Virtual Update – AMP for Endpoints

Tue Frei Nørgaard & Mikael Grotrian
Consulting Systems Engineers

7/10 - 2015
Cisco AMP Goes Beyond Detection

Results

Best Protection Value
- 99% Breach Detection
- Lowest TCO per protected Mbps (and included AMP for Endpoints)
- Security SVM leadership and Fastest Time to Detection

Cisco AMP Capabilities Go Beyond Detection (what NSS tested)
- AMP provides Continuous Protection Across the Attack Continuum
  - Point-in-Time + Continuous Analysis
  - Retrospective Security
  - File and Device Trajectory
  - Indications of Compromise

Cisco Advanced Malware Protection

Best Protection Value
99.0% Breach Detection Rating
Lowest TCO per Protected-Mbps
Advanced Malware Protection Everywhere

Best-in-Class Detection

Leader in Security Effectiveness

Broader Deployment Options

- Coming Q1CY16 Meraki MX
- Dedicated FirePOWER Appliance
- Web & Email Security Appliances
- FirePOWER Services on ISR
- FirePOWER Services on ASA

Mac OS X  PC  AnyConnect  Mobile  Virtual  Cloud Based Web Security & Hosted Email  Private Cloud
There Are Several Ways You Can Deploy AMP

<table>
<thead>
<tr>
<th>Deployment Options</th>
<th>AMP on Email and Web; Cisco® ASA; CWS</th>
<th>AMP for Networks (AMP on FirePOWER Network Appliance)</th>
<th>AMP for Endpoints</th>
<th>AMP Private Cloud Virtual Appliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Method</td>
<td>License with ESA, WSA, CWS, or ASA customers</td>
<td>Snap into your network</td>
<td>Install lightweight connector on endpoints</td>
<td>On-premises Virtual Appliance</td>
</tr>
<tr>
<td>Ideal for</td>
<td>New or existing Cisco CWS, Email /Web Security, ASA customers</td>
<td>IPS/NGFW customers</td>
<td>Windows, Windows OS for POS, Mac, Android, virtual machines; can also deploy from AnyConnect client</td>
<td>High-Privacy Environments</td>
</tr>
</tbody>
</table>

**Details**
- ESA/WSA: Prime visibility into email/web
- CWS: web and advanced malware protection in a cloud-delivered service
- AMP capabilities on ASA with FirePOWER Services
- Wide visibility inside network
- Broad selection of features—before, during, and after an attack
- Comprehensive threat protection and response
- Granular visibility and control
- Widest selection of AMP features
- Private Cloud option for those with high-privacy requirements
- Can deploy full air-gapped mode or cloud proxy mode
- For endpoints and networks
FireAMP Connector

Works With Your Existing End Point Security

Unprecedented Visibility and Control into Malware
   Ability to see and stop Advanced Malware that either the customer or
   Cisco determine to be Malicious

Protects you Inside and Outside your Network
   Complimentary to Network Based Advanced Malware Protection

Remediation in Seconds vs Days
   Fast Incident Response
Resources for AMP for Endpoints

Footprint
Win 500KB/30MB install, 512MB RAM, 150MB/1GB Disk
Mac 5MB install, 2GB RAM, 65MB Disk
Linux 16MB install, 1GB RAM, 400 MB Disk

Traffic
Cloud Query = ~ 500 Bytes
Typical Client is 40-50 Queries per Day
5000 Client Environment = 125 MB/Day
OS Requirements

- Windows
  - XP with Service Pack 3 or later
  - Vista with Service Pack 2 or later
  - Windows 7
  - Windows 8 and 8.1
  - Windows Server 2003
  - Windows Server 2008
  - Windows Server 2012

- Mac
  - OSX 10.7
  - OSX 10.8
  - OSX 10.9
  - OSX 10.10

- Android 2.1+

- Linux - new
  - Red Hat Enterprise Linux 6.5 & 6.6
  - CentOS 6.4, 6.5, & 6.6
FireAMP Installer Command Line

- For 3rd Party End Point Management
  - /S - Used to put the installer into silent mode.
    - NOTE: This must be specified as the first parameter.
  - /desktopicon0 - Used to specify no desktop icon
  - /desktopicon1 - Used to specify there is a desktop icon
  - /D= - Used to specify which directory to perform the install. For example /D=C:\tmp will install into C:\tmp. NOTE: This must be specified as the last parameter.
AMP Provides Continuous Retrospective Security

Breadth of Control Points
- Email
- Endpoints
- Web
- Network
- IPS
- Devices

Telemetry Stream

File Fingerprint and Metadata
File and Network I/O
Process Information

Continuous Feed

Continuous Analysis
POINT-IN-TIME DETECTION
Analysis Stops

Not 100%

Antivirus Sandboxing

Initial Disposition = Clean
Actual Disposition = Bad = Too Late

Blind to scope of compromise

Sleep Techniques
Unknown Protocols
Encryption
Polymorphism

RETRIESTIVE SECURITY
Analysis Continues

Cisco AMP

Initial Disposition = Clean
Actual Disposition = Bad = Blocked

Turns back time
Visibility and control are key
AMP Threat Grid
Feeds Dynamic Malware Analysis and Threat Intelligence to the Cisco AMP Solution

AMP Threat Grid platform correlates the sample result with millions of other samples and billions of artifacts

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

Analyst or system (API) submits suspicious sample to Threat Grid

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

Actionable threat content and intelligence is generated that can be utilized by AMP, or packaged and integrated into a variety of existing systems or used independently.

Actionable Intelligence

Threat Score / Behavioral Indicators
Big Data Correlation Threat Feeds

Sample and Artifact Intelligence Database

Low Prevalence Files

© 2014 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
File Trajectory

Lets you determine scope by tracking malware in motion and activity

Visibility across organization, centering on a given file

Looks **ACROSS** the organization and answers:

- What systems were infected?
- Who was infected first (“patient 0”) and when did it happen?
- What was the entry point?
- When did it happen?
- What else did it bring in?
Device Trajectory

Gives you deep visibility into file activity on a single device/endpoint

Looks DEEP into a device and helps answer:
• How did the threat get onto the system?
• How bad is my infection on a given device?
• What communications were made?
• What don’t I know?
• What is the chain of events?
Automated import into FireSight brings unrivaled correlation
Policy

• Controls the behaviour of Endpoint AMP
• The defaults are appropriate for the majority of deployments
• Here we will discuss the more interesting options
Associated Lists

- Each policy has a number of associated lists that can be applied
- Lists defined in Outbreak Control Menu…
- …and will be covered in that section
Consider privacy when selecting Send User and Send Filename

Heartbeat refers to:
- any files to restore via Cloud Recall™
- any files to restore by the administrator
- any policies to pick up
- tasks to perform such as product updates or scans

Don’t change log level unless advised to do so by support
Maintain a consistent log of events in virtual environments or when machines are re-imaged.

Binds the connector to the MAC address, so that events are maintained by new connector installs.

Not commonly used.
Product Updates

- Allows the admin to control exactly how updates occur on a per policy basis
- Update server is populated once a product version is selected
- When the connector calls home during the update windows, it will pick up the policy
- New connectors will not function correctly without the reboot occurring
Selecting “Audit” in file conviction mode will allow malware to run.

It also effects how Application Blocking functions

On Execute Mode

- Passive – don’t wait for a result from the cloud before allowing the file to run
- Active – wait for a result from the cloud. Can cause performance issues
Cache Settings

- Results from the cloud are cached locally.
- This dialog controls how long entries in the cache stay live before SHAs are resubmitted to the cloud.

Cloud Policy

- Allows the admin to control how sensitive the ETHOS and SPERO engine are.
- Hashes seen more times than listed in the threshold by the entire community will not be convicted.
- Step-up will enable more sensitive SPERO trees if a machine is deemed to be “massively infected”.
  - This is determined by the Step-Up Threshold, which is the number of detections in a 30 second period.
Device Flow Correlation (DFC)

- Allows the connector to monitor network connections
- Don’t enable it on servers
  - But have an incident response policy ready that does
- Terminate and quarantine refers to the parent process of any connection that triggers DFC, as long as it has an unknown disposition
- Data Source
  - Custom: Just those addresses added to the IP Blacklist associated with the policy
  - Sourcefire: The Talos Security Intelligence feed
Protection Across Networks

The Network platform uses indications of compromise, file analysis, and in this example file trajectory to show you exactly how malicious files have moved across the environment.
Protection Across Endpoints

The Endpoint platform has device trajectory, elastic search, and outbreak control, which in this example is shown quarantining recently detected malware on a device that has the AMP for Endpoints connector installed.
Protection Across Web and Email

Cisco® AMP for Web and Email protects against malware threats in web and email traffic by blocking known malware and issuing retrospective alerts when unknown files are convicted.
Cisco AMP Everywhere Strategy Means Protection Across the Extended Network
Choose the right option

<table>
<thead>
<tr>
<th>I want to be able to define policies for malware…</th>
<th>File Reputation</th>
<th>✔</th>
<th>✔</th>
<th>✔</th>
</tr>
</thead>
<tbody>
<tr>
<td>I want to be able to isolate suspected malware for threat analysis…</td>
<td>Sandboxing</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>I want to be able to backtrack if malware makes it into my system…</td>
<td>Retrospective Security</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>I need to identify compromised devices on my network…</td>
<td>Indications of Compromise</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>I want to track how a file has been behaving…</td>
<td>File Analysis</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>I want to track how threats traverse the network…</td>
<td>File Trajectory</td>
<td></td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>I want to see system activities, relationships and events…</td>
<td>Device Trajectory</td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>I want to search large sets of data for compromises…</td>
<td>Elastic Search</td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>I want to be able to stop the spread of malware with custom tools…</td>
<td>Outbreak Control</td>
<td></td>
<td></td>
<td>✔</td>
</tr>
</tbody>
</table>
Links og kontakt

- Angler on Cisco security blog
- Angler on Talos
- AMP
- Cisco AMP for Endpoints Demonstration (10:07)
- Cisco AMP for Networks Demonstration (9:59)
- Least Prevalence VoD
- AMP Endpoint Datasheet
- Tue Frei Noergaard tuenoerg@cisco.com
- Mikael Grotrian mikael.grotrian@cisco.com
## Cisco AMP Video Assets

<table>
<thead>
<tr>
<th>Demos</th>
<th>Customer Testimonials</th>
<th>AMP Explainer Videos</th>
<th>AMP and Incident Management</th>
<th>AMP: A User’s Perspective</th>
</tr>
</thead>
</table>
| - 5-minute AMP Demo  
- AMP for Endpoints Demo  
- AMP for Networks Demo  
- AMP Threat Grid for Incident Response  
- AMP Threat Grid: Portal overview | - First Financial Bank  
- Sam Houston State University  
- Center for Internet Security  
- FishNet VoDs | - Meet Tom, the IT Security Guy  
- External Launch Cast  
- AMP + Threat Grid External Launch Video  
- AMP for Endpoints Overview  
- AMP for Networks Overview  
- AMP Threat Grid Overview | - Series 1 (3 videos)  
- Series 2 (3 videos) | - Stories 1-6  
- Stories 1 and 2 (short versions) |

Visit [AMP Product Pages](#) for videos, demos, and other resources