Name
Parent Process Hash
Parent Process Account
DNS/Destination Hostname
Module Hash List
System Manufacturer
System Type
MAC Address
Interface Name / Type / UID

Deep Endpoint
Visibility

User
Traffic Stats
Processes
Applications
SaaS Used
Accounts
Destinations
Machine Details



Differentiating NetFlow from nvzFlow

- Network devices use 2055 for NetFlow.
- AnyConnect NVM configured to use 3055 for nvzFlow.
- UDP Director configured to send only nvzFlows to splunk & Tetration
- Splunk requires the acnvmcollector service (on-box or off-box)

Sending to Stealthwatch Flow Collector, Splunk and Tetration with UDP Director

NVM to Splunk

- 2055 is default port
- Network will use 2055 also
- Leverage 3055 for endpoints to limit what is sent to Splunk to just endpoints

NVM to Concentrator

- Endpoint Concentrator
- Tetration

Net to Flow Collector

- Flows direct to Flow Collector

Stealthwatch UDP Director

Forwarding Rules

Info! This UDP Director is currently managed by [your SMC](#). Please go to your SMC to configure the forwarding rules for this

Rule #	Description	Source IP Address:Port List	Destination IP Address	Destination Port Number	Delete
1.	Slunk nvzFlow Collector	All:3055	10.1.100.27	2055	<input type="checkbox"/>
2.	SW Endpoint Collector	All:3055	10.1.100.63	2055	<input type="checkbox"/>
3.	Tetration	All:3055	10.1.100.66	2055	<input type="checkbox"/>
4.	NetFlow to FlowCollector	All:2055	10.1.100.123	2055	<input type="checkbox"/>



AMP for Endpoints



Agenda

- Why endpoint security?
 - Protecting the human
- AnyConnect
 - It's not just for VPN
- AMP for Endpoints
 - The nuts and bolts
- Endpoint security in context
 - What about the rest of your network?

Agenda

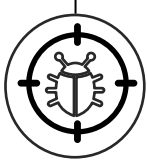
- **AMP for Endpoints – the Details**
 - AMP protection lattice part 1
 - Exploit Prevention
 - AMP protection lattice part 2
 - Duo integration
 - Threat Grid
 - Talos Threat Intelligence
 - Machine Learning
 - Endpoint Isolation (and Automated Actions)
 - Orbital Advanced Search

The background is a dark blue field filled with numerous small, semi-transparent squares and dots in various colors including light blue, green, yellow, orange, and red. These elements are scattered across the frame, with a higher density of yellow and orange squares on the right side, creating a sense of depth and movement.

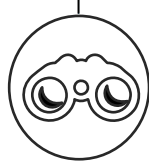
AMP Protection Overview

AMP does a lot!

Malware Protection



Visibility



Protection Everywhere



Threat Protection

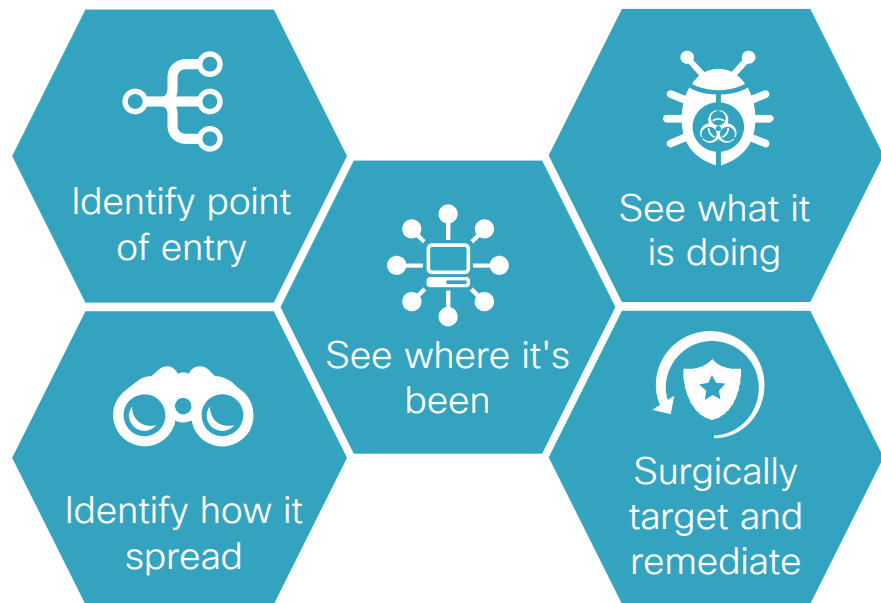
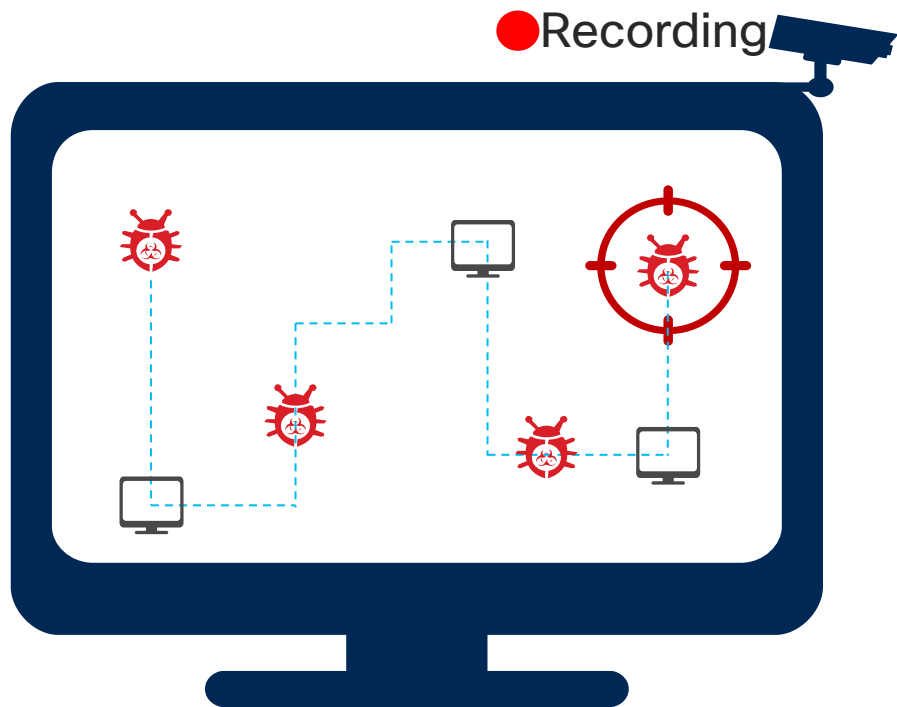


AMP for Endpoints Focus

- Cloud managed, subscription based SaaS
- Protects Windows, macOS, Linux (CentOS and RedHat), iOS, Android
- Public or private cloud deployment options
- Part of AMP Everywhere integrated architecture with intelligence sharing
- Continuous Analysis and Retrospective security



Continuous Analysis and Retrospective Security



The Convergence of EPP and EDR

Endpoint Protection Platforms

- Integrated solution with the following capabilities: anti-malware, personal firewall, port and device control
- Traditional AV (signature-based approach)

Endpoint Detection and Response

- Visibility tool for detection, Incident Response support (post-incident investigation), for proactive threat hunting
- Handling what traditional AV missed



Next Gen Endpoint Security

- A tool which detects and prevents malware infections and provides visibility and control for post infection investigations

Next Generation Endpoint Security



Prevent

Prevent attacks and block malware in real time



Detect

Continuously monitor to reduce time to detection



Respond

Accelerate investigations and remediate faster and more effectively

AMP for Endpoints Protection Lattice

- Security engines that work together to prevent, detect, and respond to malware
- Used in conjunction with each other to achieve better efficacy and visibility

AMP for Endpoints Protection Lattice

Time



Memory / Script

Exploit Prevention

Script Protection

System Process Protection

In Transit / On Disk

Realtime File Blocking through
AMP Cloud Lookup

Malicious Activity Protection

Traditional AV [Compliance]
Offline Detection Engine

Simple and Advanced
Custom Detections

Post-Infection

Machine Learning
Cognitive Threat Analytics

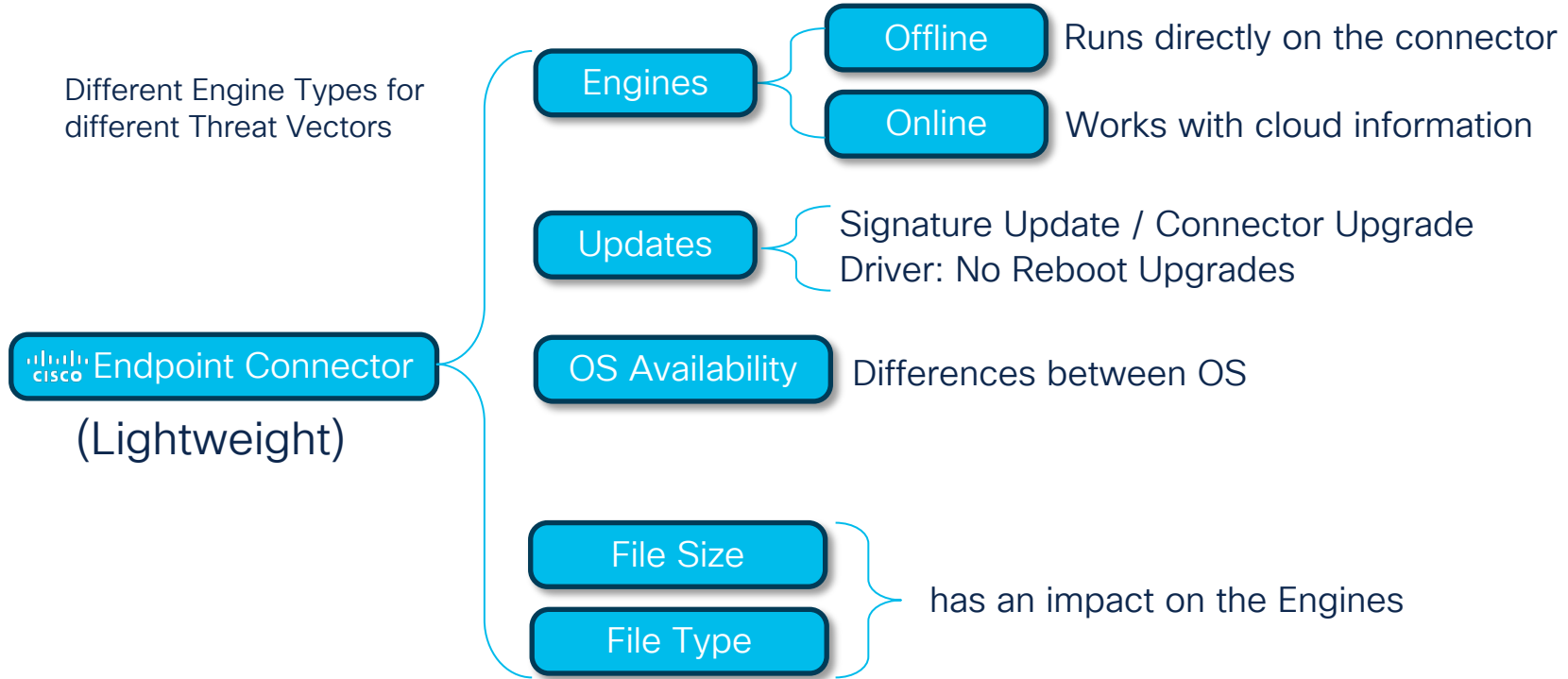
C&C Blocking
Device Flow Correlation

Automated analysis in cloud
for Indications of Compromise

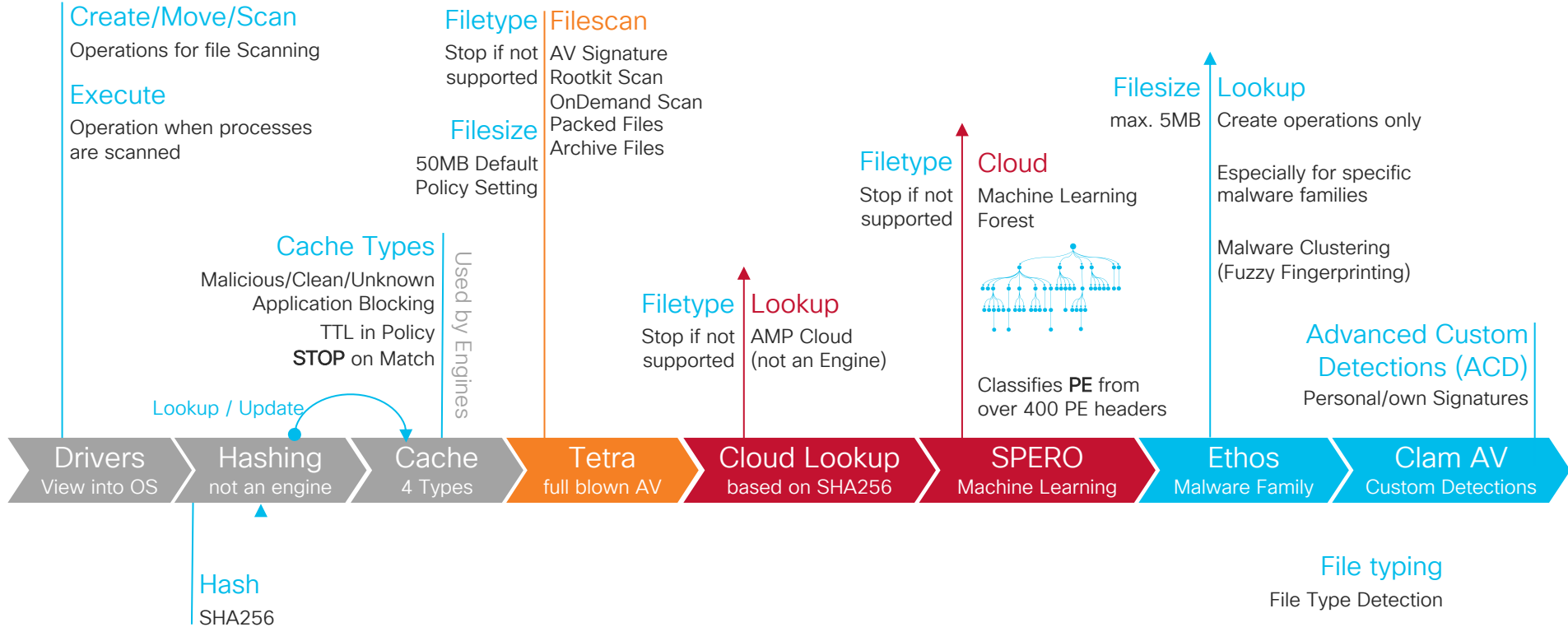
Endpoint Searching and
Artifact Hunting

Endpoint Engines – Overview and Keyfacts

Different Engine Types for different Threat Vectors



Endpoint Engines – Detection Sequence (Files)





AMP Exploit Prevention

Exploit Prevention (exPrev)

- Engine Type: Offline
- Update: Feature inside AMP connector and is upgraded through Connector upgrade
- Works in the Memory

The engine stops the following threats, malware, and exploit techniques*

Exploitation

- Memory corruption exploits
- ROP/return to lib
- Heap spraying

Post-Exploitation

- Shellcode
- Code Injection
- Process hollowing
- Reflective loading

















Malware

- Packer-based malicious attacks
- Adware

(*) Table above does not represent an exhaustive list of threats defeated by Exploit Prevention engine

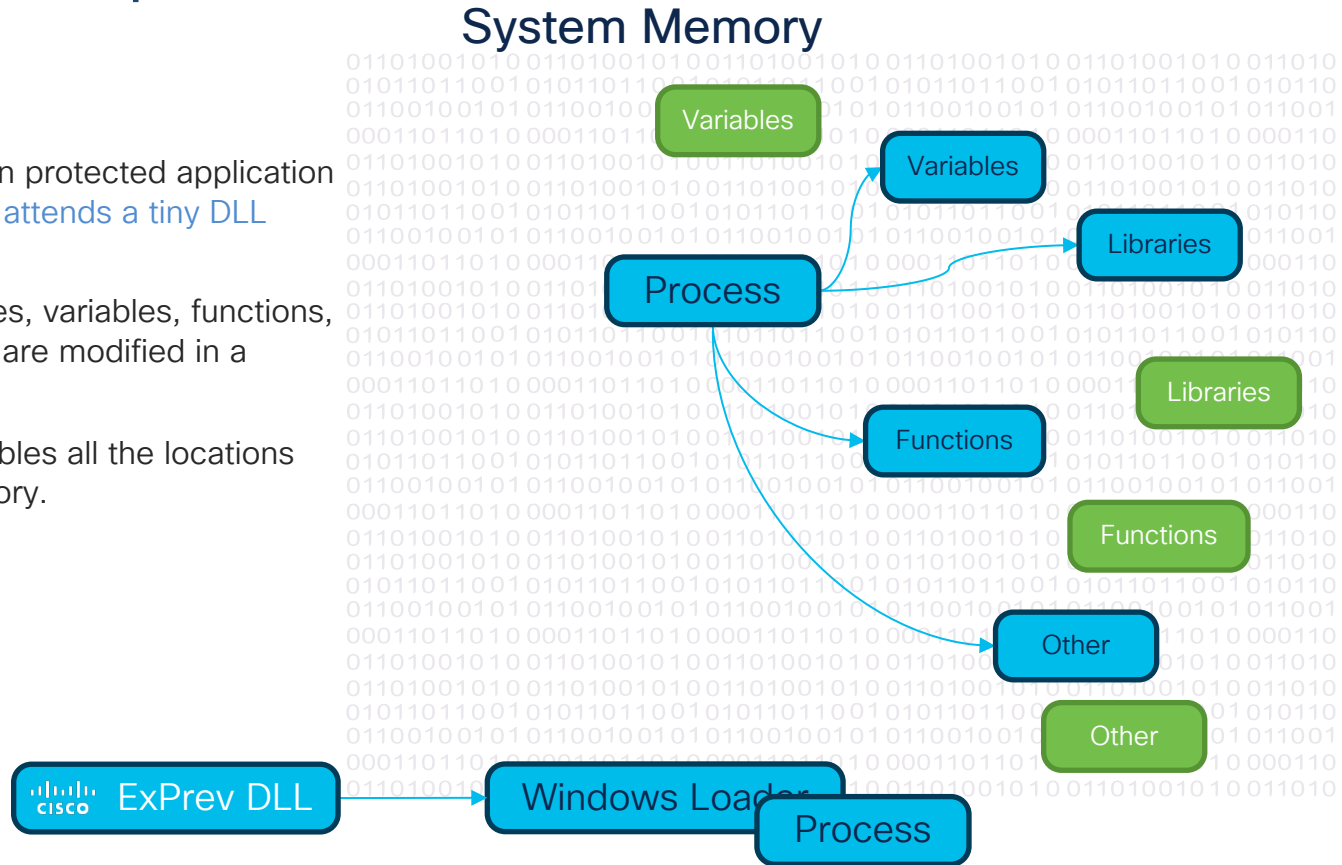
Exploit Prevention (exPrev)

The following 32-bit and 64-bit applications and their child processes, as well as the following system processes inherit protection:

<ul style="list-style-type: none">• Microsoft Excel • Microsoft Word • Microsoft PowerPoint • Microsoft Outlook • Internet Explorer • Mozilla Firefox • Google Chrome • Microsoft Skype 	<ul style="list-style-type: none">• TeamViewer • VLC Media Player • Windows Script Host • Microsoft PowerShell • Adobe Acrobat Reader • MS Register Server • MS Task Scheduler • MS Equation Editor 	<h3>Critical System Processes</h3> <ul style="list-style-type: none">• Local Security Authority• Windows Explorer• Spooler Subsystem
---	---	--

ExPrev - Step 1 of 3

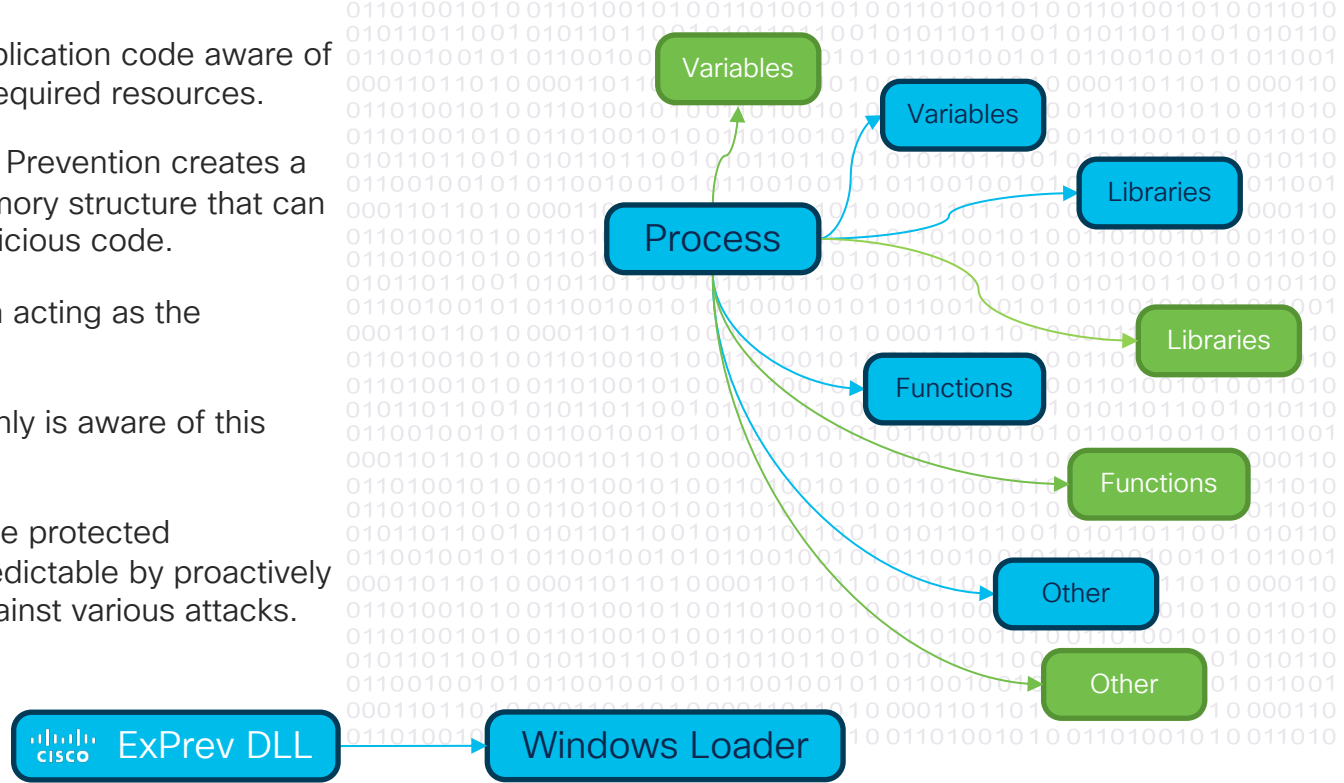
- Windows Loader loads a protected application into the Memory. *ExPrev attends a tiny DLL to the Windows Loader.*
- Goal: Locations of libraries, variables, functions, and other data elements are modified in a coordinated manner.
- Exploit Prevention scrambles all the locations of resources in the memory.



ExPrev - Step 2 of 3

- Making the legitimate application code aware of the new locations of its required resources.
- At the same time, Exploit Prevention creates a **decoy** of the original memory structure that can be used as a **trap** for malicious code.
- The original Memory area acting as the decoy is **Read-Only**.
- **Result:** The Application only is aware of this change.
- **Result:** The memory of the protected applications is now unpredictable by proactively changing its structure against various attacks.

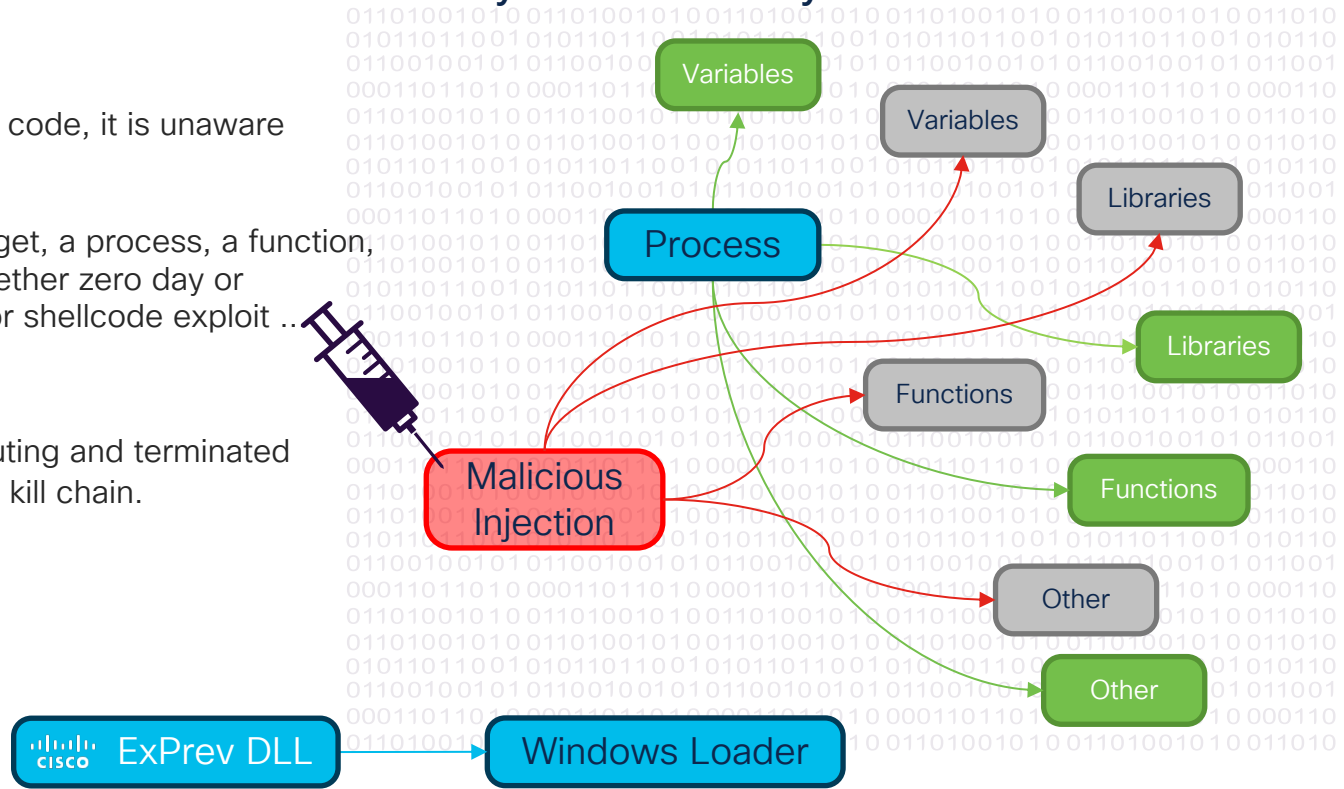
System Memory



ExPrev - Step 3 of 3

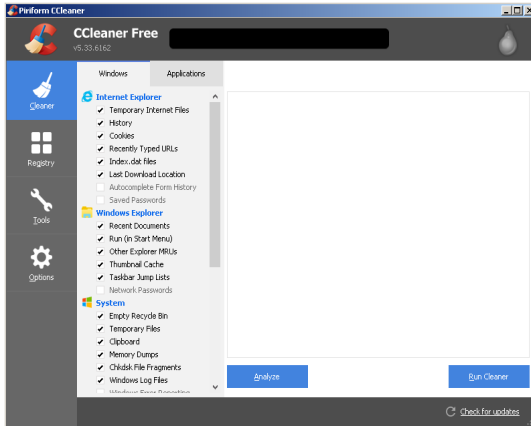
System Memory

- If a process tries to inject code, it is unaware of the memory changes.
- Activity like finding a gadget, a process, a function, a DLL, a vulnerability, whether zero day or unpatched vulnerability, or shellcode exploit ... it is blocked.
- It is prevented from executing and terminated as early as possible in the kill chain.



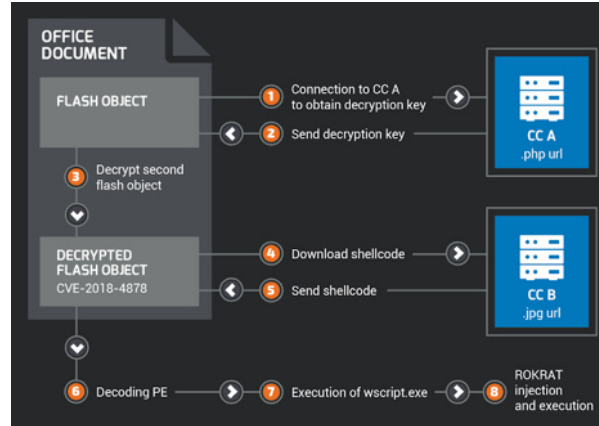
Exploit Prevention: In Field Findings

CCleaner



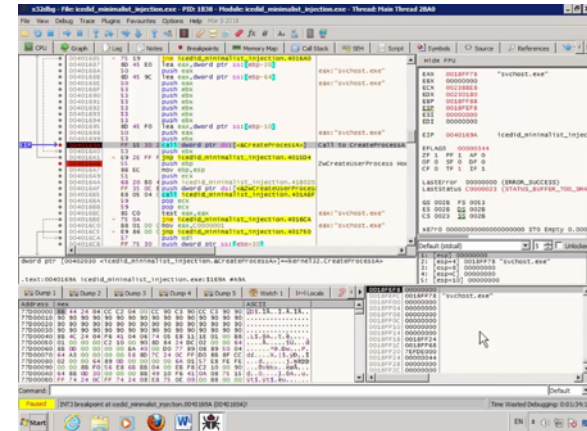
Backdoor discovered in CCleaner software from Avast

0-day Flash Exploit



0-day Remote Code Execution vulnerability prevented

IcedID Trojan



Minimalist (evolutionary) code injected technique prevented

CCleaner: <https://blog.talosintelligence.com/2017/09/avast-distributes-malware.html>

0-day Flash: <http://blog.talosintelligence.com/2018/02/group-123-goes-wild.html>

IcedID: Talos Analysis: <https://blog.talosintelligence.com/2018/04/icedid-banking-trojan.html>

Exploit Prevention vs. Microsoft EMET

- Microsoft Enhanced Mitigation Experience Toolkit (EMET)
 - Toolkit for Windows to address the same problem space
 - Looks for known in-memory attacks
 - Applications must be designed to work with EMET
- For Windows 10+, EMET has been merged into Windows Defender as “Exploit Guard”
- So.... Why Cisco AMP w/ Exploit Prevention?

Exploit Prevention vs. Microsoft EMET

EMET/Exploit Guard

EMET has a signature-based approach to the problem space:

- Explicit rules are defined to detect specific types of attacks (rule per set of attacks); attackers bypass EMET if they understand these rules
- Applications must be coded for EMET
- Must disable many rules due to blocking behaviour many applications require, many of the rules in EMET should be disabled decreasing protection
- Requires a large amount of RAM, system reboots required to apply changes, impacts performance
- No forensic data on blocked attacks
- Can be bypassed in Windows 7, 8, 10
- Offers exploitation-only protection

Exploit Prevention

Exploit Prevention takes a completely different approach that is prevention focused:

- Fully proactive prevention that is not rule based
- No prior knowledge of the attack required – any access to original memory addresses is malicious
- No application compatibility issues, but there are 2 rules in EMET that must be disabled if running both EMET & ExPrev
- No run-time components and no run-time performance penalty, only load time
- Provides detailed forensic information through the AMP for Endpoints Console and APIs
- Part of an enterprise-grade security solution
- Protects against exploitation, post-exploitation, and malware



AMP for Endpoints

Agenda

- **AMP for Endpoints – the Details**
 - AMP protection lattice part 1
 - Exploit Prevention
 - AMP protection lattice part 2
 - Duo integration
 - Threat Grid
 - Talos Threat Intelligence
 - Machine Learning
 - Endpoint Isolation (and Automated Actions)
 - Orbital Advanced Search



More of the Protection Lattice

System Process Protection

- Protects critical Windows system processes from being compromised through memory injection attacks
- Evaluates desired process/thread access and truncates potentially dangerous access
- Example threat defeated: Mimikatz dumping credentials from the Local Security Authority Subsystem (lsass.exe)

```
.#####.  mimikatz 2.0 alpha (x86) release "Kiwi en C" (Apr  6 2014 22:02:03)
.## ^ ##.
## / \ ## /* * *
## \ / ## Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
'## v ##' http://blog.gentilkiwi.com/mimikatz           (oe.eo)
'#####'                                     with 13 modules * * */
```

- Session Manager Subsystem (smss.exe)
- Client/Server Runtime Subsystem (csrss.exe)
- Local Security Authority Subsystem (lsass.exe)
- Windows Logon Application (winlogon.exe)
- Windows Startup Application (wininit.exe)

Malicious Activity Protection Engine

- Engine Type: Offline (Proactively)
- Update: Feature inside AMP connector and is upgraded through Connector upgrade
- Works with File/Memory / Behavioral Engine



MAP is the „Anti Ransomware“ Engine!



Solves the IOC/STIX limitations with dynamic criteria



Stix Challenges

- Cannot describe time relations between events
- Cannot describe complex relationships between attributes
- Cannot count (repeat this event n times)
- Not a match for dynamic rules

Malicious Activity Protection

Rules Example:

are included inside the Engine

- Ransomware Sample is downloaded from Internet
- Process renames several files in a short time period
- Ransomware starts to encrypt disk

} No Cloud

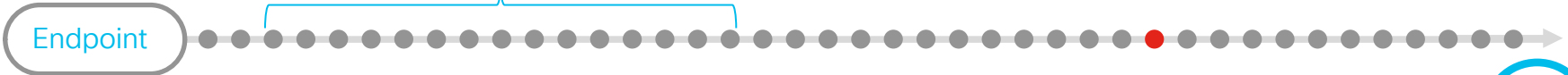


Guardrails Check

- prevent accidental blocking or quarantine of legitimate applications and Operating System components
- does a Cloud Lookup
- guardrails check for digital signatures (Embedded, Catroot signed)
- honors excluded folders and processes



MAP monitors System activities





Endpoint

OS Event: ● 1 of approx. 46 Million in 20min





Script Protection

- The Script Protection engine uses Microsoft's Anti-Malware Scanning Interface (AMSI) to identify, analyze, and control script executions in the same way as AMP has always covered PE executables.
- Coverage includes Powershell, User Account Control, Windows Script Host, Javascript, VBScript, Office VBA macros.
- AMP Windows connector versions 7.2.3 and newer.

▼ Win10x64-localY detected a Cloud IOC: W32.Excel.PowerShell.ioic Medium  

File Detection	Description	Microsoft Excel launched PowerShell. This is indicative of multiple dropper variants that make use of Visual Basic Scripting Engine (VBS) for downloading and executing malicious executables.
Connector Info	Tactics	Initial Access Execution
Comments	Fingerprint (SHA-256)	7762a476...3e6e57d6
	File Name	powershell.exe
	File Path	file:///C:/Users/qgauser/Desktop/BD_Sample/test_samples/test_samples_pass_notinfected!/ps1/test
	Command Line Arguments	powershell -f C:\Users\qgauser\Desktop\BD_Sample\test_samples\test_samples_pass_notinfected!\ps1\tes
	Parent Fingerprint (SHA-256)	24bffeda...fd33e26d

[Analyze](#)  [View Upload Status](#) 

Configuring Engines

- Policy settings can be applied to groups of endpoints.
- Windows connector settings shown here, because that's (still) where most of the action is.

The screenshot displays the Cisco AMP for Endpoints Advantage interface. At the top, the navigation bar includes 'Dashboard', 'Analysis', 'Outbreak Control', 'Management', and 'Accounts'. The 'Edit Policy' page is for a Windows connector with the name 'Lab Desktops' and description 'AMP TME Lab systems'. The 'Modes and Engines' sidebar on the left lists 'Exclusions' (3 sets), 'Proxy', 'Outbreak Control', 'Product Updates', and 'Advanced Settings'. The main content area is titled 'Conviction Modes' and includes sections for 'Files', 'Network', 'Malicious Activity Protection', 'System Process Protection', and 'Script Protection', each with buttons for 'Quarantine', 'Audit', and 'Blocked'. The 'Detection Engines' section at the bottom shows 'TETRA' and 'Exploit Prevention' are checked. A 'Recommended Settings' sidebar on the right provides a summary of settings for Workstation and Server.

Configuring Engines

- The **Files** setting controls the behavior when the AMP cloud lookup returns a **malicious** disposition.
- **Quarantine** means the file is quarantined and any running processes terminated.
- **Audit** only logs the event.

The screenshot shows the Cisco AMP for Endpoints management console. The top navigation bar includes the Cisco logo, 'AMP for Endpoints Advantage', a user profile for Brian McMahon, and a search bar. The main content area is titled 'Edit Policy' and shows a policy named 'Lab Desktops' with the description 'AMP TME Lab systems'. A red box highlights the 'Files' setting, which is currently set to 'Quarantine'. Below this, there are sections for 'Outbreak Control', 'Product Updates', and 'Advanced Settings'. The 'Network' section has 'Block', 'Audit', and 'Disabled' options. The 'Malicious Activity Protection' section has 'Quarantine', 'Block', 'Audit', and 'Disabled' options. The 'System Process Protection' section has 'Protect', 'Audit', and 'Disabled' options. The 'Script Protection' section has 'Quarantine', 'Audit', and 'Disabled' options. The 'Detection Engines' section has checkboxes for 'TETRA' and 'Exploit Prevention', both of which are checked. On the right side, there is a 'Recommended Settings' panel with a list of settings for Workstation, Network, Malicious Activity Protection, System Process Protection, Script Protection, and Server.

Configuring Engines

- The **Network** setting controls the behavior of Device Flow Correlation (DFC).
- **Block** stops the network connection.
- **Audit** logs the event.
- **Disabled** means no lookup is performed.

The screenshot shows the Cisco AMP for Endpoints Management console. The main heading is "Edit Policy" for a policy named "Lab Desktops". The description is "AMP TME Lab systems". A callout box highlights the "Network" setting, which is currently set to "Block". Other settings visible include "Malicious Activity Protection" set to "Quarantine", "System Process Protection" set to "Protect", and "Script Protection" set to "Quarantine". The "Detection Engines" section shows "TETRA" and "Exploit Prevention" are both checked.

Configuring Engines

- For **Malicious Activity Protection**, the **Quarantine** setting stops the suspicious activity and quarantines the file.
- **Block** stops the activity but does not quarantine the file.
- **Audit** and **Disabled** behave as described earlier.

The screenshot shows the Cisco AMP for Endpoints Management console. The top navigation bar includes the Cisco logo, 'AMP for Endpoints Advantage', a user profile for Brian McMahon, and a search bar. The main content area is titled 'Edit Policy' and shows a policy named 'Lab Desktops' with the description 'AMP TME Lab systems'. A highlighted section titled 'Malicious Activity Protection' shows four buttons: 'Quarantine' (selected), 'Block', 'Audit', and 'Disabled'. Below this, a table shows the configuration for various protection engines:

Outbreak Control	Block	Audit	Disabled	
Product Updates	Quarantine	Block	Audit	Disabled
Advanced Settings	Protect	Audit	Disabled	
	Quarantine	Audit	Disabled	

The 'Detection Engines' section shows 'TETRA' and 'Exploit Prevention' both checked. A summary box on the right indicates the current settings: Files: Quarantine, Network: Disabled, Malicious Activity Protection: Disabled, System Process Protection: Disabled, and Script Protection: Audit.

Configuring Engines

- For **System Process Protection**, the **Protect** setting stops attempts to interfere with a protected process.
- **Audit** and **Disabled** behave as described earlier.

The screenshot shows the Cisco AMP for Endpoints management console. The top navigation bar includes the Cisco logo, 'AMP for Endpoints Advantage', a user profile for Brian McMahon, and a search bar. The main content area is titled 'Edit Policy' and shows a policy named 'Lab Desktops' with the description 'AMP TME Lab systems'. A callout box highlights the 'System Process Protection' settings, showing three options: 'Protect' (selected), 'Audit', and 'Disabled'. Below this, a table shows settings for various protection engines: Network (Block, Audit, Disabled), Malicious Activity Protection (Quarantine, Block, Audit, Disabled), System Process Protection (Protect, Audit, Disabled), and Script Protection (Quarantine, Audit, Disabled). The 'Detection Engines' section shows 'TETRA' and 'Exploit Prevention' both checked.

Setting	Protect	Audit	Disabled	
Network	Block	Audit	Disabled	
Malicious Activity Protection	Quarantine	Block	Audit	Disabled
System Process Protection	Protect	Audit	Disabled	
Script Protection	Quarantine	Audit	Disabled	

Detection Engines

- TETRA
- Exploit Prevention

Configuring Engines

- For **Script Protection**, the **Quarantine** setting causes behavior similar to the quarantine action for executable files.
- **Audit** and **Disabled** behave as described earlier.
- Note that the interpreter of a script might be an application like Word.

The screenshot displays the Cisco AMP for Endpoints Advantage interface. At the top, the navigation bar includes 'Dashboard', 'Analysis', 'Outbreak Control', 'Management', and 'Accounts'. The main content area is titled 'Edit Policy' for a policy named 'Lab Desktops' with the description 'AMP TME Lab systems'. A callout box highlights the 'Script Protection' settings, showing three options: 'Quarantine' (selected), 'Audit', and 'Disabled'. Below this, the 'Network' setting is set to 'Block', 'Malicious Activity Protection' is set to 'Quarantine', 'System Process Protection' is set to 'Protect', and 'Script Protection' is set to 'Quarantine'. The 'Detection Engines' section shows 'TETRA' and 'Exploit Prevention' both checked. On the right, a 'Recommended Settings' panel lists various settings and their current values, including 'Script Protection: Audit'.

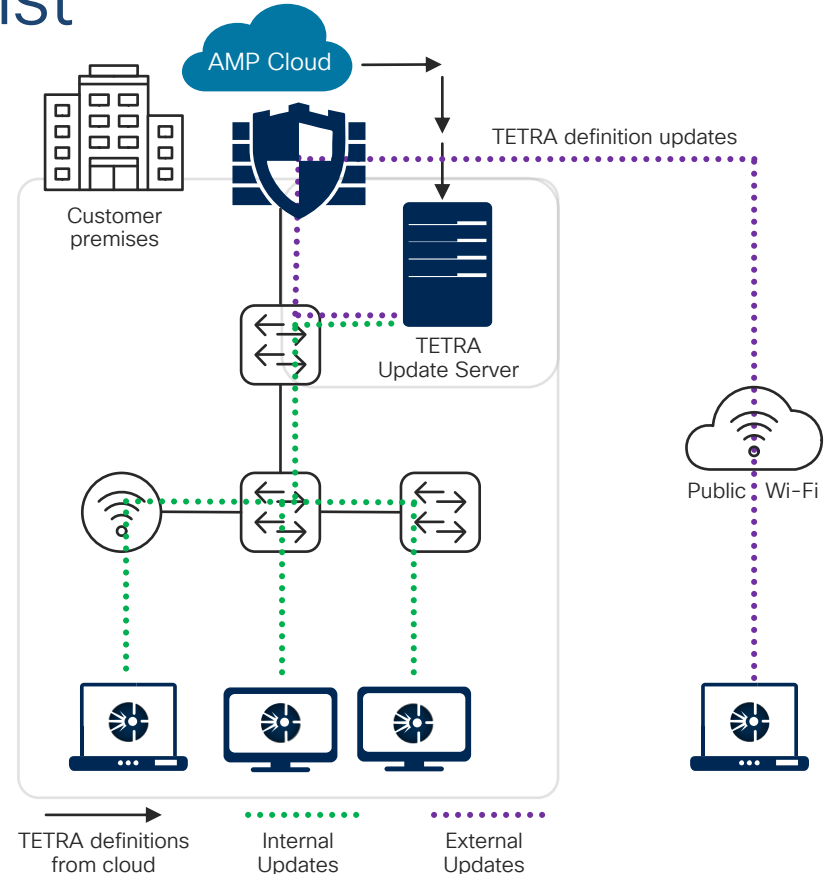
Configuring Engines

- Some engines only support an on/off configuration.
- Currently, those are the offline AV scanning engine and ExPrev.

The screenshot displays the Cisco AMP for Endpoints management interface. At the top, the navigation bar includes 'Dashboard', 'Analysis', 'Outbreak Control', 'Management', and 'Accounts'. The user is identified as 'Brian McMahon'. The main content area is titled 'Edit Policy' for 'Windows' and shows a policy named 'Lab Desktops' with the description 'AMP TME Lab systems'. A modal window titled 'Detection Engines' is overlaid on the screen, showing two engines checked: 'TETRA' and 'Exploit Prevention'. To the right, a 'Recommended Settings' panel lists various protection settings for 'Workstation' and 'Server' environments. Below the modal, the 'Advanced Settings' section shows a row of buttons: 'Quarantine', 'Block', 'Audit', and 'Disabled'. Further down, 'System Process Protection' and 'Script Protection' are each configured with 'Protect' and 'Quarantine' buttons respectively. At the bottom of the settings, the 'Detection Engines' section is repeated, showing 'TETRA' and 'Exploit Prevention' both checked.

Anti-Virus & Custom Blocklist

- Offline Anti-Virus engine for Windows: TETRA
- On-prem Anti-Virus update Server
- Custom File Blocking
 - Simple:
 - SHA256 hash
 - Advanced:
 - MD5 hash
 - PE section-based signatures
 - File Body-based signatures
 - Extended signature format (offsets, wildcards, regex)
 - Logical signatures
 - Icon signatures



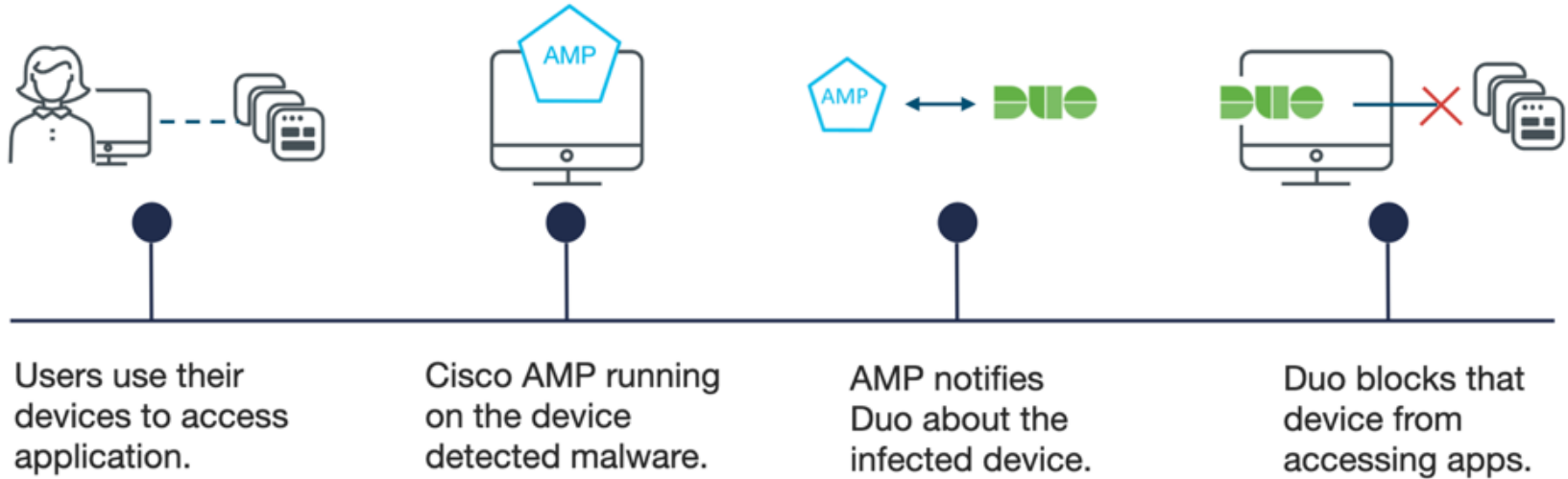
Cloud IOCs = Detect Likely Breaches

- Surface suspicious behavior on a host, a combination of events with malicious intent
- No automated blocking, trigger investigations
- Driven by Cisco Research team
- Example threat detections:
 - Word document launching shell
 - Powershell downloaded a file
 - Registry keys modified to persist
 - WMI executed on a remote system

The screenshot displays a user interface for a Cloud IOC (Indicator of Compromise) detection. The title bar reads "Demo_Command_Line_Arguments_Meterpreter detected a Cloud I..." and includes a "Cloud IOC" label and a timestamp of "2018-10-29 10:32:58 UTC". The main content area is a table with the following rows:

File Detection	Description	A named pipe was created in a manner similar to that used for local privilege escalation through named pipe impersonation. Tools such as meterpreter often use this technique to escalate to NT Authority\System.
Connector Info	Fingerprint (SHA-256)	935c1861...65d44ad2
Comments	File Name	cmd.exe
	File Path	/C:/WINDOWS/system32/cmd.exe
	Command Line Arguments	cmd.exe /c echo smzhqd > \\.\pipe\smzhqd
	Parent Fingerprint (SHA-256)	69d6fff3...19c384b9
	Analyze View Upload Status Add to Whitelist File Trajectory	

AMP for Endpoints – Cisco DUO Integration

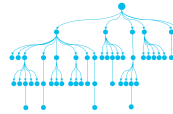


AMP Connector Engine Summary

Different engine types for different threat vectors (including scripts)

Filescan
 AV Signature
 Rootkit Scan
 On Demand Scan
 Packed Files
 Archive Files

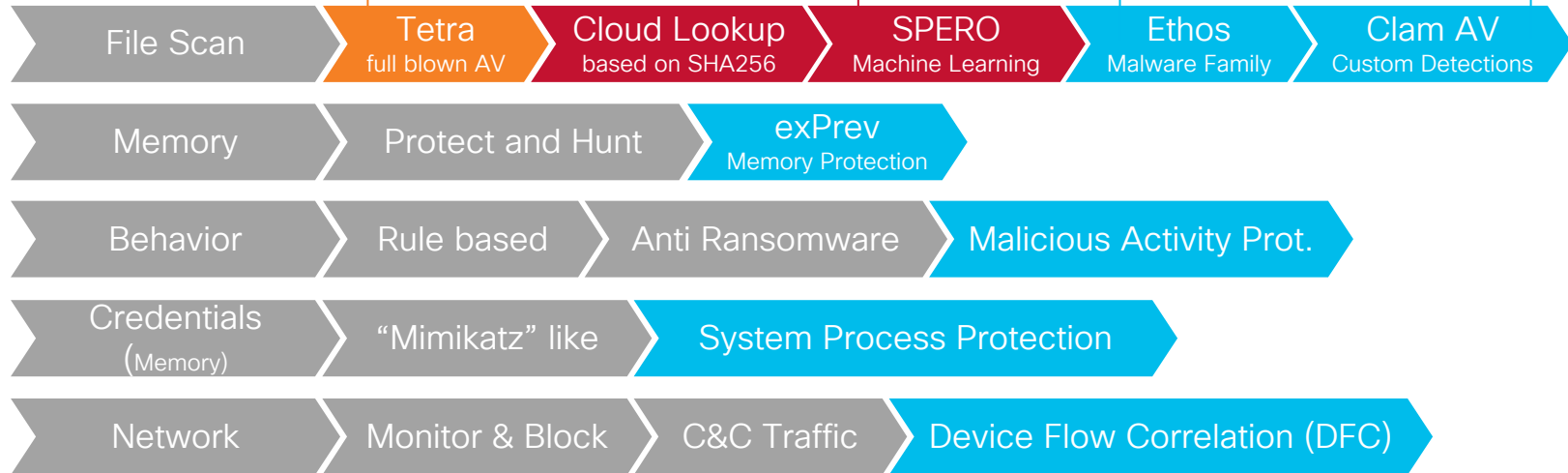
Cloud
 Machine Learning
 Forest



Lookup
 Malware Family Clustering
 (Fuzzy Fingerprinting)
 Polymorphic detection

**Advanced Custom
 Detections (ACD)**
 Personal/own Signatures

File typing
 File Type Detection





AMP for Endpoints

Agenda

- **AMP for Endpoints – the Details**
 - AMP protection lattice part 1
 - Exploit Prevention
 - AMP protection lattice part 2
 - Duo integration
 - Threat Grid
 - Talos Threat Intelligence
 - Machine Learning
 - Endpoint Isolation (and Automated Actions)
 - Orbital Advanced Search

Question:
What about
dynamic analysis
when the file hash
is *unknown*?

Answer:
Cisco Threat Grid

Cisco Threat Grid – How does it work?

1. Sample submission

2. Analyze, Correlate, and Enhance

3. Produce Intelligence & Inform AMP Architecture



Input

Submit suspicious samples to Threat Grid via Integration, API, or Portal

Process

Sample is executed and analyzed using multiple techniques

- Proprietary techniques for static and dynamic analysis
- “Outside looking in” approach
- 1000+ Behavioral Indicators

Output

- Behavioral Indicators & Threat Score
- Pokes AMP cloud, integrations will block
- Threat Intel Feeds & Global Intel

Behavioral Indicators

- 1800 + Indicators
- Human Readable
- Actionable Intelligence and Prioritization
- Indicators also mapped to the MITRE ATT&CK™ Framework

The screenshot displays the 'Indicators' interface with a search bar and a filter sidebar on the left. The main content area shows a list of indicators, each with a description, category, ATT&CK mapping, tags, and a score. The indicators are sorted by score, with all shown having a score of 100.

Indicator	Category	ATT&CK	Tags	Score
360 Anti Virus Signed Executable DLL Execution	code-injection	defense evasion, persistence, privilege escalation	DLL, DLL Hijacking, file, legitimate	100
7ev3n Ransomware Detected	ransomware		malware, ransomware	100
A File Associated With The Turia APT Was Detected	data-theft	execution, persistence	artifact, process	100
<p>An artifact known to be associated with the Turia advanced persistent threat (APT) group was seen being created or modified on the system. The Turia group is also known as Snake or Uroboros. The Turia malware targets European governments and defense companies. Once on a system, Turia will steal emails by forwarding all outgoing messages to the attackers. Email attachments are used for communication with the command and control server and for sensitive information exfiltration.</p>				
Adload Malware Detected	dropper		backdoor, dropper, trojan	100
Adload Malware Domain Detected	dropper		backdoor, dropper, trojan	100
Adware Adposhel Detected	puu		adware, browser hijacker, keylogger, PUU	100
Adwind Mutex Detected	rat		host, mutex, process, RAT, trojan, ttp	100
Adzok RAT Lockfile Detected	rat		downloader, java, keylogger, lock, RAT	100
AlienSpy RAT Detected	rat		host, process, RAT, trojan	100
AlienSpy RAT Detected v2	rat		forensic, RAT, trojan	100
Aliplex Mutex Detected	worm		host, lock, mutex, process, worm	100
<p>Aliplex is a multi-threaded, polymorphic network worm designed to spread over local area networks and conduct denial-of-service attacks against a remote site. Aliplex targets unpatched Windows machines and exploits weak logon passwords using a built-in dictionary to attack remote systems. Aliplex first appeared in 2006 as part of a denial-of-service campaign. Though the author was arrested, the malware continues to operate and is still very active today.</p>				
Andromeda Downloader Detected Dropping Gamarue Bot	rat		downloader, dropper, process, RAT, trojan	100
Andromeda Downloader Detected Dropping Gamarue Bot	rat		downloader, dropper, host, lock, process, RAT, trojan	100
AnonymizerGadget Detected	puu		adware, puu	100
Apalimpe Dropper Detected	dropper		host, RAT, trojan	100
AppWizard Packer Detected	lookit		dropper, packer, process	100
APT Stealer Malware Detected	data-theft		APT, Iran, malware, RAT, Saffron Rose, targeted, trojan	100
Arcom Remote Access Trojan Detected	rat		host, RAT, registry, trojan	100
Arduik Registry Key Detected	worm		registry, worm	100
Asprox/KuluoZ Default Mutex Detected	rat		downloader, RAT, trojan	100
Asprox/KULUOZ Legacy URL Pattern detected	rat		asprox, KuluoZ, RAT	100
Asprox/KULUOZ URL Pattern detected	rat		asprox, KuluoZ, RAT	100

Sandboxing Challenges

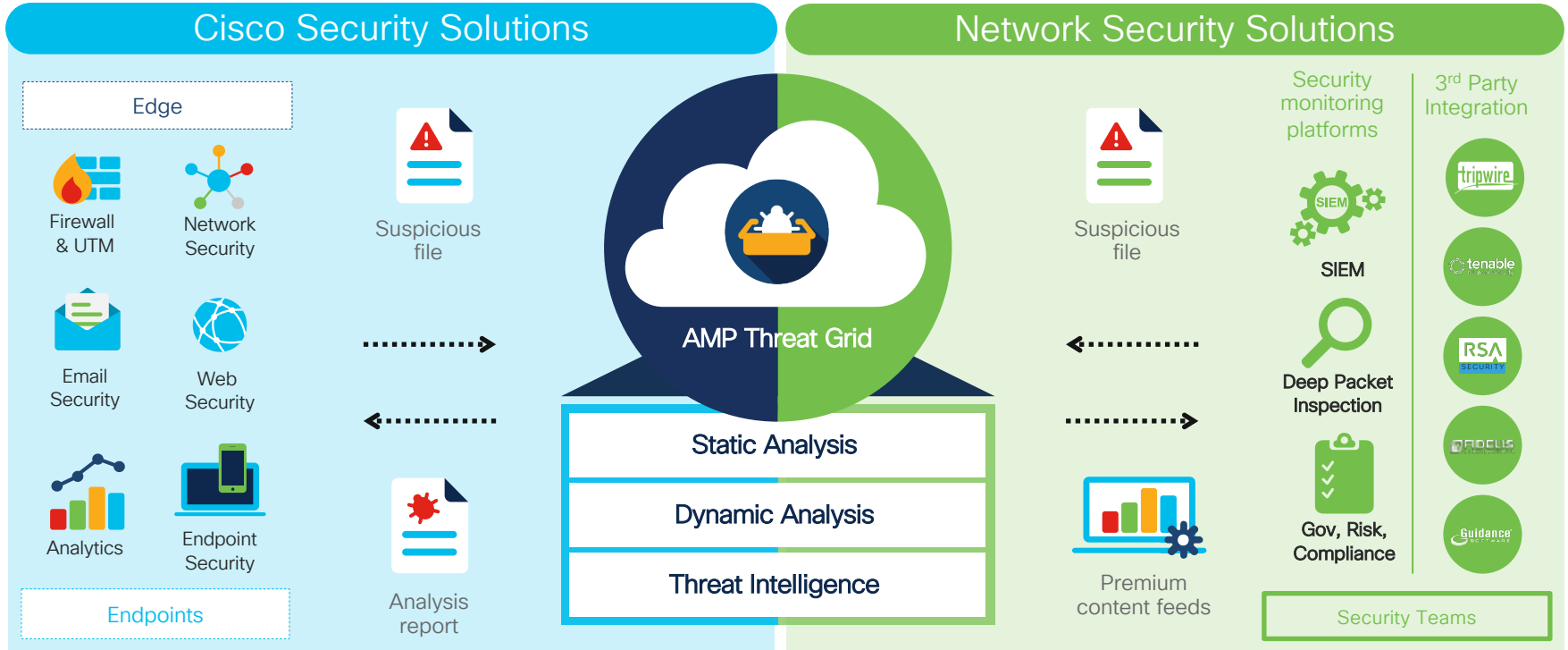
Adversaries Hate Us Analyzing Their Work

Category	Details
Debugger	Checks for debugger with IsDebuggerPresent
Timing	Detects if there is large or small change when calling asm:rdtsc
CPU Flags	Checks the Hypervisor bit, fails if set
Mouse Movement	Detects if mouse moves in 2 sec window
User Artifacts	Download History, Recent Browsing
Registry	Checks registry for "HARDWARE\\Description\\System", Value: "SystemBiosVersion", Data: "QEMU"
Drivers	Check for drivers in %windir%\system32\drivers (vmci.sys, vmhgfs.sys, VBoxMouse.sys, etc.)
Vendor Information	Queries SMBIOS for the "model" name. Can be done via `wmic computersystem get model`
Hardware Checks	Checks the MAC address for one of VMware prefixes:00:05:69, 00:0C:29, 00:1C:14, 00:50:56

How AMP Works Together with Threat Grid

- All AMP for Endpoints customers have the ability to submit samples to Threat Grid.
- This can be done automatically (as an automated action and/or by low prevalence) and manually.
- The AMP Advantage license also includes access to the Threat Grid cloud portal.

Threat Grid Everywhere



Machine Learning Role in Prevention and Detection

- What Machine Learning Is and What it Isn't
- When and Why to Use Machine Learning
- Cisco's Approach to drive increased efficacy

Machine Learning: What It Isn't



Black Box



Robot Apocalypse



Magical Unicorns

https://commons.wikimedia.org/wiki/File:Cube_subspace_3_gray.png
https://commons.wikimedia.org/wiki/File:Campaign_to_Stop_Killer_Robots.jpg
https://commons.wikimedia.org/wiki/File:Twemoji12_1f984.svg

Machine Learning: What It Is


“Field of study that gives computers the ability to learn without being explicitly programmed”

Arthur Samuel's definition of machine learning in 1959

Machine Learning: When To Use?


Static, well-understood domain, limited variability



Machine Learning
not needed 

Evolving, not-well understood domain, large variability



Machine Learning
needed 

Why Use Machine Learning in Cyber Security

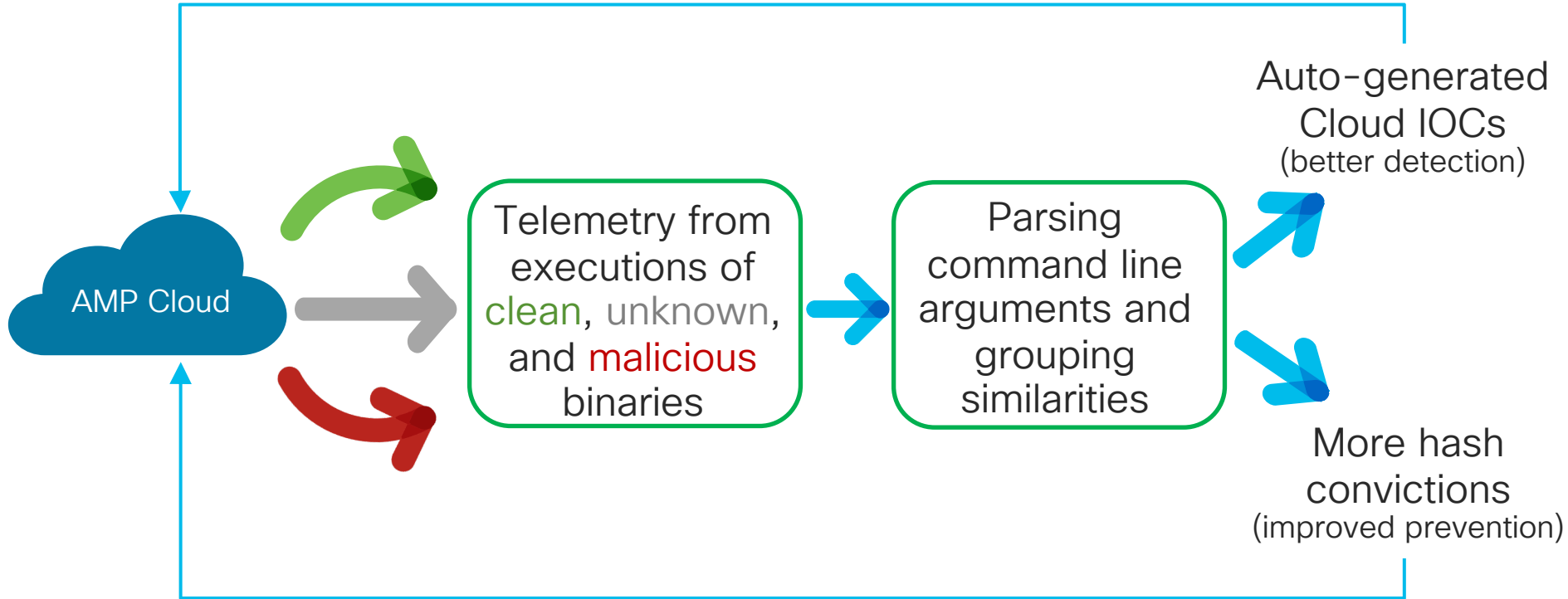
Domain of advanced threats is constantly evolving and is not static

Advanced threats are generally not well understood and novel

The data sets are very large at scale and hide the 1% that matters

The use of Machine Learning is a part of the solution, not the solution by itself.

Endpoint Analysis

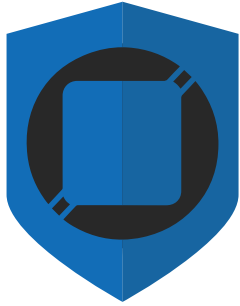


<https://blogs.cisco.com/security/defeating-polymorphic-malware-with-cognitive-intelligence-part-2-command-line-argument-clustering>

Talos Role in Prevention and Detection

- Leading Threat Intelligence
- Backbone of Cisco Security product portfolio
- Forcing the bad guys to innovate

Talos Mission



Cisco Talos' core mission is to provide verifiable and customizable defensive technologies and techniques that help customers quickly protect their assets from cloud to core.

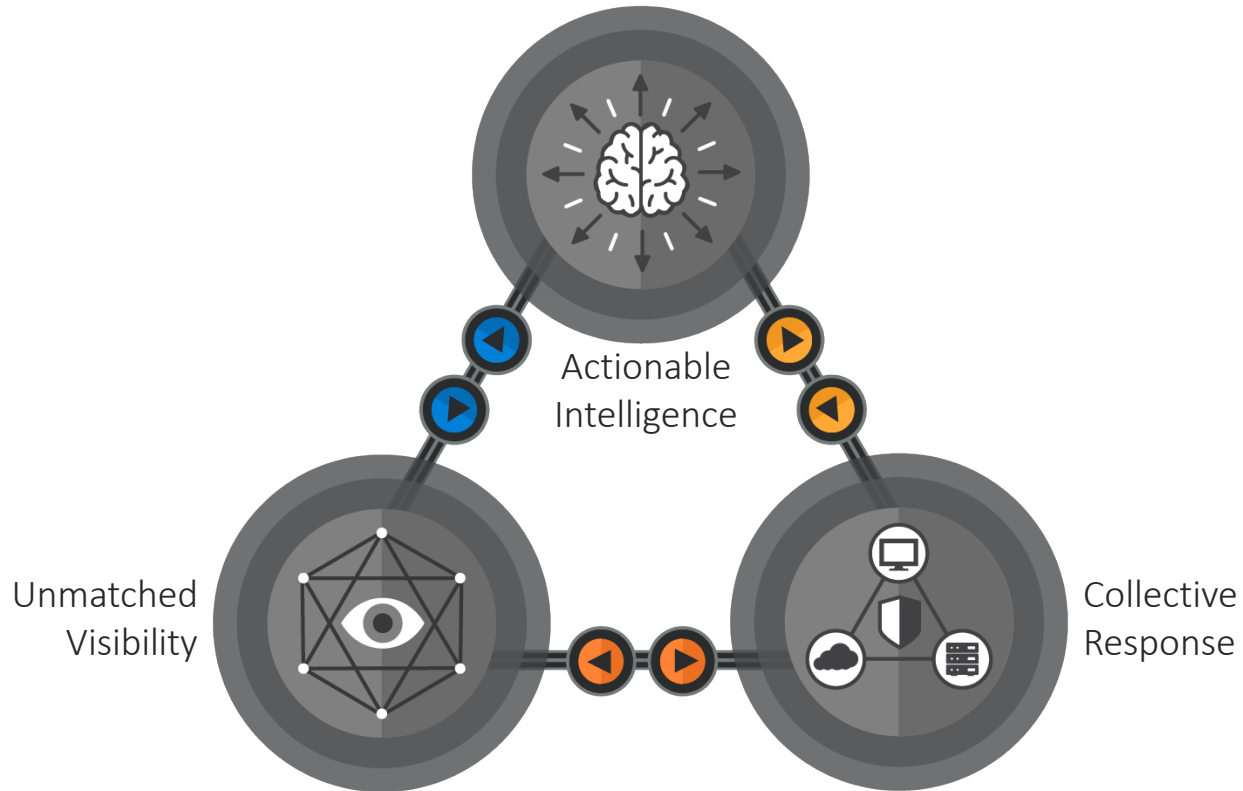
Talos encompasses six key areas:

- Threat Intelligence & Interdiction
- Detection Research
- Engine Development
- Vulnerability Research & Discovery
- Open Source & Education
- Global Outreach



**Our job is
protecting your
network.**

Why trust Talos?



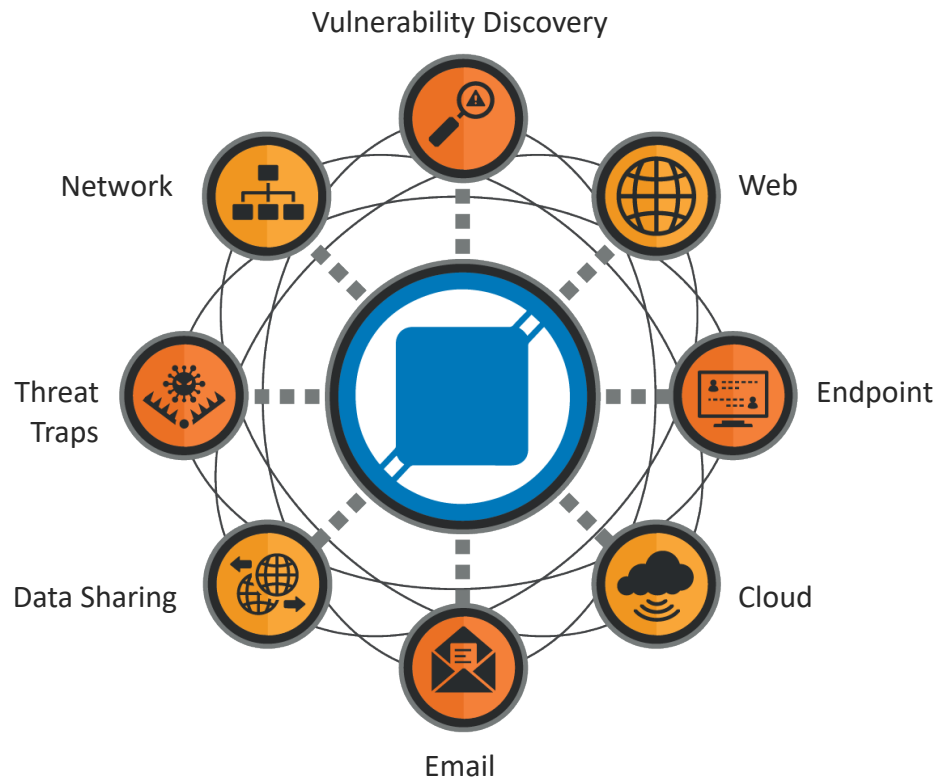


Unmatched Visibility

To stop more, you have to see more.

- The most diverse data set
- Community partnerships
- Proactively finding problems

Unmatched visibility is built on relationships



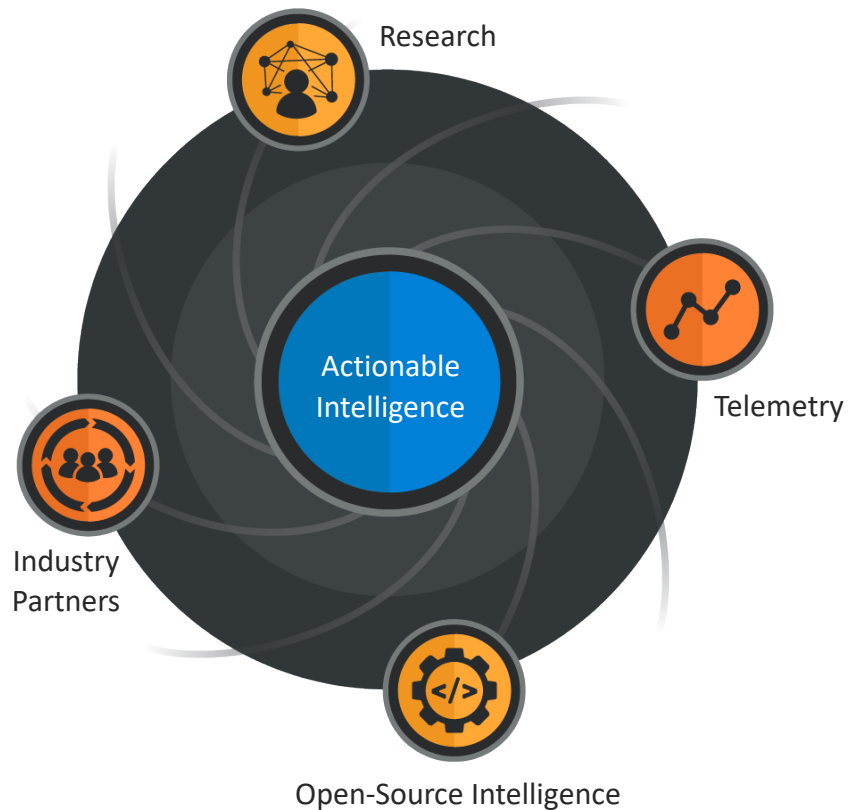


Actionable Intelligence

Security controls are best served by data that lets tools respond to immediate threats.

- Rapid coverage
- Distillation and analysis
- Threat Context

It's not detect and forget, it's detect and analyze.





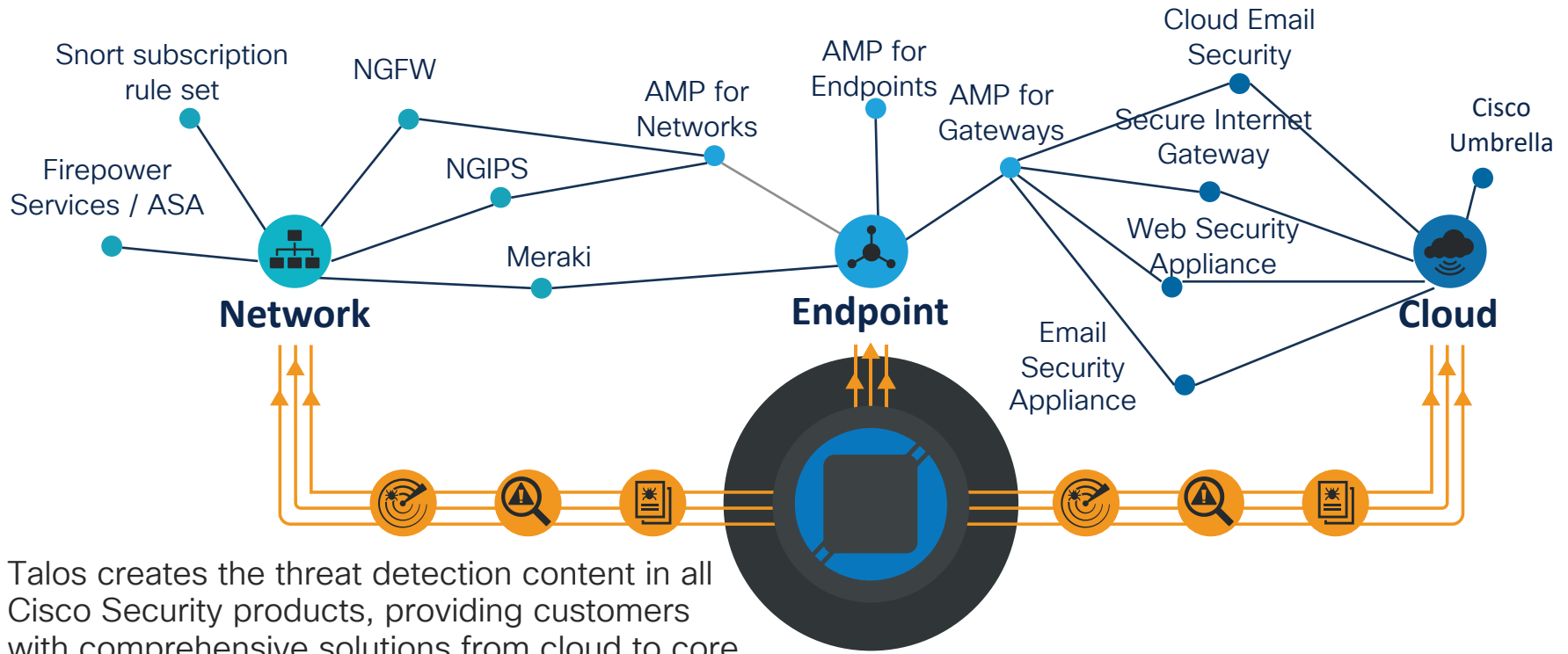
Collective Response

The ability to bring rapid protection to close off multiple attack vectors instantaneously is crucial

- **Breadth:** See once, protect everywhere
- **Depth:** Response and interdiction drives continuous research
- **Scale:** Delivering portfolio-wide protection, in real-time



The Backbone of Cisco Security



Talos creates the threat detection content in all Cisco Security products, providing customers with comprehensive solutions from cloud to core.

Forcing The Bad Guys to Innovate



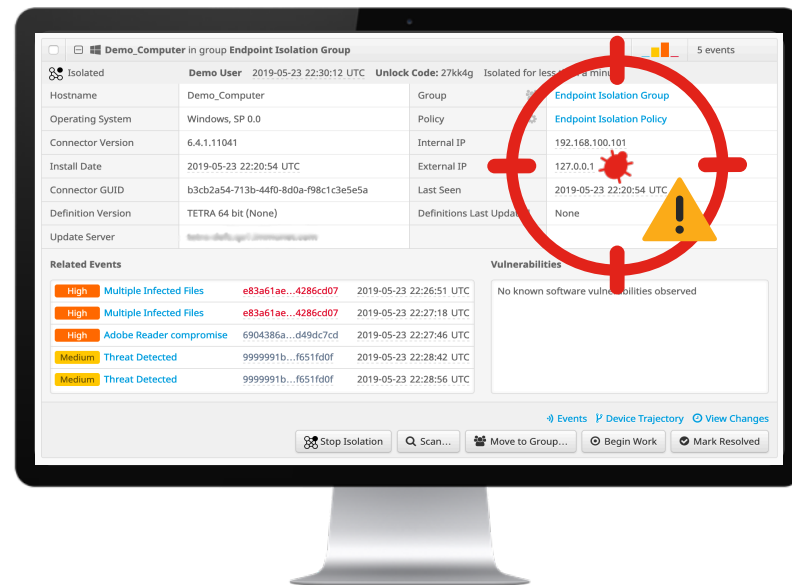
Talos publically shares security information through numerous channels to help make the internet safer for everyone.



Endpoint Isolation

Endpoint Isolation

- Isolate infected hosts from the rest of the network
- Contain the threat without losing forensics data
- Shrink remediation cost by limiting the scale of attack
- Fast endpoint reactivation once remediation is complete
- Automated Actions for isolation and data collection



Contain attack fast

Key Features

- Controlled by portal or API
- Isolates IPv4 and IPv6
- Allows for IP Whitelisting
 - Cisco AMP IPs are implicitly whitelisted
- Local Manual De-Isolation available via unique code
- DFC monitoring still works
- Prevents uninstall and/or upgrade during Isolation

Create an Allow IP List

Create a new list

Outbreak Control >
Network - IP
Blocked and Allowed
Lists

Enter CIDR Blocks

Add your own
special management
IP's for remediation
(optional)

The screenshot shows the Cisco AMP for Endpoints interface. The breadcrumb trail is Dashboard > Analysis > Outbreak Control > Management > Accounts. The page title is 'New IP List'. The form fields are:

- Name: EPIsolationAllowList
- Description: Allow these IP's when Endpoint is isolated
- List Type: Allowed

The 'IPs and CIDR Blocks' table contains the following entries:

IPs and CIDR Blocks	Actions
10.1.100.0/24	CIDR, Delete
172.28.57.0/24	CIDR, Delete

Buttons at the bottom: + Add Row, + Add Multiple Rows..., Upload..., Save.

Add the Allowed IP List(s)

Endpoint Isolation

In the Advanced Settings section

Select your list

From the drop down

< Edit Policy
Windows

Name: Endpoint Isolation Policy
Description: Imported policy settings from ATW-WindowsPolicy.

Modes and Engines

Exclusions
1 exclusion set

Proxy

Outbreak Control

Product Updates

Advanced Settings

- Administrative Features
- Client User Interface
- File and Process Scan
- Cache
- Endpoint Isolation ^{BETA}**
- Engines
- TETRA
- Networks

Endpoint Isolation

Allow Endpoint Isolation ⓘ

Allowed IP Lists

Clear Select Lists

1 + EPIsolationAllowList

Allow notifications to end-user

Client User Interface

Where the notifications are configured

Uncheck this

System Process Protection Notifications are used for Endpoint Isolation

< Edit Policy
Windows

Name: Endpoint Isolation Policy

Description: Imported policy settings from ATW-WindowsPolicy.

Modes and Engines

Exclusions
1 exclusion set

Proxy

Outbreak Control

Product Updates

Advanced Settings

- Administrative Features
- Client User Interface**
- File and Process Scan
- Cache
- Endpoint Isolation ^{BETA}
- Engines
- TETRA

Start Client User Interface ⓘ

Cloud Notifications ⓘ

Hide Cataloging Notifications ⓘ

Hide File Notifications ⓘ

Hide Network Notifications ⓘ

Hide System Process Protection Notifications ⓘ

Hide Exploit Prevention Notifications ⓘ

Hide Malicious Activity Protection Notifications ⓘ

Hide Exclusions ⓘ

Start isolation from the computers page

Endpoint Isolation Policy

New policy copied from existing

The screenshot displays a device card for 'loxx-surfacepro' in the 'Endpoint Isolation Group'. The card shows the device is 'Within Policy'. Below the card is a table with the following data:

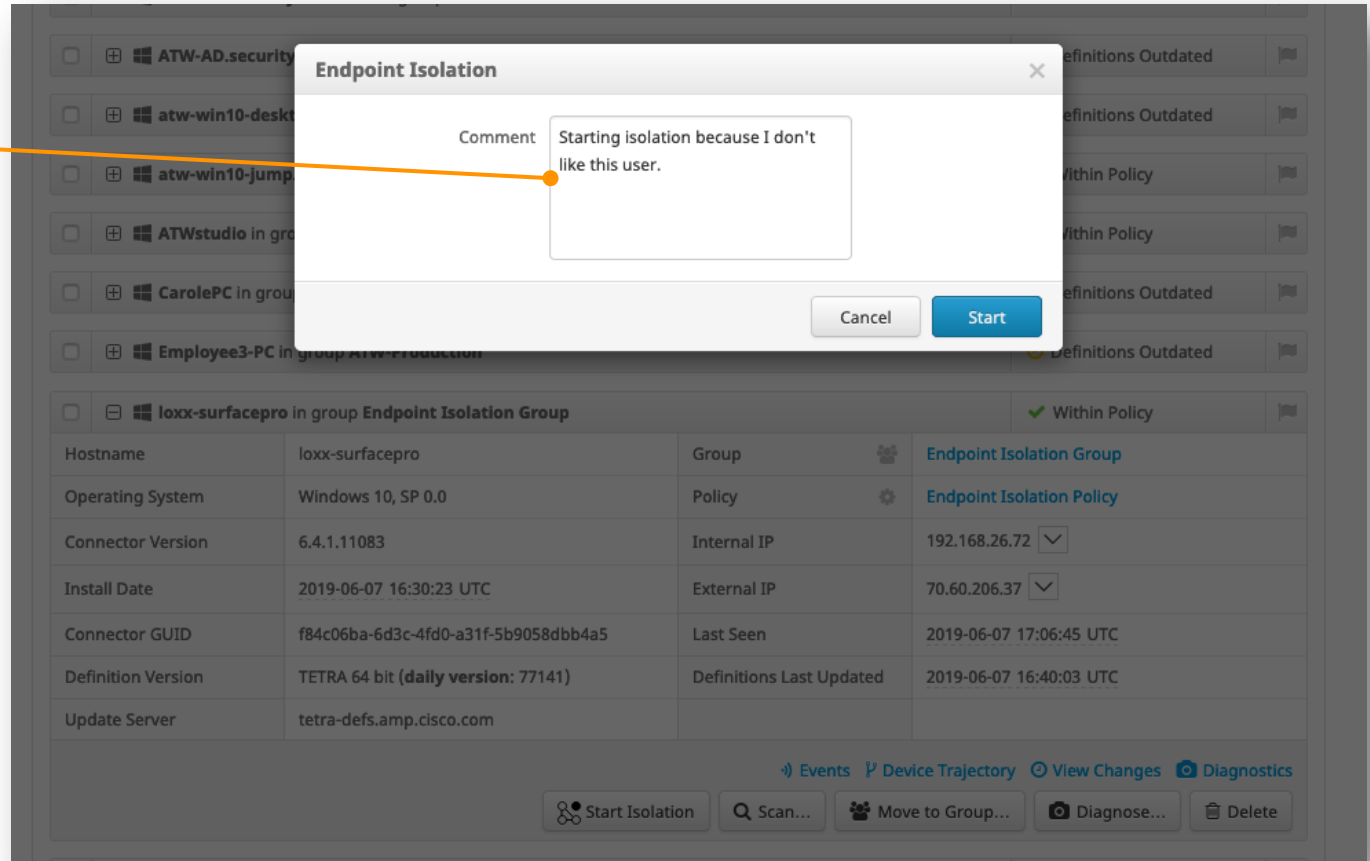
Hostname	loxx-surfacepro	Group	Endpoint Isolation Group
Operating System	Windows 10, SP 0.0	Policy	Endpoint Isolation Policy
Connector Version	6.4.1.11083	Internal IP	192.168.26.72
Install Date	2019-06-07 16:30:23 UTC	External IP	70.60.206.37
Connector GUID	f84c06ba-6d3c-4fd0-a31f-5b9058dbb4a5	Last Seen	2019-06-07 17:06:45 UTC
Definition Version	TETRA 64 bit (daily version: 77141)	Definitions Last Updated	2019-06-07 16:40:03 UTC
Update Server	tetra-defs.amp.cisco.com		

At the bottom of the interface, there are navigation links: Events, Device Trajectory, View Changes, and Diagnostics. Below these are action buttons: Start Isolation, Scan..., Move to Group..., Diagnose..., and Delete.

Click start to isolate the endpoint

Comment

Has field for comments on why the endpoint was put into isolation.



The screenshot shows the Cisco Secure Endpoint console interface. A modal dialog titled "Endpoint Isolation" is open, allowing a user to isolate an endpoint. The dialog includes a "Comment" field where the user has entered "Starting isolation because I don't like this user." Below the comment field are "Cancel" and "Start" buttons. An orange arrow points from the "Comment" label to the text in the input field. The background shows a list of endpoints, with the selected endpoint "loxx-surfacepro" displayed in a detailed view below the dialog.

Hostname	loxx-surfacepro	Group	Endpoint Isolation Group
Operating System	Windows 10, SP 0.0	Policy	Endpoint Isolation Policy
Connector Version	6.4.1.11083	Internal IP	192.168.26.72
Install Date	2019-06-07 16:30:23 UTC	External IP	70.60.206.37
Connector GUID	f84c06ba-6d3c-4fd0-a31f-5b9058dbb4a5	Last Seen	2019-06-07 17:06:45 UTC
Definition Version	TETRA 64 bit (daily version: 77141)	Definitions Last Updated	2019-06-07 16:40:03 UTC
Update Server	tetra-defs.amp.cisco.com		

Endpoint is isolated

Who + comment

Who isolated the endpoint & what comment they added

Unlock Codes!

Just in case, a unique code is generated for the end user to remove themselves from isolation. Helpdesk would give this code to “stuck user”

How long?

How long endpoint has been isolated

loxx-surfacepro in group Endpoint Isolation Group		Within Policy
Isolated	Aaron Woland 2019-06-07 17:12:36 UTC	Unlock Code: hox28w Isolated for 2 minutes
Starting isolation because I don't like this user.		
Hostname	loxx-surfacepro	Group Endpoint Isolation Group
Operating System	Windows 10, SP 0.0	Policy Endpoint Isolation Policy
Connector Version	6.4.1.11083	Internal IP 192.168.26.72
Install Date	2019-06-07 16:30:23 UTC	External IP 70.60.206.37
Connector GUID	f84c06ba-6d3c-4fd0-a31f-5b9058dbb4a5	Last Seen 2019-06-07 17:13:13 UTC
Definition Version	TETRA 64 bit (daily version: 77141)	Definitions Last Updated 2019-06-07 16:40:03 UTC
Update Server	tetra-defs.amp.cisco.com	

Free the endpoint

Stopping isolation

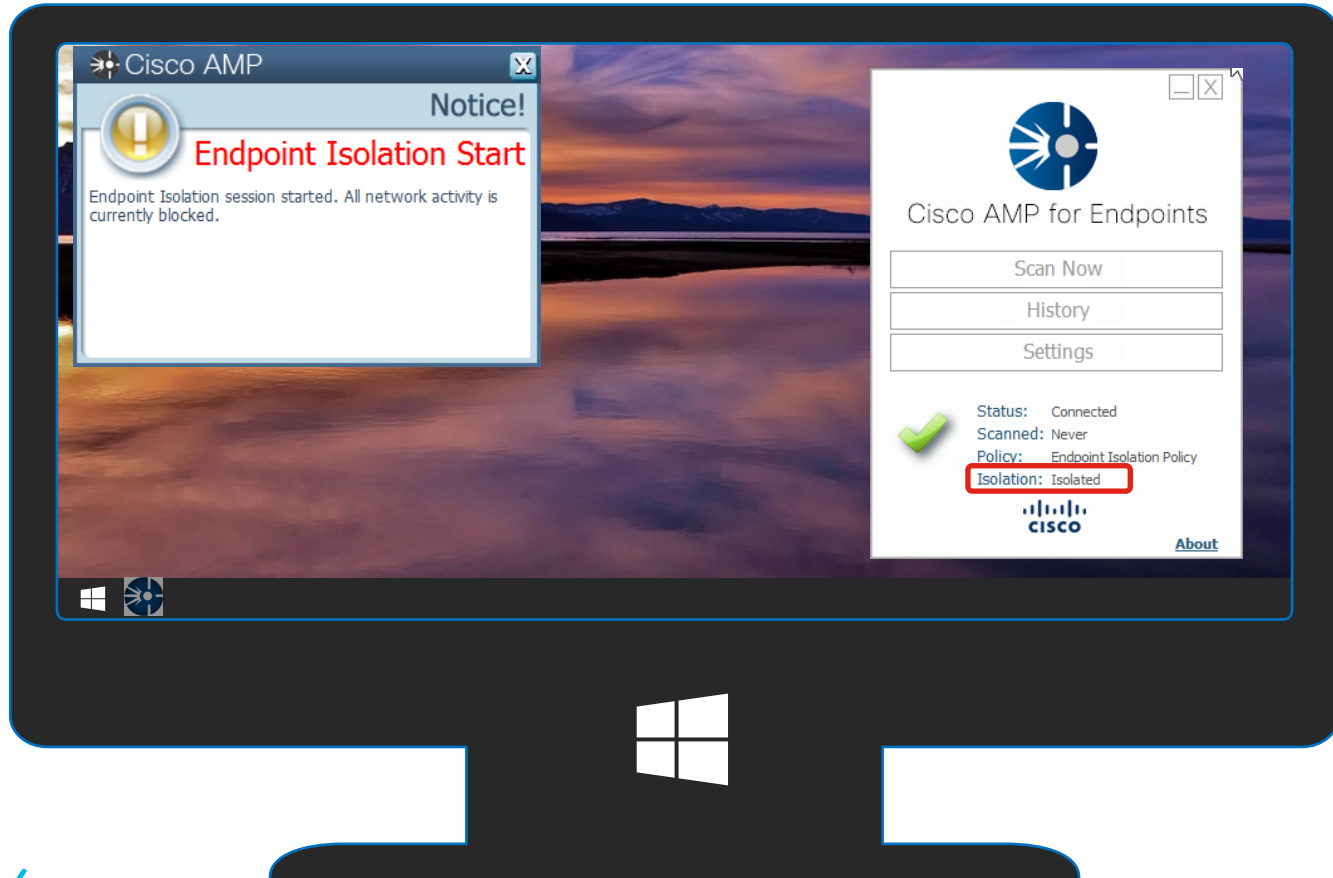
Comment

Has field for comments on why the endpoint was released from isolation

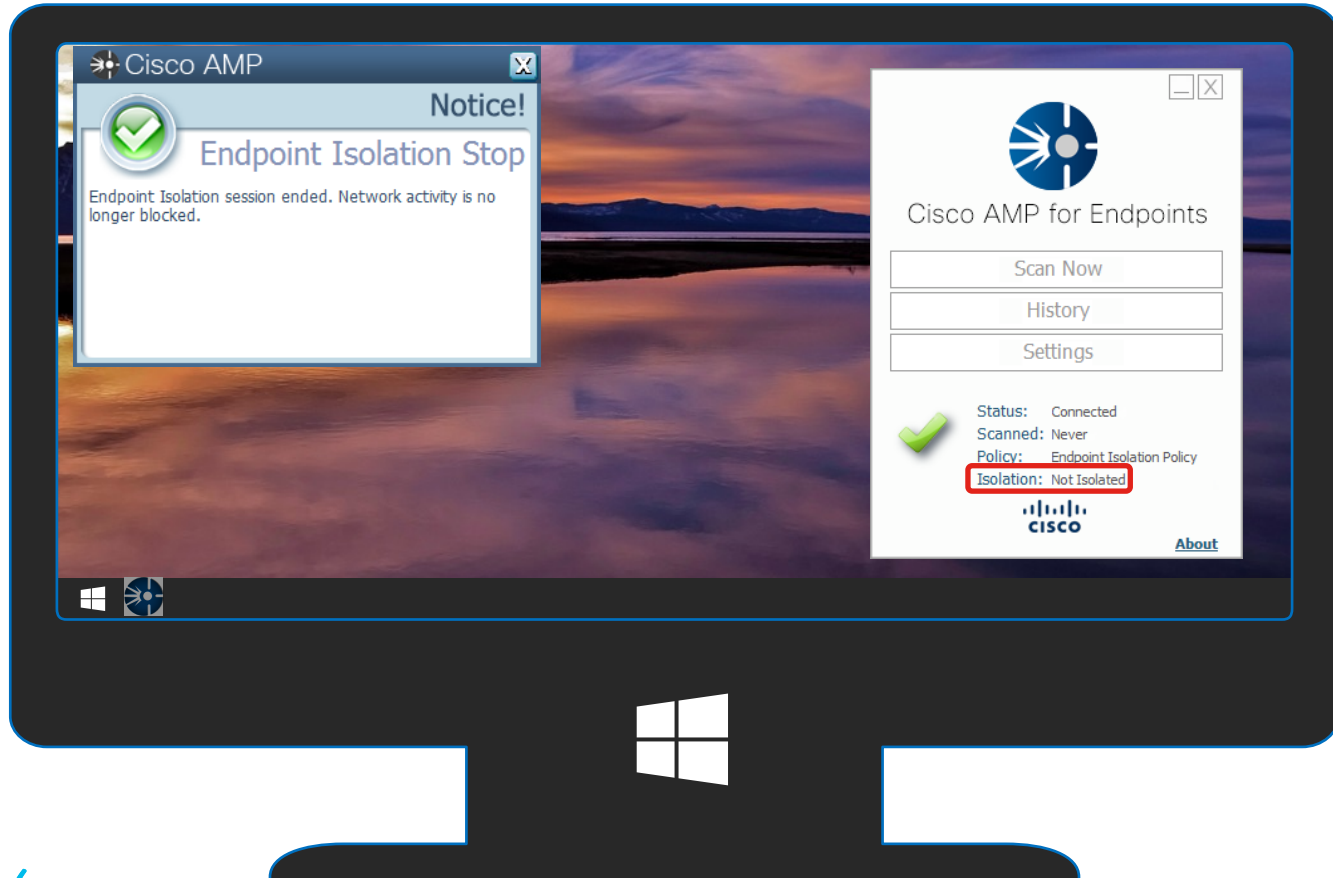
The screenshot displays the Cisco Duo interface. A modal dialog box titled "Endpoint Isolation" is open, featuring a "Comment" field with the text "Freeing the jailed machine!". Below the field are "Cancel" and "Stop" buttons. An orange line connects the "Comment" label in the text to the input field in the dialog. The background shows a list of endpoints, with the selected endpoint "loxx-surfacepro" in group "Endpoint Isolation Group" highlighted. Below the endpoint name, it shows "Isolated" status, user "Aaron Woland", and a timestamp. A table of details is visible below, including Hostname, Operating System, Connector Version, Install Date, Connector GUID, Definition Version, and Update Server. At the bottom, a "Stop Isolation" button is highlighted with a blue box, along with other action buttons like "Scan...", "Move to Group...", "Diagnose...", and "Delete".

Hostname	loxx-surfacepro	Group	Endpoint Isolation Group
Operating System	Windows 10, SP 0.0	Policy	Endpoint Isolation Policy
Connector Version	6.4.1.11083	Internal IP	192.168.26.72
Install Date	2019-06-07 16:30:23 UTC	External IP	70.60.206.37
Connector GUID	f84c06ba-6d3c-4fd0-a31f-5b9058dbb4a5	Last Seen	2019-06-07 17:13:13 UTC
Definition Version	TETRA 64 bit (daily version: 77141)	Definitions Last Updated	2019-06-07 16:40:03 UTC
Update Server	tetra-defs.amp.cisco.com		

End user experience – Isolation Start



End user experience – Isolation Stop



End user experience – Stop isolation via CLI

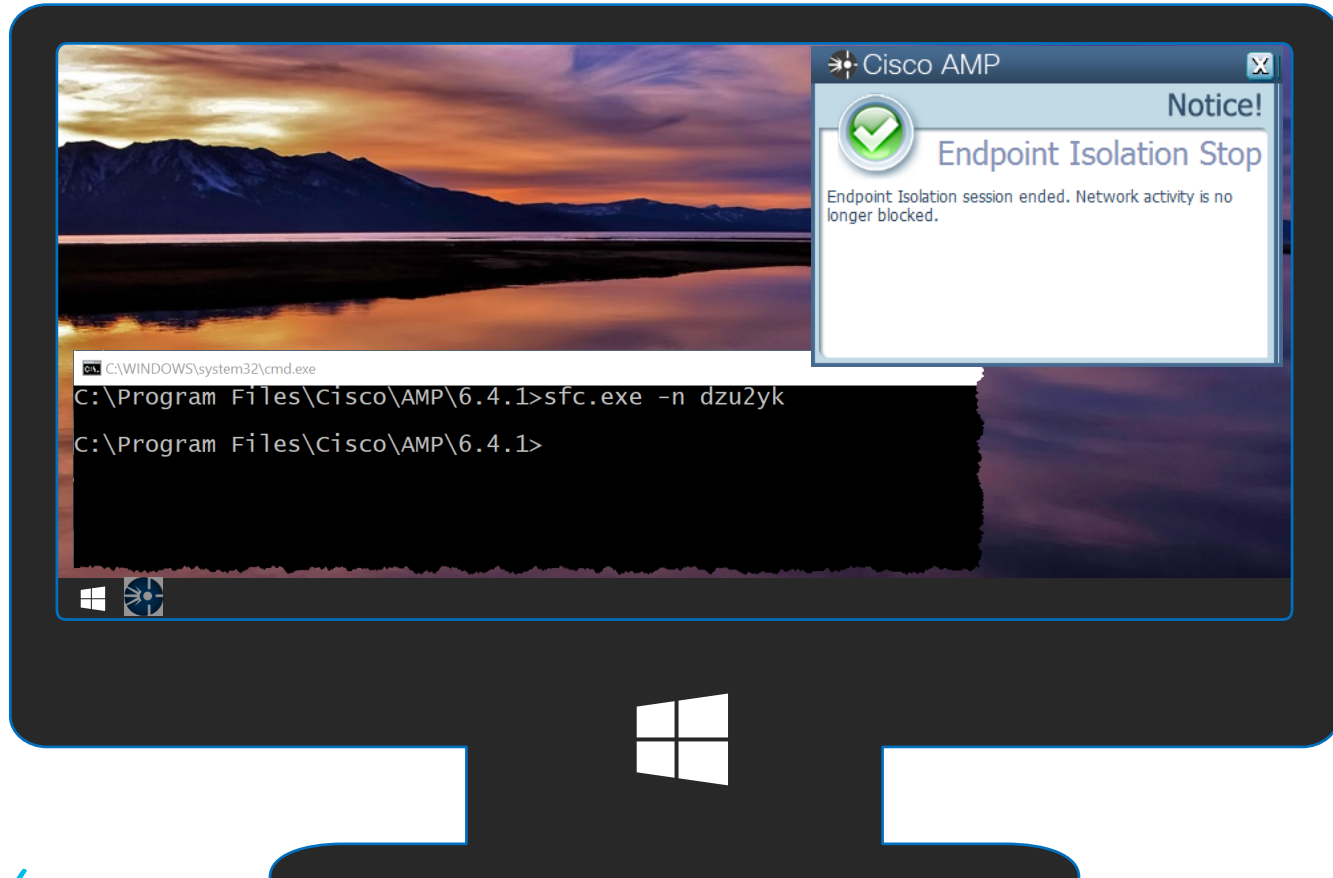


The screenshot shows the Cisco AMP console interface for a device named "loxx-surfacepro" in the "Endpoint Isolation Group". The device is in an "Isolated" state. A red box highlights the "Unlock Code: dzu2yk" in the top right corner. Below this, a message states "Isolating to show the CLI release." A table of device details is shown below:

Hostname	loxx-surfacepro	Group
Operating System	Windows 10, SP 0.0	Policy
Connector Version	6.4.1.11083	Internal IP
Install Date	2019-06-07 16:30:23 UTC	External IP
Connector GUID	f84c06ba-6d3c-4fd0-a31f-5b9058dbb4a5	Last Seen
Definition Version	TETRA 64 bit (daily version: 77141)	Definitions Last
Update Server	tetra-defs.amp.cisco.com	

At the bottom of the console, there are buttons for "Stop Isolation" and "Scan...".

End user experience – Stop isolation via CLI



Isolation from CTR

Threat Response

Cisco Threat Response (CTR) adding Host-Isolation-AMP actions

Relations Graph Showing 89 nodes

Target
Windows Server 2016, S...
Targeted by 1 unique threat, 100 times in the last 2 days

Hostname
ERP-WIN-DC1

AMP Computer GUID
048e2204-0979-4f86-9949-...

IP Address
192.168.189.130

MAC Address
00:0c:29:cb:c3:a8

048e2204-0979-4f86-9949-1d7f9f55fa06
AMP GUID

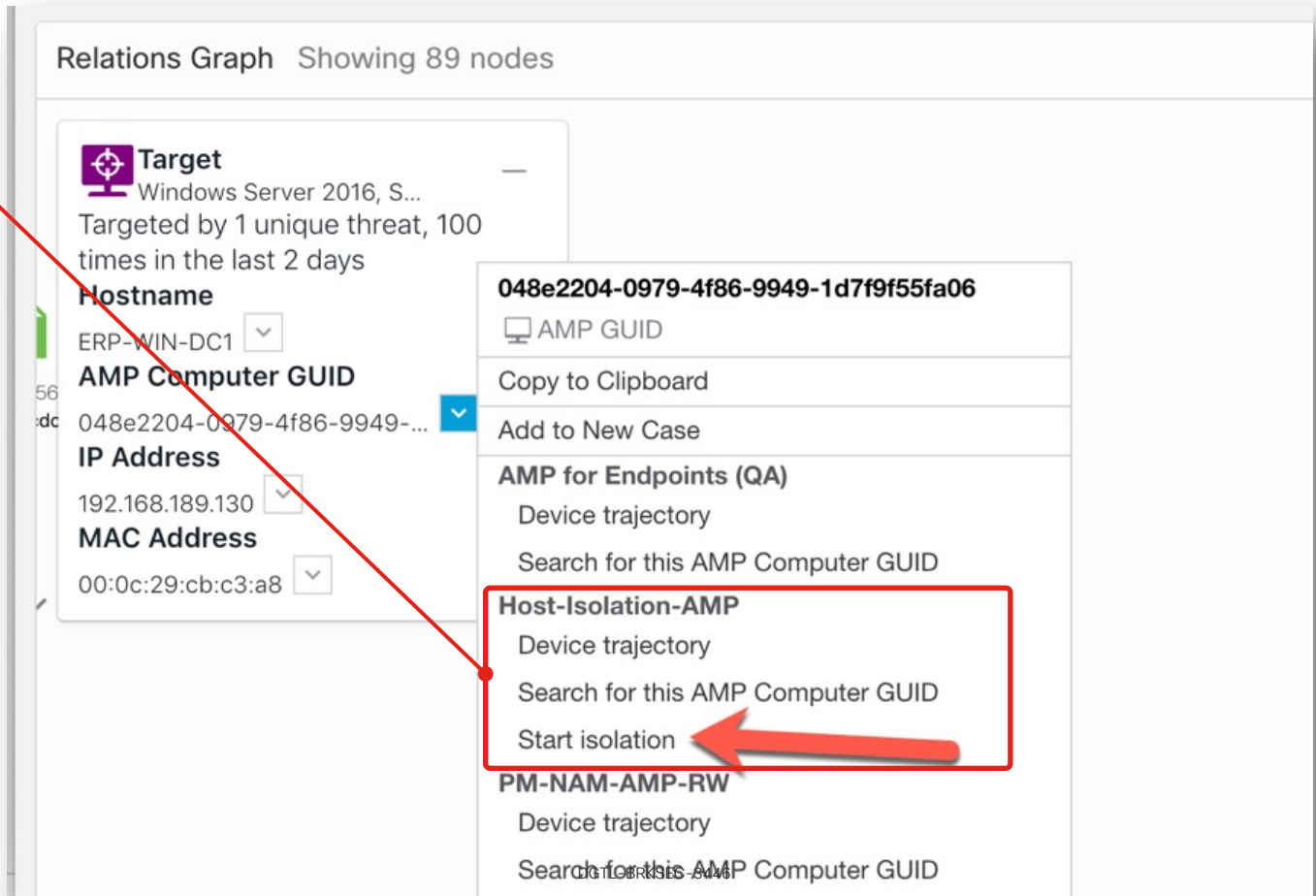
Copy to Clipboard

Add to New Case

AMP for Endpoints (QA)
Device trajectory
Search for this AMP Computer GUID

Host-Isolation-AMP
Device trajectory
Search for this AMP Computer GUID
Start isolation

PM-NAM-AMP-RW
Device trajectory
Search for this AMP Computer GUID



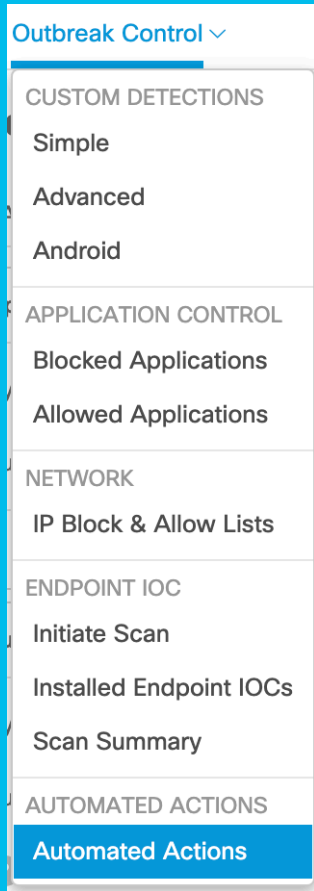
Other details

- Stays on, even if sfc.exe stopped
- While Isolated
 - Cannot Upgrade
 - Cannot Uninstall
 - Can only be disabled locally by unique code generated randomly each session

Other details

- Current support is for Windows systems only
 - Connector version 7.05 or newer
 - macOS support will follow
- Only shows pop-up for users with UI enabled
 - Written to system log

Automated Actions



- Automated Actions can be defined based on event severity and host group.
- Actions include:
 - Orbital forensic snapshot
 - Endpoint isolation
 - Threat Grid submission
 - Move system to different policy group

▼ Isolate a Computer upon Compromise (5 computers in the selected groups can be isolated.)

High severity or higher in groups 25 selected ▾

0 Compromise Events occurred in the last 7 days, affecting 0 distinct computers in the selected groups.

Rate Limit 10 ?

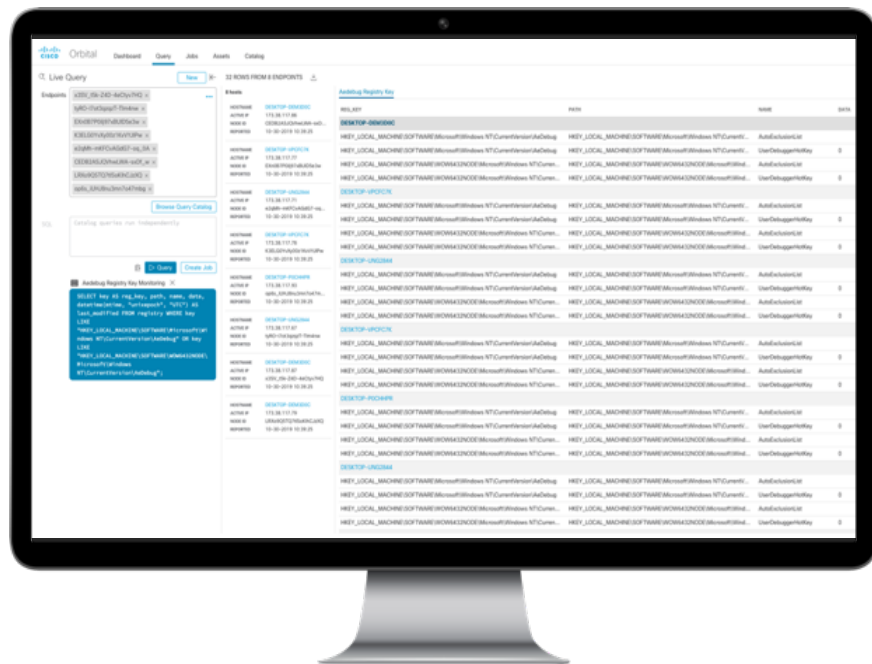
The Rate Limit must be between 1 and 1000.



Orbital Advanced Search

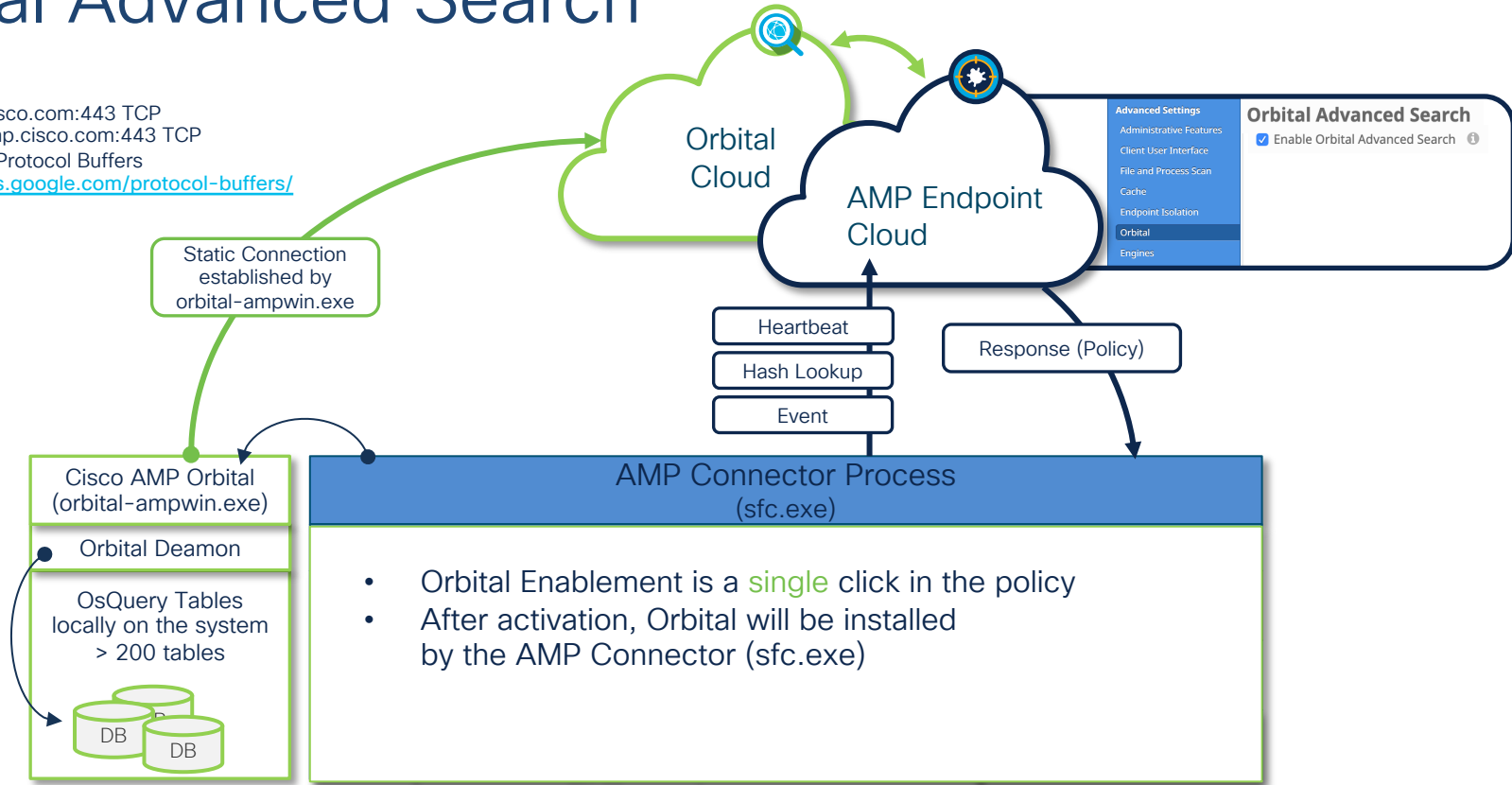
Orbital Advanced Search

- Run complex queries on your endpoints for threat indicators
- Run live search on demand or on a schedule
- Get the answers you need about your endpoints in near real time
- Store queries in the cloud or apps like Cisco Threat Response



Orbital Advanced Search

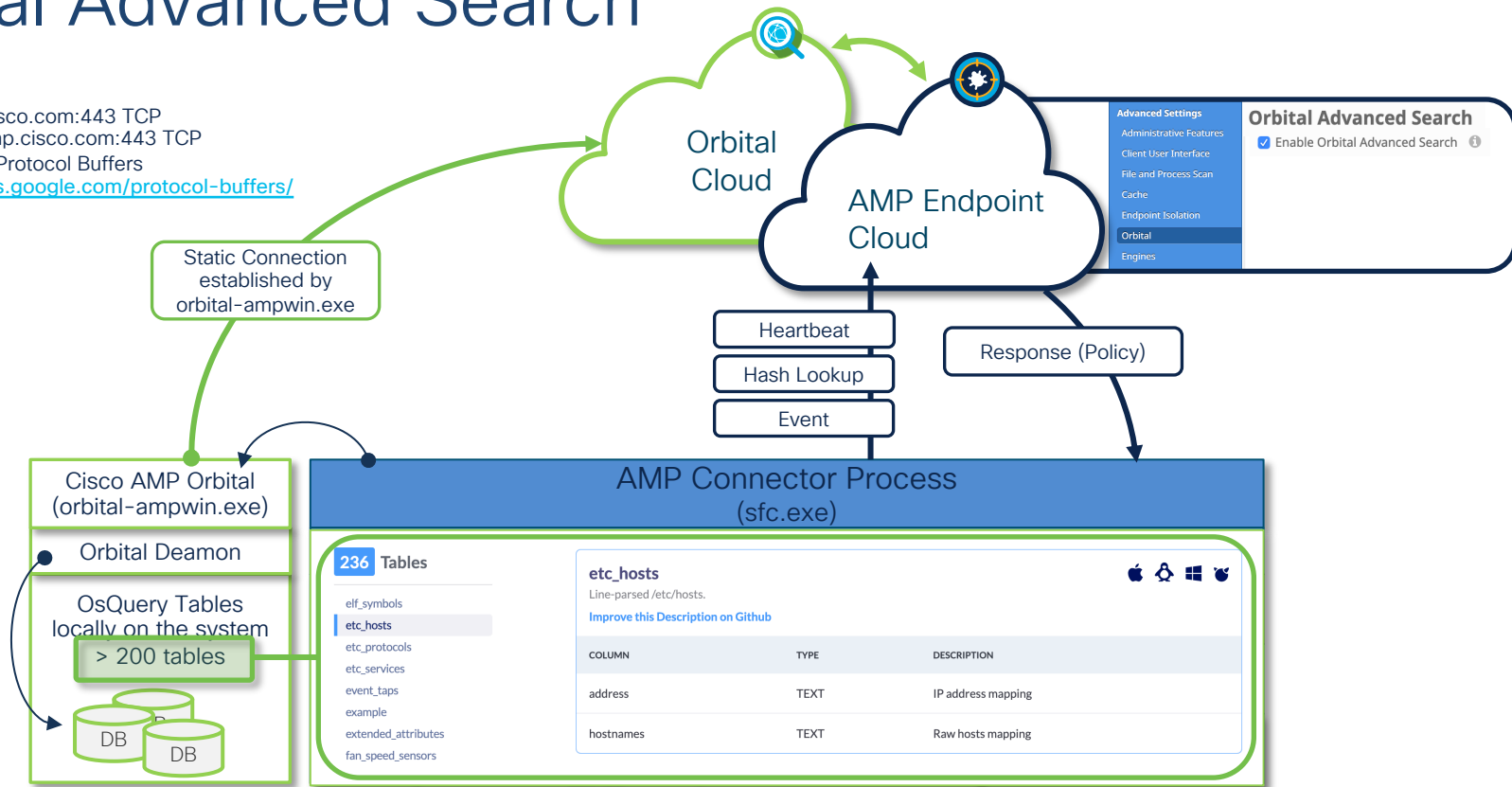
- orbital[.eu].amp.cisco.com:443 TCP
- ncp[.eu].orbital.amp.cisco.com:443 TCP
- Based on Google Protocol Buffers
<https://developers.google.com/protocol-buffers/>



- Orbital Daemon constantly adds information into the Orbital Databases
- SQL-Lite is used
- <https://www.osquery.io/schema/4.1.2>

Orbital Advanced Search

- orbital[.eu].amp.cisco.com:443 TCP
- ncp[.eu].orbital.amp.cisco.com:443 TCP
- Based on Google Protocol Buffers
<https://developers.google.com/protocol-buffers/>

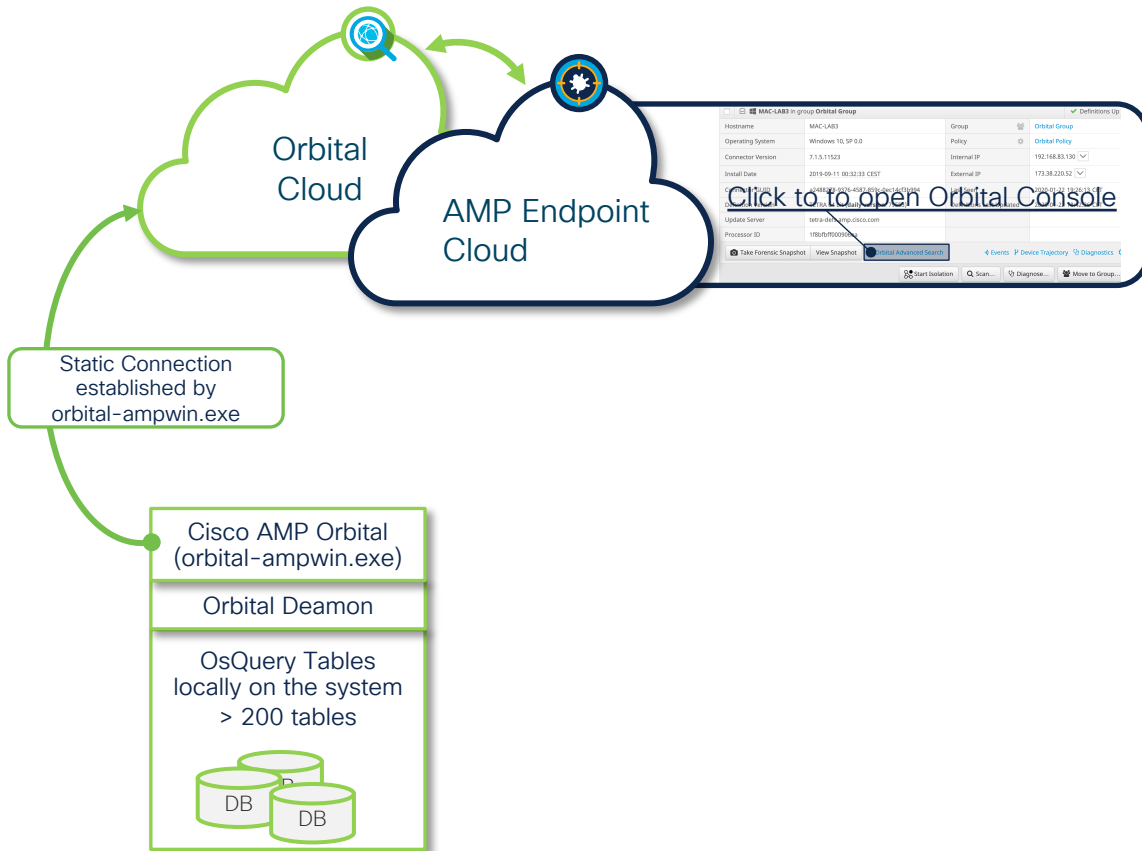


- Orbital Daemon constantly adds information into the Orbital Databases
- SQL-Lite is used
- <https://www.osquery.io/schema/4.1.2>

Live Query

The screenshot shows the Cisco AMP Orbital console interface. At the top, there are navigation tabs: "Query", "Jobs", "Assets", and "Catalog". Below the tabs, there is a search bar labeled "Live Query" with a "New" button. Underneath, there is a field for "Endpoints" containing a sample MAC address: "amp:a2488278-9376-4587-859c-0ec14cf3...". A "Browse Query Catalog" button is located below the endpoint field. A green arrow points from the endpoint field to a list of query filters:

- host:<hostname>
- ip:<IP-address, type auto-detected>
- ip4:<IPv4-address>
- ip6:<IPv6-address>
- mac:<MAC-address>
- os: <operating-system: darwin,linux,windows>
- all



The screenshot shows a detailed view of a host's configuration in the AMP console. The host name is "MAC-A8B3 in group Orbital Group". The configuration includes fields for Hostname, Operating System, Connector Version, Install Date, Update Server, and Processor ID. A call to action "Click to open Orbital Console" is overlaid on the screenshot.

Live Query

Orbital

Query Jobs Assets Catalog

Live Query New

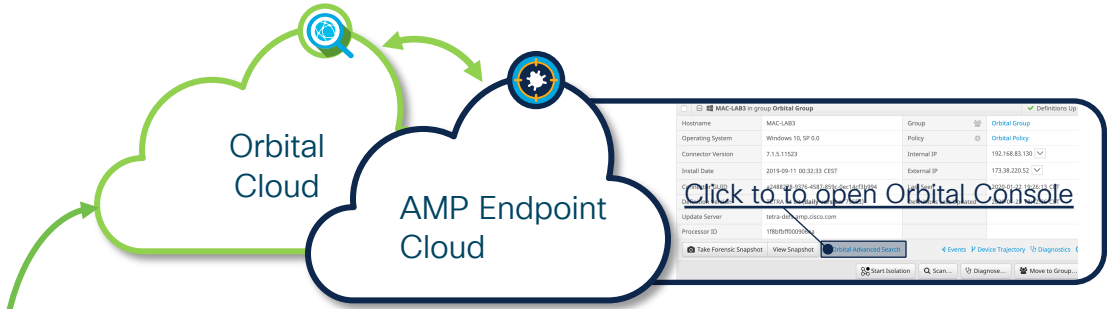
Endpoints .amp:a2488278-9376-4587-859c-0ec14cf3... x

Browse Query Catalog

SQL

Enter SELECT statement

Query Create Job



Query Catalog ×

Back

Hosts File Monitoring

Created by Cisco 2019-02-12. Updated 2019-08-15.

This query is applicable to Windows, Linux and MacOS. The hosts file is the local host database which is checked before a name resolution request is sent to a DNS server. A host entry consists of a hostname, and it's corresponding IP address. It is often used by the malware authors to redirect traffic from the intended destination to sites hosting malicious or unwanted content. It may also be used to block legitimate content such as AV signature updates. On the other hand, it can be used legitimately, and this query may need to be customized to exclude legitimate entries.

ID etc_hosts_monitoring

OS Windows, Linux, Darwin

Categories Posture Assessment

ATT&CK™ Techniques Fallback Channels Web Service

ATT&CK™ Tactics Command and Control

+

1 Catalog queries are designed to run independently.

SQL

```
SELECT address, hostnames FROM etc_hosts WHERE hostnames NOT IN ("localhost", "::1", "fe00::0", "ff00::0", "ff02::1", "ff02::2");
```

Live Query



Orbital

Query

Jobs

Assets

Catalog

tschranz+us@cisco.com

Live Query

New

2 ROWS FROM 1 ENDPOINT

Endpoints .amp:a2488278-9376-4587-859c-0ec14cf3... x

Browse Query Catalog

SQL Catalog queries run independently

Query

Create Job

Hosts File Monitoring

```
SELECT address, hostnames FROM etc_hosts
WHERE hostnames NOT IN ("localhost",
"::1", "fe00::0", "ff00::0", "ff02::1",
"ff02::2");
```

1 host

HOSTNAME	MAC-LAB3
ACTIVE IP	173.38.220.59
NODE ID	70E5SD4rr8FD7ZocP4f9yQ
REPORTED	2020-01-23 13:06:18

Hosts File Data

ADDRESS	HOSTNAMES
MAC-LAB3	
127.0.0.1	found.by.Orbital.cisco.com
127.0.0.1	TECSEC-2599.cisco.live.2020.barcelona

Predefined Query Catalog



Orbital

Query Jobs Assets **Catalog**

tschranz+us@cisco.com

Query Catalog

Filters [Reset](#)

> Categories

> ATT&CK™ Tactics

▼ ATT&CK™ Techniques

- .bash_profile and .bashrc
- Access Token Manipulation
- Accessibility Features
- Account Discovery
- Account Manipulation
- AppCert DLLs
- AppInit DLLs
- AppleScript
- Application Deployment Software
- Application Shimming
- Application Window Discovery
- Audio Capture
- Authentication Package
- Automated Collection
- Automated Exfiltration
- Bash History
- Binary Padding

hosts

NAME	CREATED	UPDATED	ID	OS	CATEGORY	ATT&CK™ TACTIC	ATT&CK™ TECHNIQUE
> Hosts File Monitoring	2019-02-12	2019-08-15	etc_hosts_monitoring	Windows, Linux, Darwin	Posture Assessment	Command and Control	Fallback Channels Web Service
> Parent Process Not Wininit	2019-01-29	2019-08-16	parent_process_not_wininit	Windows, Linux, Darwin	Threat Hunting	Execution Defense Evasion	Masquerading
> Malware Bernew Registry Monitoring	2019-08-21	2019-08-22	malware_bernew_registry_monitoring	Windows	Malware	Persistence	Registry Run Keys / Startup Folder
> Malware ShadowRat Detected	2019-07-24	2019-08-19	malware_shadowrat_detected	Windows	Malware Threat Hunting	Persistence	Service Registry Permissions Weakness
> Malware Trickbot Mutex Detected	2019-07-26	2019-08-14	malware_trickbot_mutex_detected	Windows	Threat Hunting Malware	Persistence	
> Registry Network Shares Monitoring	2019-08-26	2019-09-04	registry_network_shares_monitoring	Windows	Posture Assessment Forensics	Persistence Collection Discovery Defense Evasion	Data from Network Shared Drive Network Share Discovery Network Share Connection Removal
> Microsoft Office Macros Registry Keys Monitoring	2019-09-03	2019-09-04	registry_office_security_monitoring	Windows	Posture Assessment Forensics Threat Hunting	Persistence Execution Defense Evasion	Office Application Startup Masquerading
> Host Uptime Search	2019-05-15	2019-07-23	uptime_based_search	Windows, Linux, Darwin	Posture Assessment		

< 1 >

Orbital and Threat Grid Cloud

Orbital Cloud

Threat Grid Cloud

Only show Indicators with Orbital queries

Title	Orbital Queries	Score
Snort Triggered On A Domain Flagged Malicious By Umbrella	Orbital Queries	95
Registry Persistence Mechanism Refers to an Executable in a Temporary Folder	Orbital Queries	90
Process Modified Autorun Registry Key Value	Orbital Queries	45

Registry Persistence Mechanism Refers to an Executable in a Temporary Folder

Score: 90 Hits: 1

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 the 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 executable in a temporary directory.

Process	Process Name	RegKey Name	RegKey Value Name	RegKey Data Type	RegKey Data	Actions
Process 30	SqGGuYXyy.exe	MACHINE\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN	overdrive	SZ	C:\Users\ADMINI~1\AppData\Local\Temp\overdrive.exe\0	Orbital Query

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 and Threat Grid



Export the whole Report as .JSON File

Query for all active endpoints

Predefined Query Statement by Threat Grid using table registry

Parameters to refine the query statement

The Registry key is not available on any of the queried endpoints

0 ROWS FROM 3 ENDPOINTS

HOSTNAME	MAC-LAB3
ACTIVE IP	173.38.220.59
NODE ID	70ESSD4rr8FD7ZocP4f9yQ
REPORTED	2020-01-23 14:40:51

HOSTNAME	MAC-LAB2
ACTIVE IP	173.38.220.59
NODE ID	xSBnuYTqJyRnlU7awR5hgz
REPORTED	2020-01-23 14:40:51

HOSTNAME	mac-lab1
ACTIVE IP	173.38.220.59
NODE ID	g_xgRbmYmDcFdr4OeQU...
REPORTED	2020-01-23 14:40:51

REG_KEY	PATH	NAME	DATA
MAC-LAB3			No results for this host.
MAC-LAB2			No results for this host.
mac-lab1			No results for this host.

```
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\SOFTWARE

reg_key_value: overdrive

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



Endpoint Security in the Larger Context



Agenda

- Why endpoint security?
 - Protecting the human
- AnyConnect
 - It's not just for VPN
- AMP for Endpoints
 - The nuts and bolts
- Endpoint security in context
 - What about the rest of your network?

AMP Everywhere – See More. Respond Faster.

Get visibility and control across all attack vectors to defend against today's most advanced threats.

AMP for Endpoints

Protect your endpoints! Get visibility into file and executable-level activity, and remediate advanced malware on devices running Windows, Mac OS, Linux, and Android.

AMP for Networks

Get deep visibility into threat activity and block advanced malware with AMP deployed as a network-based solution running on AMP-bundled NGIPS

Threat Grid

An on-premises appliance or cloud-based solution for static and dynamic malware analysis (sandboxing) and threat intelligence.

AMP for Firewalls

Supercharge your next-generation firewall by turning on AMP capabilities on the Cisco Firepower NGFW or the Cisco ASA with FirePOWER™ Services.

AMP for ISR

Combat and block network-based threats by deploying AMP capabilities on the Cisco® Integrated Services Router (ISR).

AMP Everywhere – See More. Respond Faster.

Get visibility and control across all attack vectors to defend against today's most advanced threats.

AMP for Meraki MX

Add AMP to Cisco Meraki® MX and take advantage of simplified threat protection with advanced capabilities, providing visibility into threats on your network across multiple sites.

AMP for Private Cloud Virtual Appliance

For high-privacy environments that restrict the use of the public cloud, use an on-premises, air-gapped private cloud deployment of AMP for Networks or AMP for Endpoints.

AMP for Email

Add AMP to a Cisco Email Security Appliance (ESA) and get visibility and control to defend against advanced threats launched via email.

AMP for Web

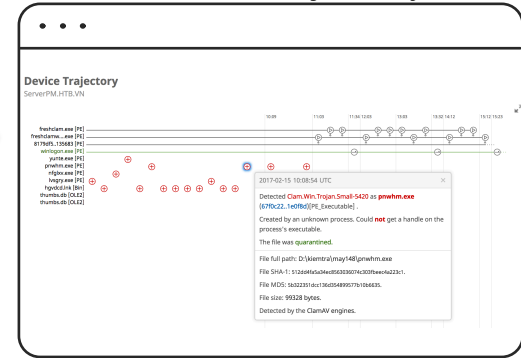
Add AMP to a Cisco Web Security Appliance (WSA) or Cisco Secure Internet Gateway (SIG) and get visibility and control to defend against advanced threats launched from the web.

AMP Unity

Common Objects

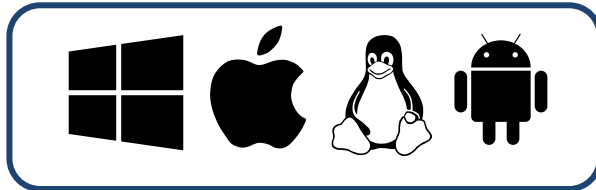


Global Trajectory



AMP Cloud

Endpoints



Network Appliances

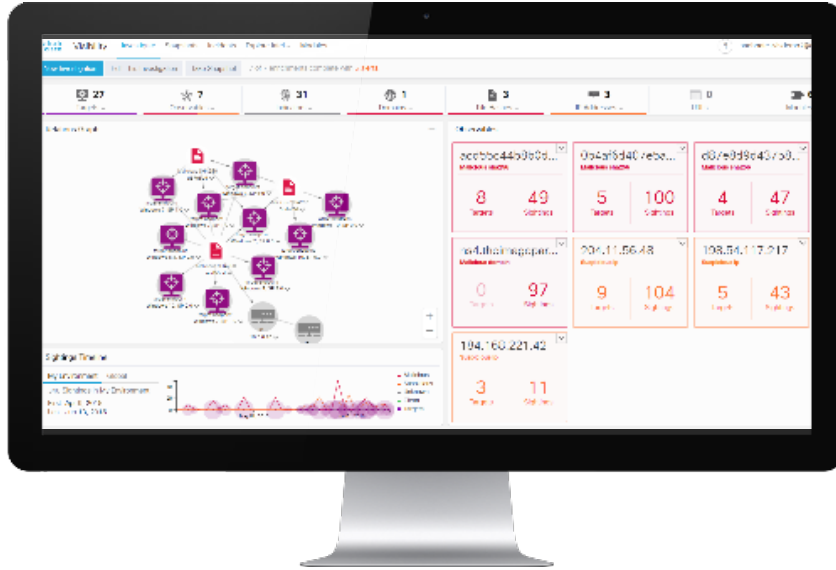


Content Security



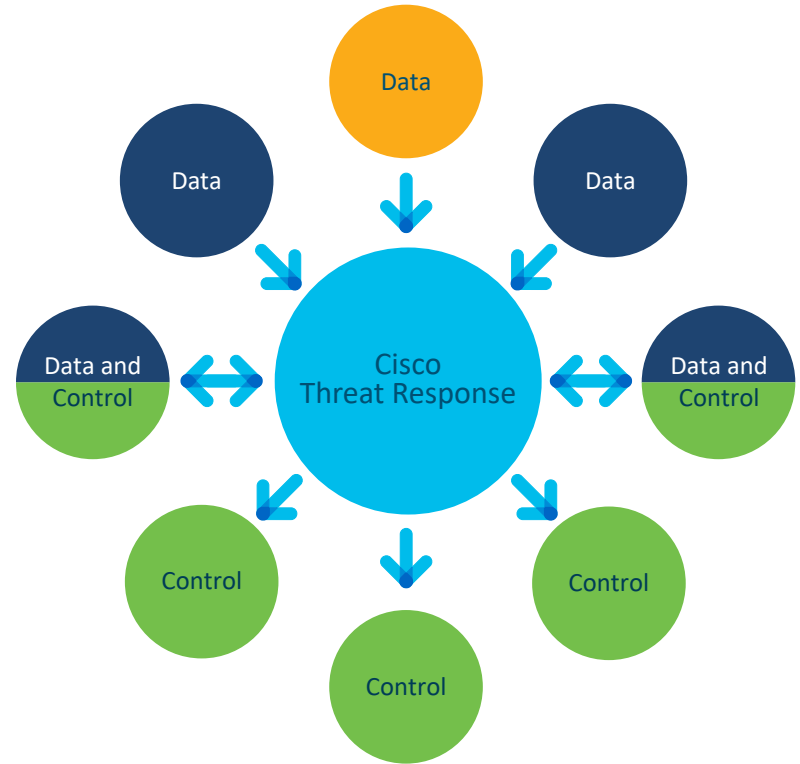
Cisco Threat Response

Integrating security for faster defense



- Automates & Orchestrates across security products
- Integrates with AMP, Umbrella, Threat Grid, Email and Web Security, Firepower, Stealthwatch, Orbital
- Accelerate response with AMP and Umbrella blocks
- Integrated casebook
- Extensible to third parties (e.g., Virustotal)
- Browser plugin for cross-platform support in Chrome and Firefox

Cisco Threat Response Modules



SecureX builds the “mortar” into Cisco Security to deliver desirable outcomes with less effort

Backend INTEGRATION

- Navigate displays effortlessly with secure single sign-on
- Cisco Talos, Advanced Malware Protection, and Cognitive Intelligence constantly deliver new understanding
- Event aggregation and correlation within seconds
- Information flows privately from your on-prem devices to our regional clouds
- Alert notifications with high-fidelity cross-platform analytics
- Automation with no/low-code drag-and-drop action orchestrator and 3rd-party adapters

It's embedded across the Cisco Security portfolio



Frontend
experience

Closing Thoughts



Agenda

- Why endpoint security?
 - Protecting the human
- AnyConnect
 - It's not just for VPN
- AMP for Endpoints
 - The nuts and bolts
- Endpoint security in context
 - What about the rest of your network?

Protect the Business



Our #1 Responsibility Is to Protect the Business

- A business is comprised of the people who make it happen
- Those people use devices to interact with our business
- Ergo: we must protect our people and the devices they use

Infrastructure

Network



Firepower
ASA



Stealthwatch

Corporate Assets

Desktops, Servers



AMP for
Endpoints



AnyConnect

Employees

People



Umbrella







Duo

Endpoint Security is critical to Threat-Centric & Trust-Centric approaches alike.

Additional Resources

- <http://cs.co/ats-youtube>
- <http://cs.co/ats-community>

  CCIE Professional Development Integrated Security Technologies and Solutions Volume I Cisco Security Solutions for Advanced Threat Protection with Next Generation Firewall, Intrusion Prevention, AMP and Content Security http://a.co/7O5fPZK Aaron Woland, CCIE #20113 Vivek Santuka, CCIE #17621 Mason Harris, CCIE #5916 Jamie Sanbower, CCIE #13637 <small>ciscopress.com</small>	  SECURITY Cisco Next-Generation Security Solutions All-in-one Cisco ASA FirePOWER Services, NGIPS, and AMP http://a.co/iir9D6E Omar Santos, CISSP No. 463598 Panos Kampanakis, CCIE No. 28561 Aaron Woland, CCIE No. 20113 <small>ciscopress.com</small>
--	--

Related Breakout Sessions

- DGTL-BRKSEC-2433: Threat Hunting and Incident Response with Cisco SecureX
- BRKSEC-2890: Advanced Malware Protection (AMP) and Threat Grid Integrations - covering Web, Email, Firepower & Endpoint Security
- DGTL-BRKSEC-3144: Malware Execution As A Service: A Deep Dive into Threat Grid Advanced File Analysis

Thank you

CISCO *Live!*

#CiscoLive





Possibilities

#CiscoLive