

Think Outside the Sandbox

Cisco AMP (Advanced Malware Protection)



Dubai, UAE
February 18-19, 2015

*TOMORROW
starts here.*

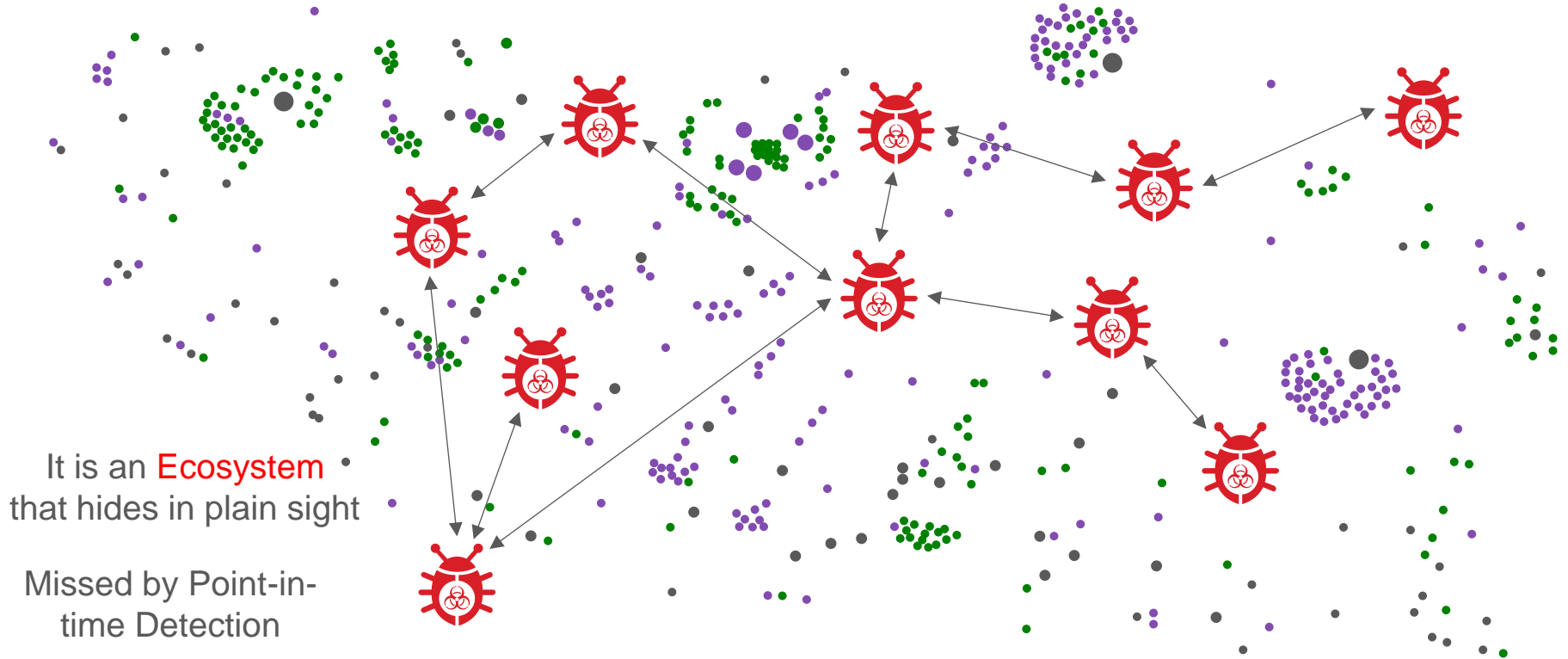
Think Outside the Sandbox

Cisco AMP (Advanced Malware Protection)

Mahmoud Rabi

Consulting Systems Engineer - Security

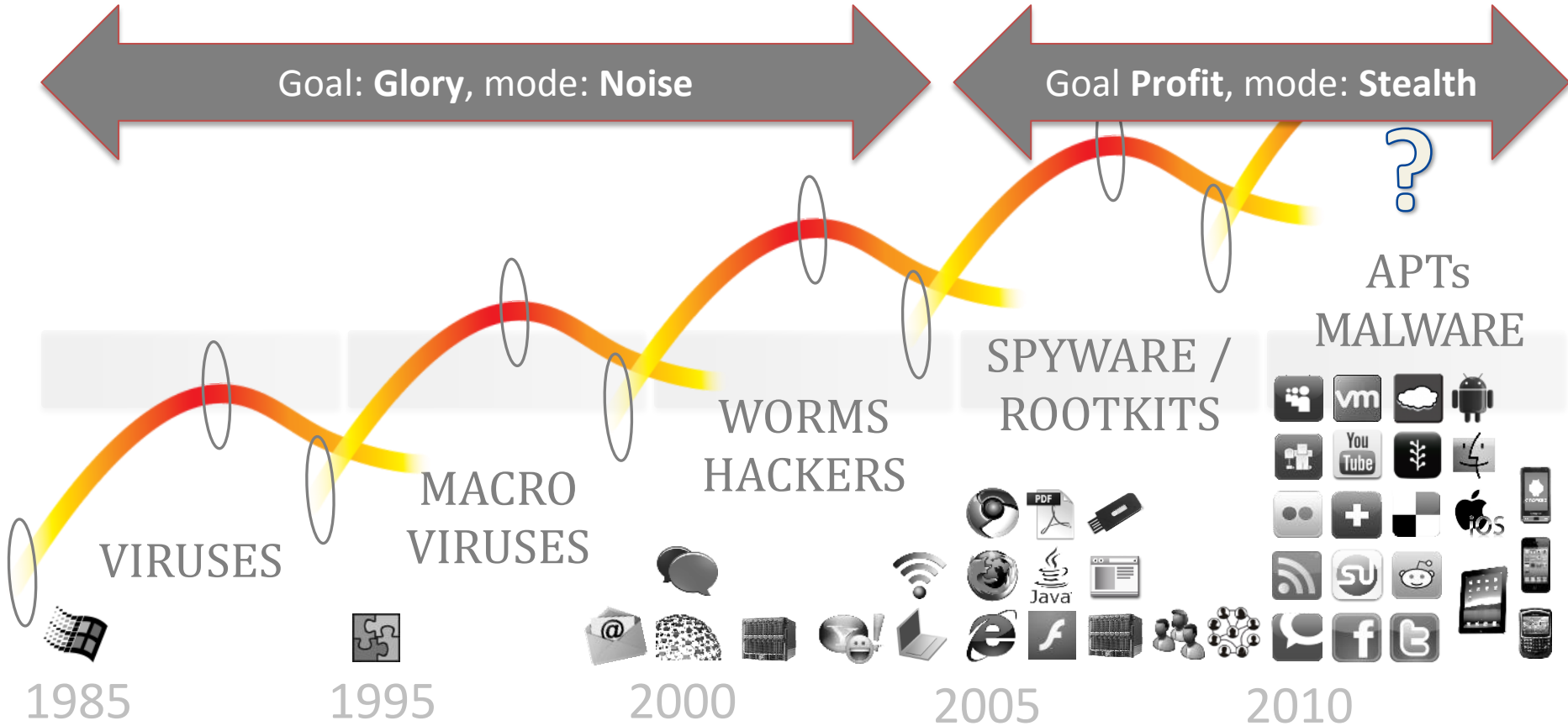
Today's advanced malware is not just a single entity



The Industrialisation of Hacking

Goal: **Glory**, mode: **Noise**

Goal **Profit**, mode: **Stealth**



1985

1995

2000

2005

2010

How Hacking is done today



Survey

What does environment look like?
What are the countermeasures?
Identify weak/vulnerable assets..

Write

Craft context-aware malware to penetrate *this* environment

Test

Validate malware works, can evade countermeasures and stay undetected

Execute

Use malware. Move laterally, establish secondary access,

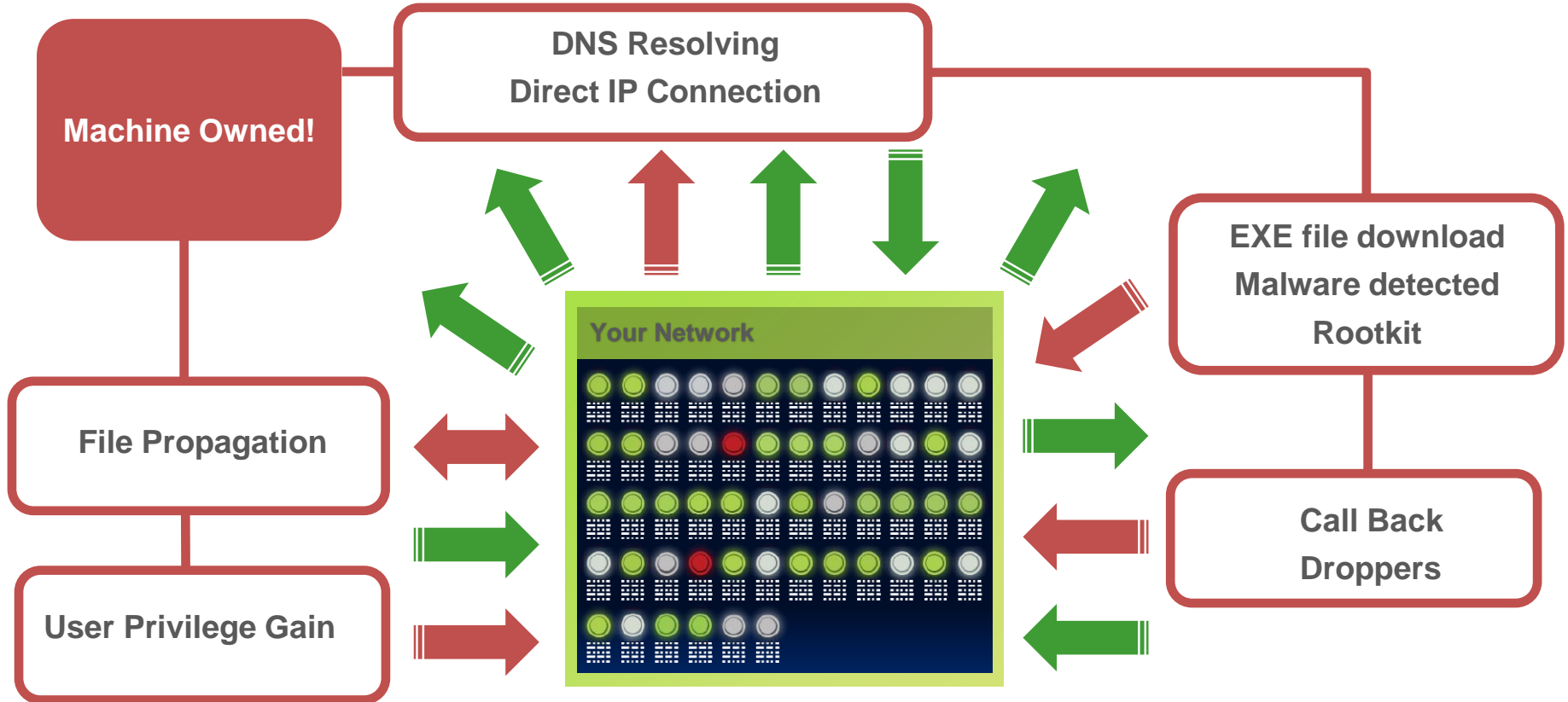
Accomplish

The mission: Extract data, destroy, plant evidence, compromise.

Each stage may generate a Weak Signal indicating malicious activity.

We must find these signals in the noise.

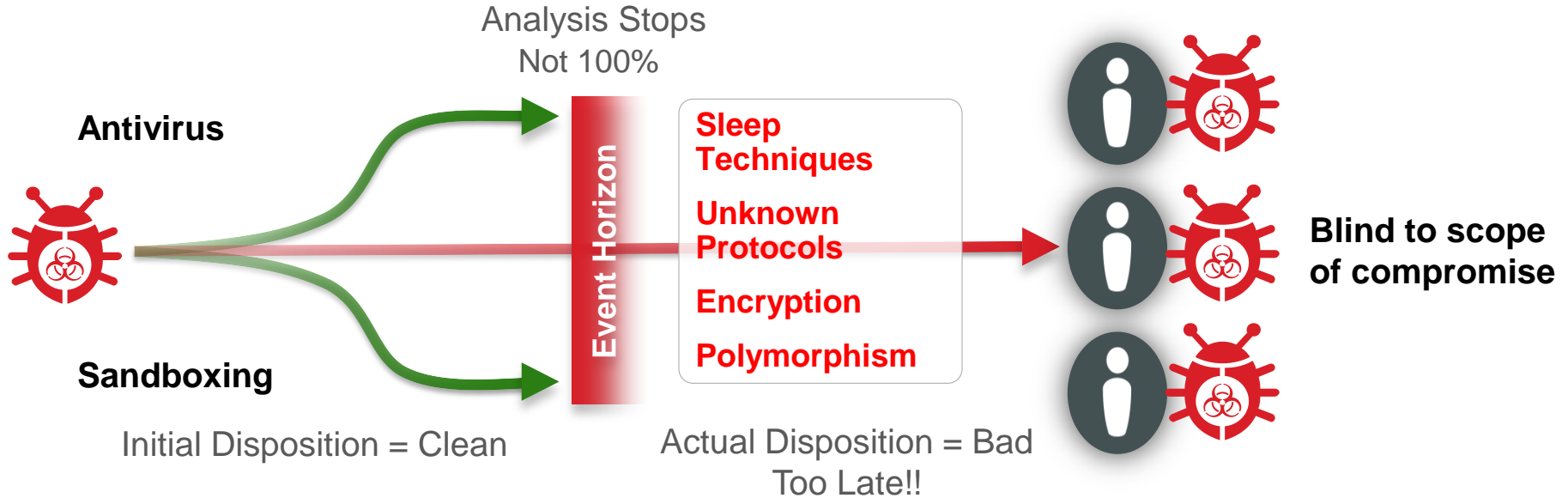
Can you correlate multiple events to indicate a compromise?



It's Time to Think Outside the Sandbox!



Point-in-time Detection Evasion Technique

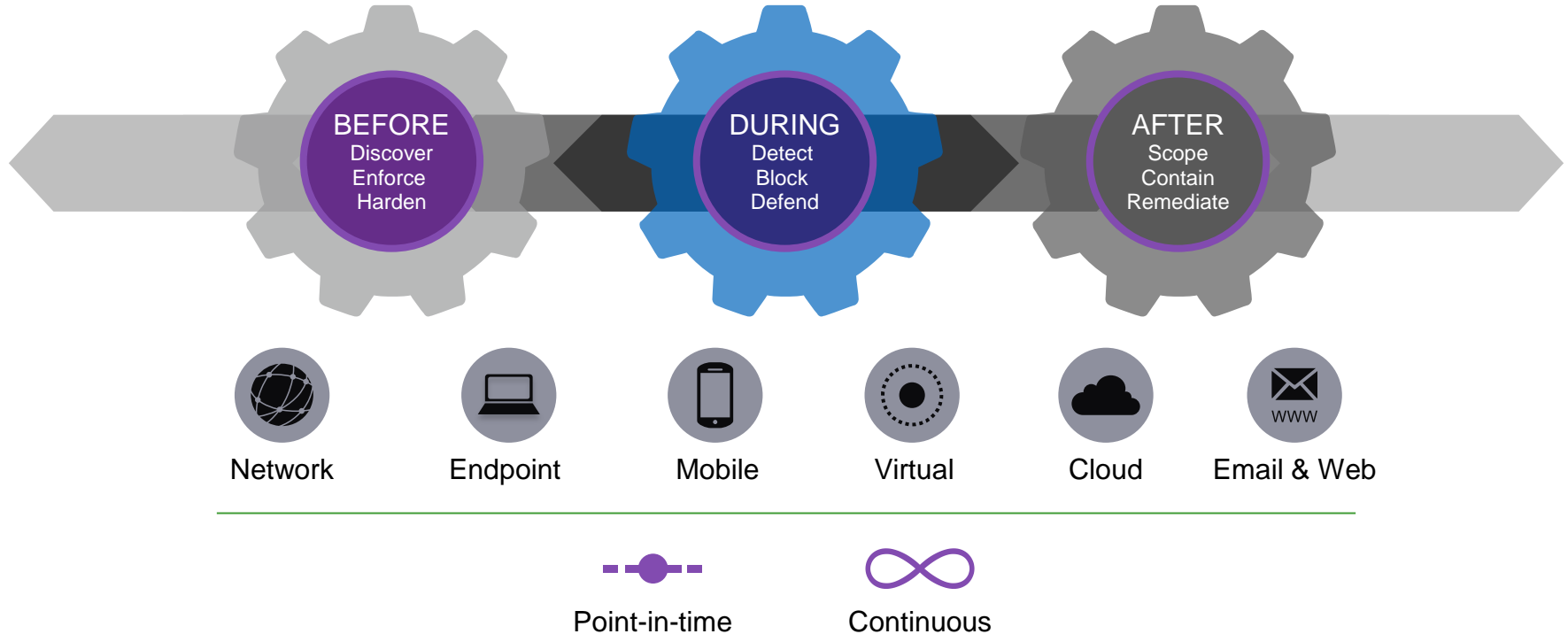


“Would you do **Security** differently “**if**” you knew you would be compromised?”

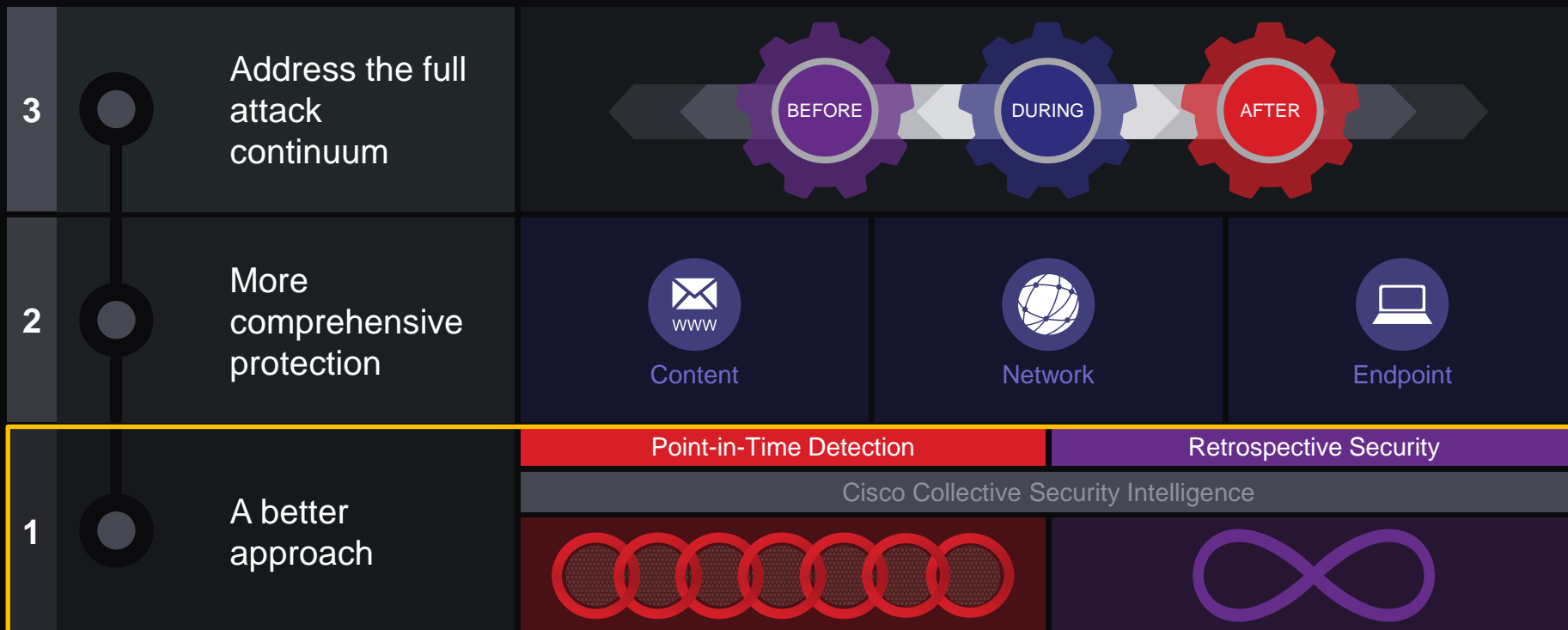
It is no longer a question of “*if*” you will be breached...

It is a matter of “*when*”.

Think Differently about Security



Cisco AMP Delivers Three Advantages



Cisco Has The Best-In-Class Security Asset To Deliver Against These Requirements

Cisco
SIO

Cisco Collective
Security Intelligence

Sourcefire
VRT®
(Vulnerability
Research Team)



Automatic Updates
every 3-5 minutes

1.6 million

global sensors

35%

worldwide email traffic

100 TB

of data received per day

13 billion

web requests

150 million+

deployed endpoints

24x7x365

operations

600+

engineers, technicians,
and researchers

40+ Languages

AMP ∞

Advanced Malware Protection



300,000+ File Samples per Day

FireAMP™ Community, 3+ million

Advanced Microsoft
and Industry Disclosures

Snort and ClamAV Open Source Communities

Honeypots

Sourcefire AEGIS™ Program

Private and Public Threat Feeds

Dynamic Analysis

Cisco AMP Delivers A Better Approach

Point-in-Time Detection



File Reputation & Behavioral Detection

Retrospective Security



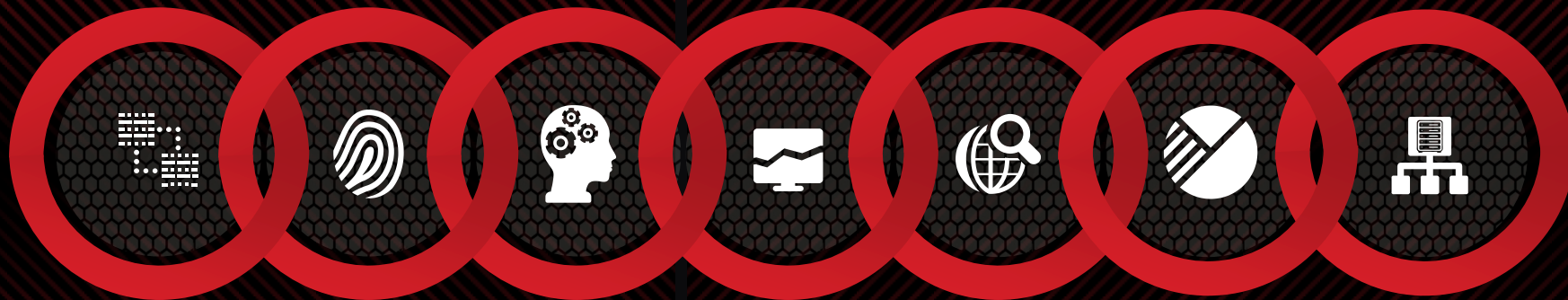
Continuous Protection

Unique To Cisco AMP

Cisco AMP Defends With Reputation Filtering And Behavioral Detection

Reputation Filtering

Behavioral Detection



One-to-One
Signature

Fuzzy
Finger-printing

Machine
Learning

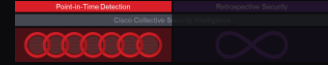
Indications
of Compromise

Dynamic
Analysis

Advanced
Analytics

Device Flow
Correlation

Reputation Filtering Is Built On Three Features



Reputation

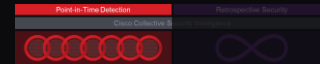


One-to-One
Signature

- 1 Unknown file's signature is analyzed and sent to the cloud
- 2 File's signature is not known to be malicious and is admitted
- 3 Unknown file's signature is analyzed and sent to the cloud
- 4 File's signature is known to be malicious and is prevented from entering the system



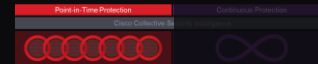
Reputation Filtering Is Built On Three Features



- 1** Fingerprint of file is analyzed and determined to be malicious
- 2** Malicious file is not allowed entry
- 3** Polymorphic form of the same file tries to enter the system
- 4** The fingerprints of the two files are compared and found to be similar to one another
- 5** Polymorphic fingerprint is denied entry based on its similarity to known malware



Reputation Filtering Is Built On Three Features

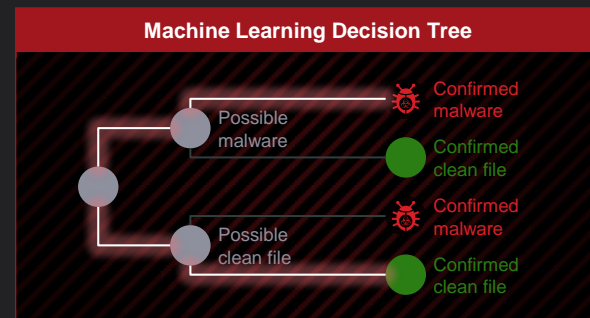


to-One
nature

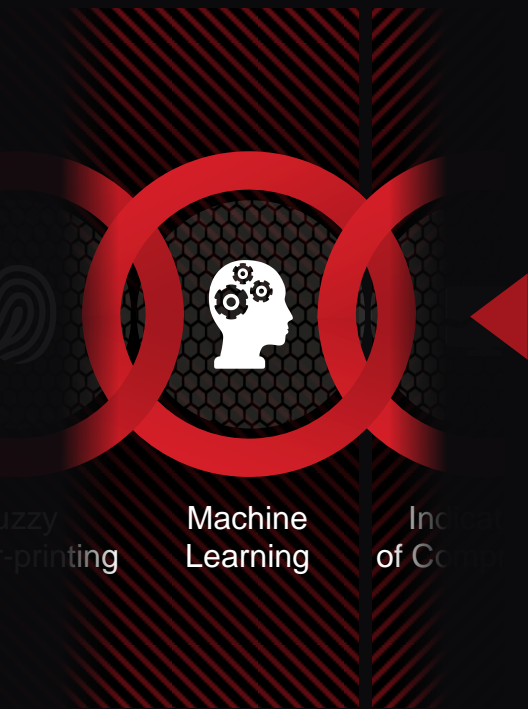
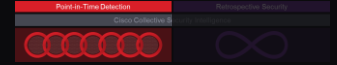
Fuzzy
Finger-printing

M
L

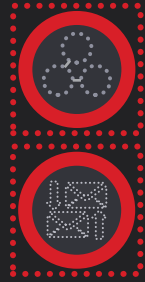
- 1 Unknown file's metadata is sent to the cloud to be analyzed
- 2 Metadata is recognized as possible malware
- 3 File is compared to known malware and is confirmed as malware
- 4 A second unknown file's metadata is sent to cloud to be analyzed
- 5 Metadata is similar to known clean file, possibly clean
- 6 File is confirmed as a clean file after being compared to a similarly clean file



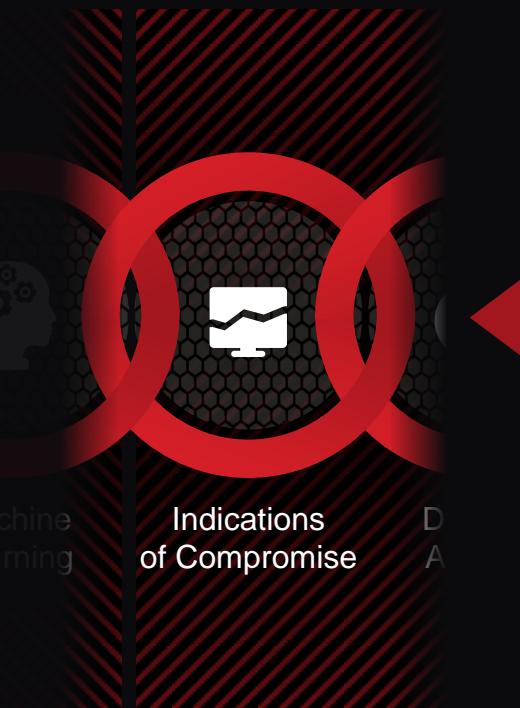
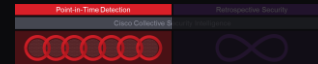
Behavioral Detection Is Built On Four Features



- 1** Unknown file is analyzed, indications of self-replication are found
- 2** These indications of self-replication are communicated to the cloud
- 3** Unknown file is also performing independent external transmissions
- 4** The transmission behavior is also sent to the cloud
- 5** These actions are reported to user to identify the file as possible malware



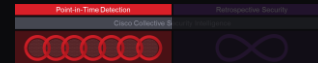
Behavioral Detection Is Built On Four Features



- 1 Unknown files are uploaded to the cloud where the Dynamic Analysis Engine executes them in sandboxes
- 2 Two files are determined to be malware, one is confirmed as a clean file
- 3 Malicious signatures are updated to the Intelligence cloud and broadcasted to user base



Behavioral Detection Is Built On Four Features



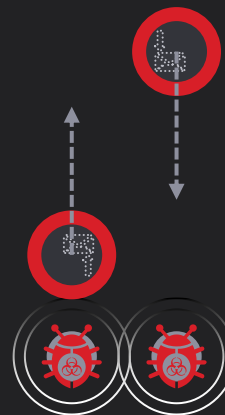
Dynamic
Analysis

Dev
Co

- 1** Device Flow Correlation monitors the source and destination of I/O traffic on a network
- 2** Two unknown files are seen communicating with a particular IP address
One is communicating
- 3** information outside the network, the other is receiving commands from the IP
- 4** Collective Security Intelligence Cloud recognizes the external IP as a confirmed, malicious site
- 5** Unknown files are identified as malware because of the association

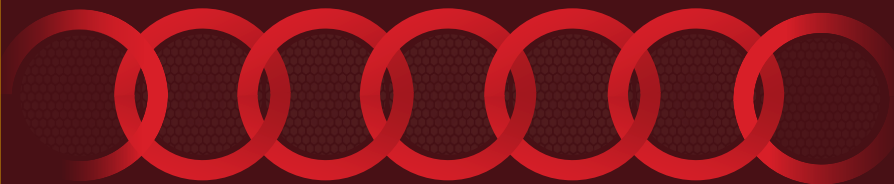


IP: 64.233.160.0



Cisco AMP Delivers A Better Approach

Point-in-Time Detection



File Reputation & Behavioral Detection

Retrospective Security



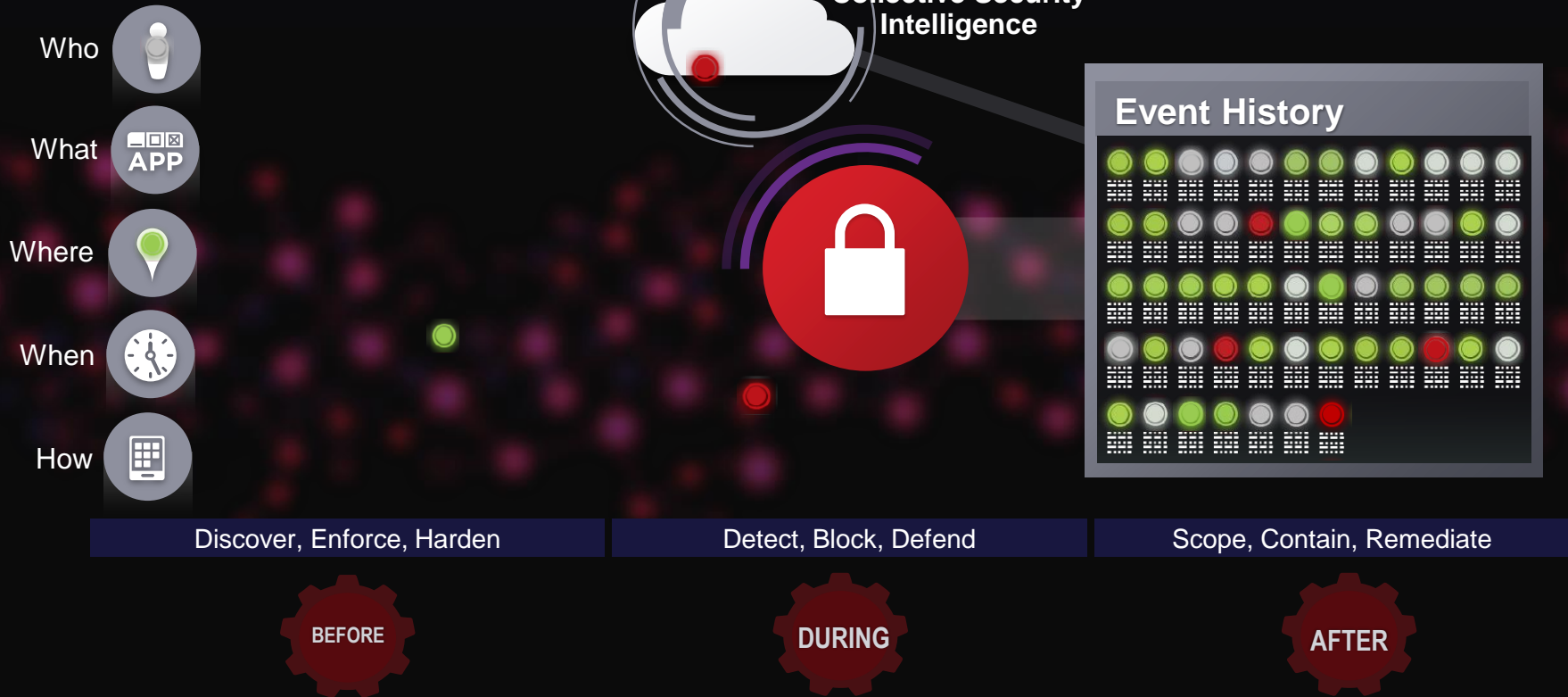
Continuous Protection

Unique to Cisco AMP

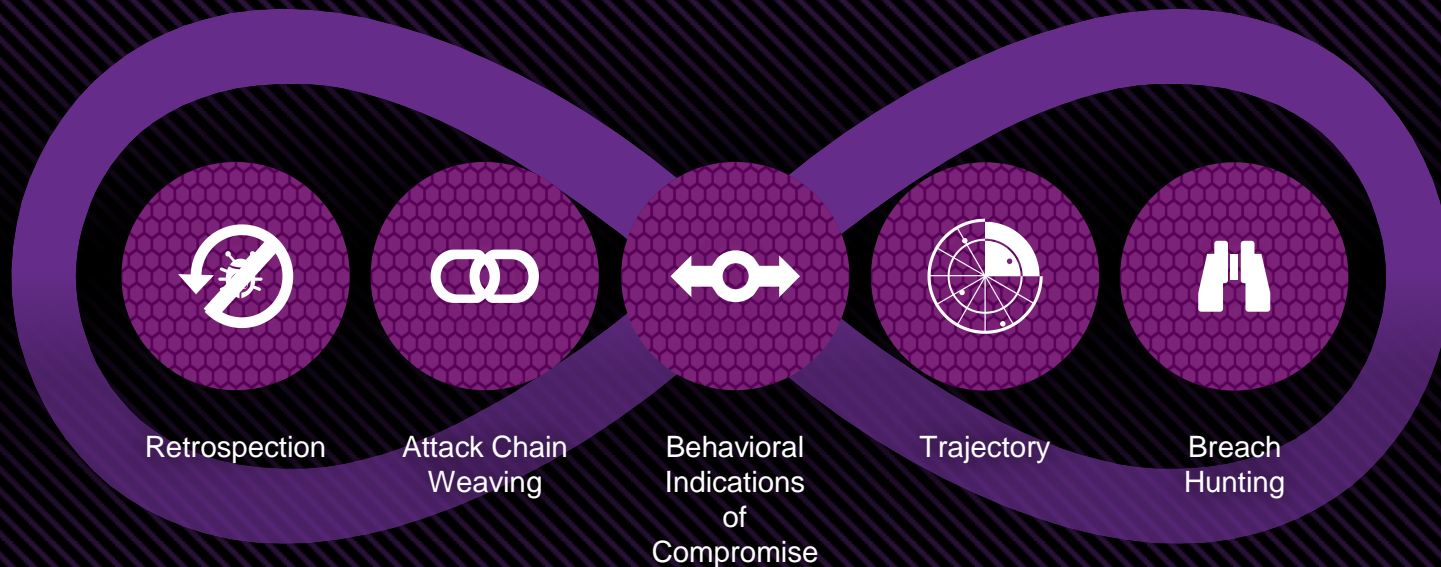
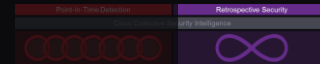
Putting It All Together



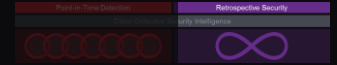
Putting It All Together



Cisco AMP Defends With Retrospective Security



Retrospective Security Is Built On...



1

Performs analysis the first time a file is seen

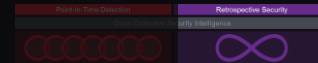
2

Persistently analyzes the file over time to see if the disposition is changed

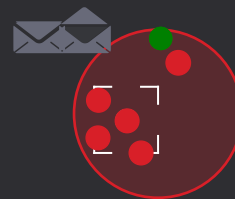
3

Giving unmatched visibility into the path, actions or communications that are associated with a particular piece of software

Retrospective Security Is Built On...



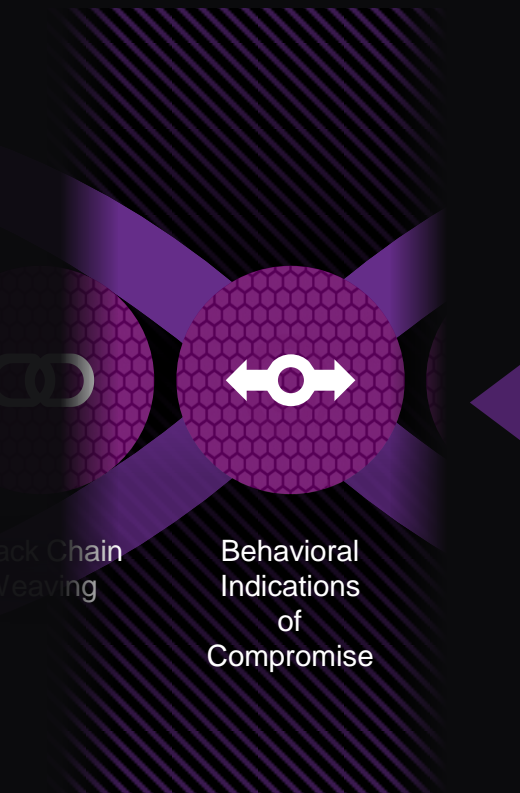
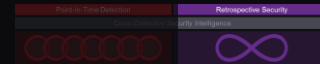
Behavioral Indications of Compromise uses Retrospection to monitor systems for suspicious and unexplained activity



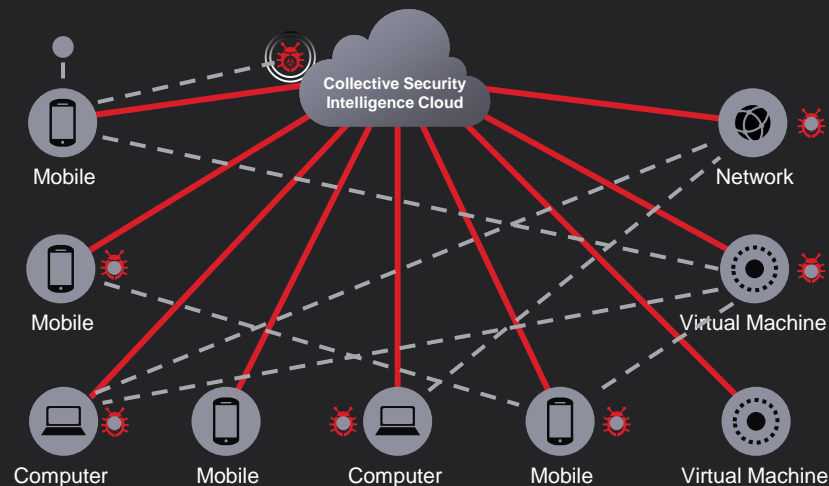
- 1** An unknown file is admitted into the network
- 2** The unknown file copies itself to multiple machines
- 3** Duplicates content from the hard drive
- 4** Sends duplicate content to an unknown IP address

Leveraging the power of Attack Chain Weaving, AMP is able to recognize patterns and activities of a given file, and identify an action to look for across your environment rather than a file fingerprint or signature

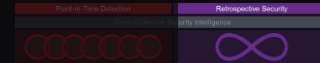
Retrospective Security Is Built On...



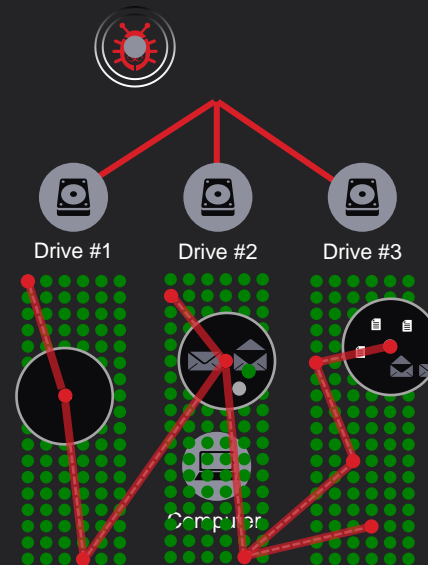
- 1** Unknown file is downloaded to device
- 2** Fingerprint is recorded and sent to cloud for analysis
- 3** The unknown file travels across the network to different devices
File trajectory automatically records time, method, point of entry, systems impacted and prevalence of the file
Sandbox analytics determines the file is malicious and notifies all devices
- 4** File trajectory provides greater visibility into the extent of an infection



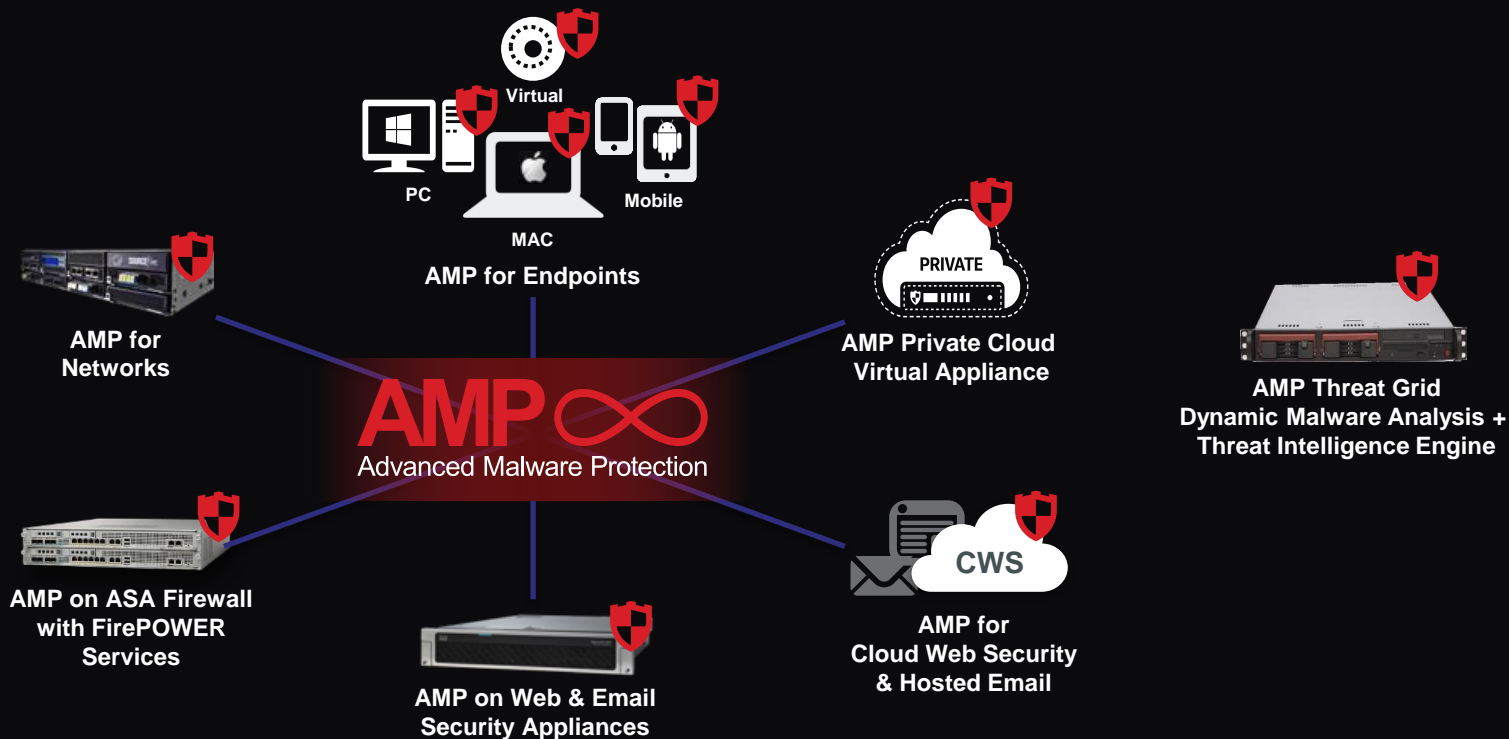
Retrospective Security Is Built On...







- 1** Unknown file is downloaded to a particular device
- 2** The file moves around the device, executing different operations
Meanwhile, device trajectory records the root cause, lineage and actions of the files on a machine
- 3** That data pinpoint the exact cause and extent of the compromise on the device
- 4**



Cisco's AMP Everywhere Strategy Means Protection Across the Extended Network



There are several ways you can deploy AMP

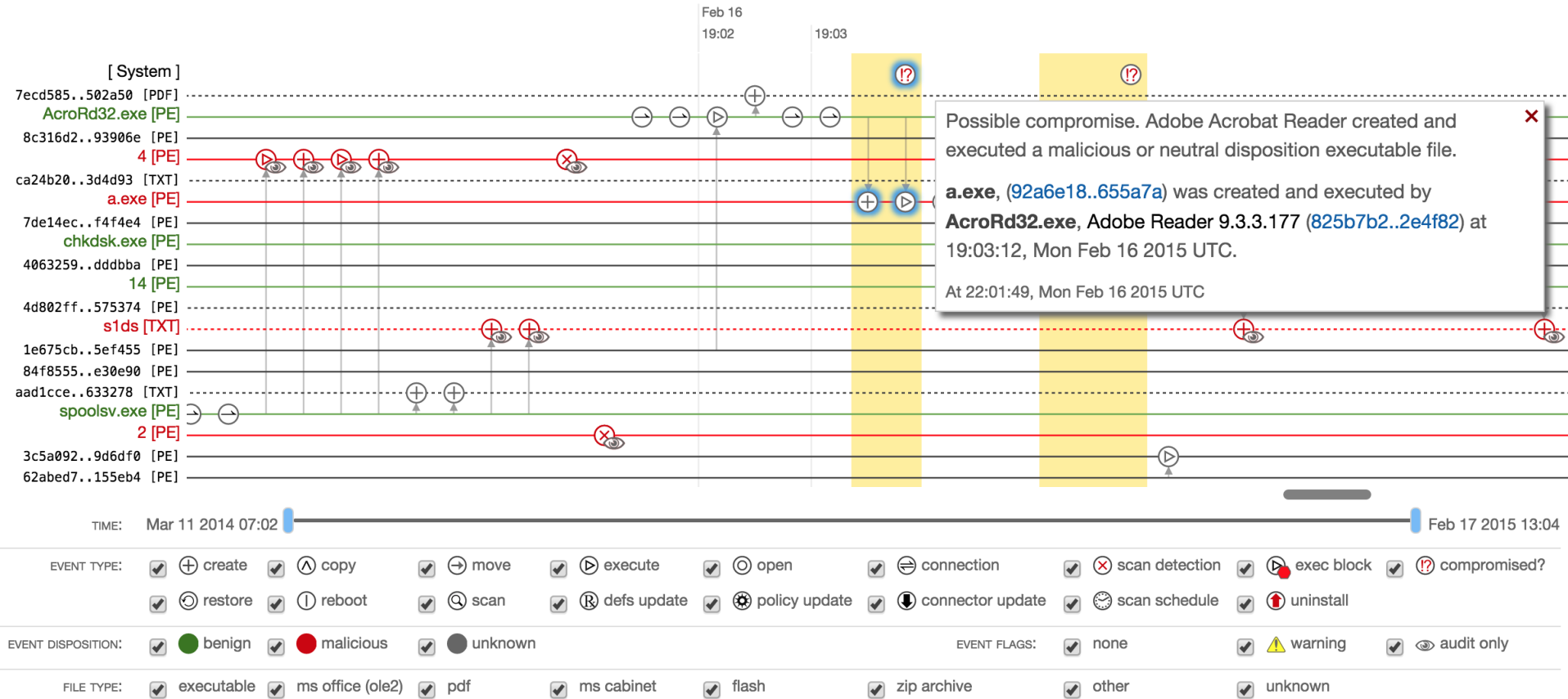
<p>Deployment Options</p>	 <p>Email and Web; AMP on ASA CWS</p>	 <p>AMP for Networks (AMP on FirePOWER Network Appliance)</p>	 <p>PC / MAC Mobile Virtual</p> <p>AMP for Endpoints</p>	 <p>AMP Private Cloud Virtual Appliance</p>
<p>Method</p>	<p>License with ESA, WSA, CWS, or ASA customers</p>	<p>Snap into your network</p>	<p>Install lightweight connector on endpoints</p>	<p>On-premise Virtual Appliance</p>
<p>Ideal for</p>	<p>New or existing Cisco CWS, Email /Web Security, ASA customers</p>	<p>IPS/NGFW customers</p>	<p>Windows, Mac, Android, VMs</p>	<p>High Privacy Environments</p>
<p>Details</p>	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • Wide visibility inside network • Broad selection of features- before, during and after an attack 	<ul style="list-style-type: none"> • Comprehensive threat protection and response • Granular visibility and control • Widest selection of AMP features 	<ul style="list-style-type: none"> • Private Cloud option for those with high privacy requirements • For endpoints and networks



Cisco Advanced Malware Protection

<https://www.youtube.com/watch?v=7IbI7DXWSs4>

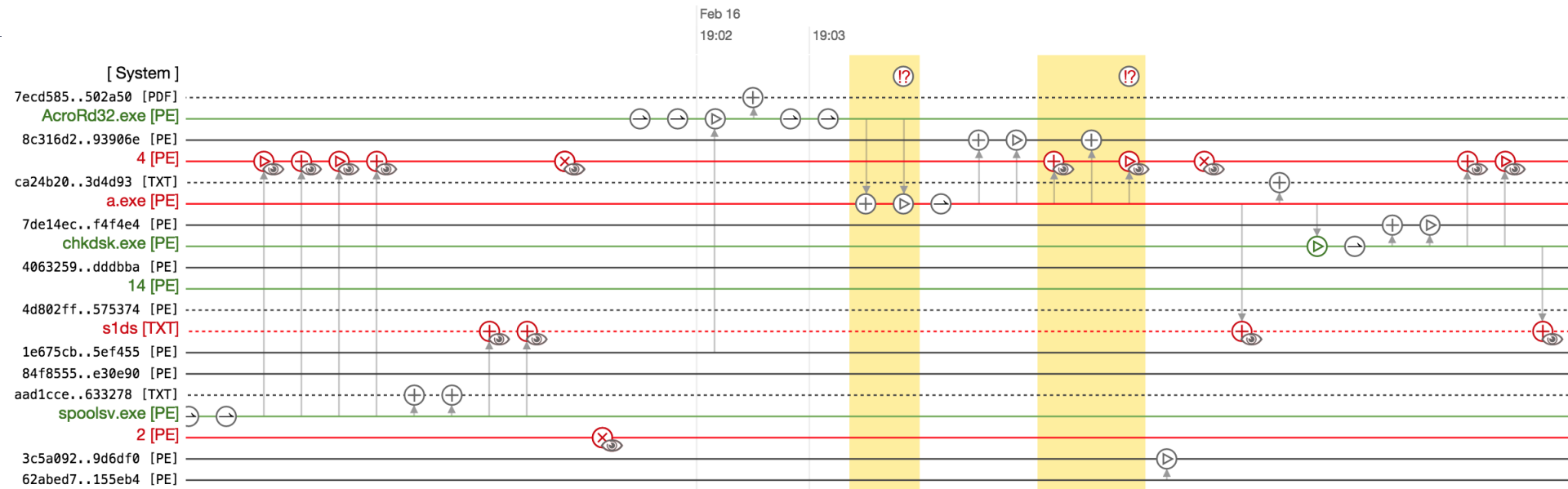
AMP for Endpoint Analysis – Adobe Acrobat Reader Compromise



Search...

Select All Clear All

AMP for Endpoint Analysis – Adobe Acrobat Reader Compromise



TIME: Mar 11 2014 07:02

Feb 17 2015 13:04

- EVENT TYPE: create copy move execute open connection scan detection exec block compromised?
 restore reboot scan defs update policy update connector update scan schedule uninstall
- EVENT DISPOSITION: benign malicious unknown
- EVENT FLAGS: none warning audit only
- FILE TYPE: executable ms office (ole2) pdf ms cabinet flash zip archive other unknown

Search...

Select All Clear All

ThreatGRID AMP – Behavioral Indicators

Threat Score: 90

Behavioral Indicators

⊕ Process Modified an Executable File

Severity: 95 Confidence: 95

⊕ A Document File Established Network Communications

Severity: 90 Confidence: 90

⊖ Downloaded PE Executable

Severity: 80 Confidence: 95

A PE executable was downloaded over the network. While this does not necessarily imply that it is malicious, it is suspicious. Malware will often download additional executables for added capabilities and so this file should be reviewed for additional activity that might be suspicious.

Categories file, network, artifact

Tags dropper, executable

Report Error

IP	Port	Protocol	Network Stream	Artifact ID
74.122.246.154	80	HTTP	Stream 4	36

⊕ Outbound HTTP GET Request

Severity: 75 Confidence: 75

⊕ Process Modified File in a User Directory

Severity: 70 Confidence: 80

⊕ Process Disabled Internet Explorer Proxy

Severity: 70 Confidence: 70

⊕ Potential Sandbox Detection - Enumeration of ProductID

Severity: 60 Confidence: 70

⊕ Process Created an Executable in a User Directory

Severity: 60 Confidence: 95

⊕ Command Exe File Execution Detected

Severity: 50 Confidence: 80

⊕ Potential Code Injection Detected

Severity: 50 Confidence: 50

⊕ Executable with Encrypted Sections

Severity: 30 Confidence: 30

⊕ Outbound Communications to Nginx Web Server

Severity: 25 Confidence: 25

⊕ Executable Imported the IsDebuggerPresent Symbol

Severity: 20 Confidence: 20

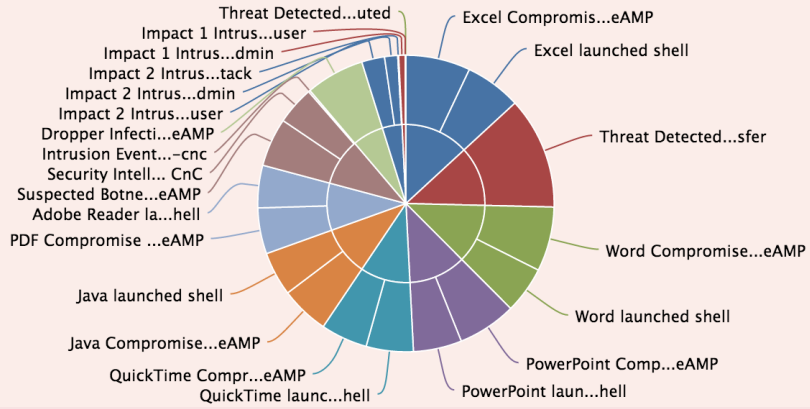
Process Tree for Sample e2112cc9655d4d4f9798d3223b88bd56



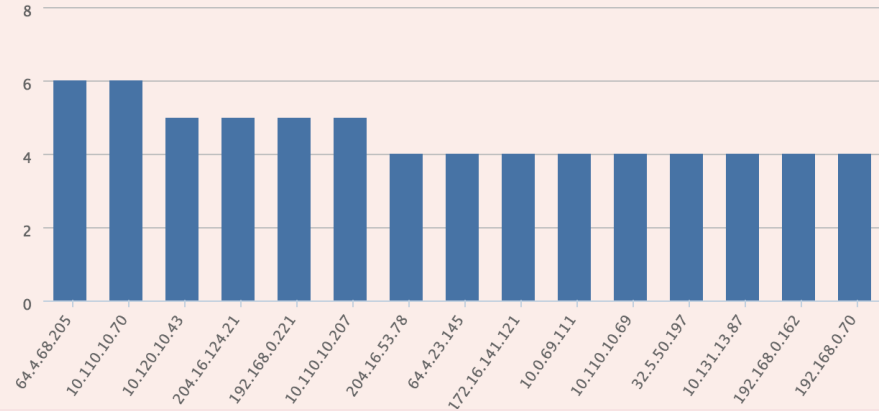
Network AMP Indications of Compromise and Correlation

Indications of Compromise

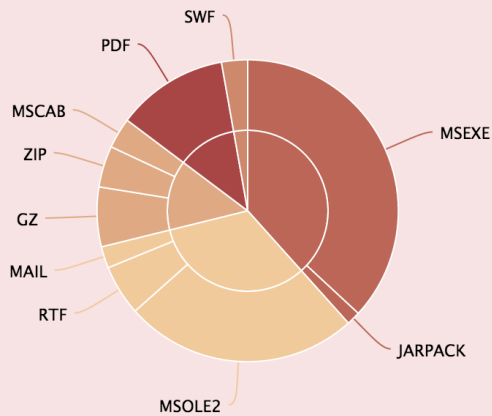
Hosts by Indication



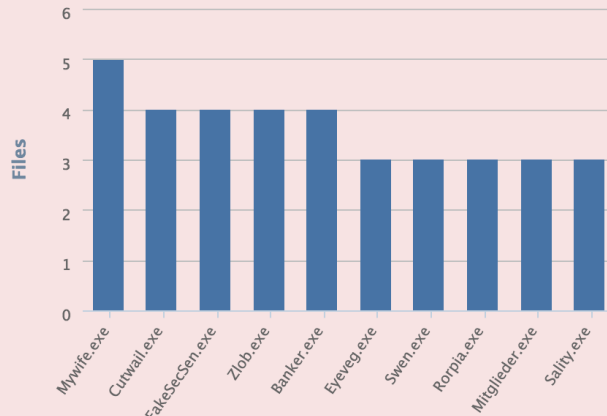
Indications by Host



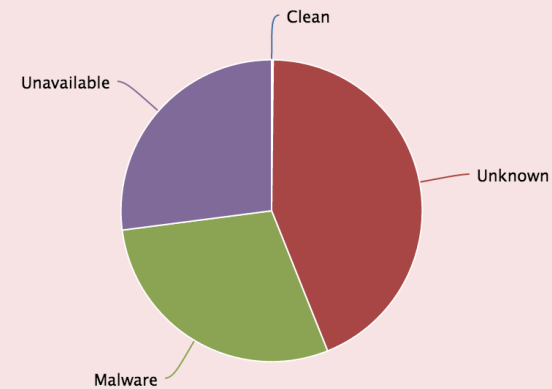
Top File Types



Top File Names



Files by Disposition



NSS Labs Breach Detection Systems SVM

Cisco AMP is a Leader in Security Effectiveness and TCO and offers Best Protection Value



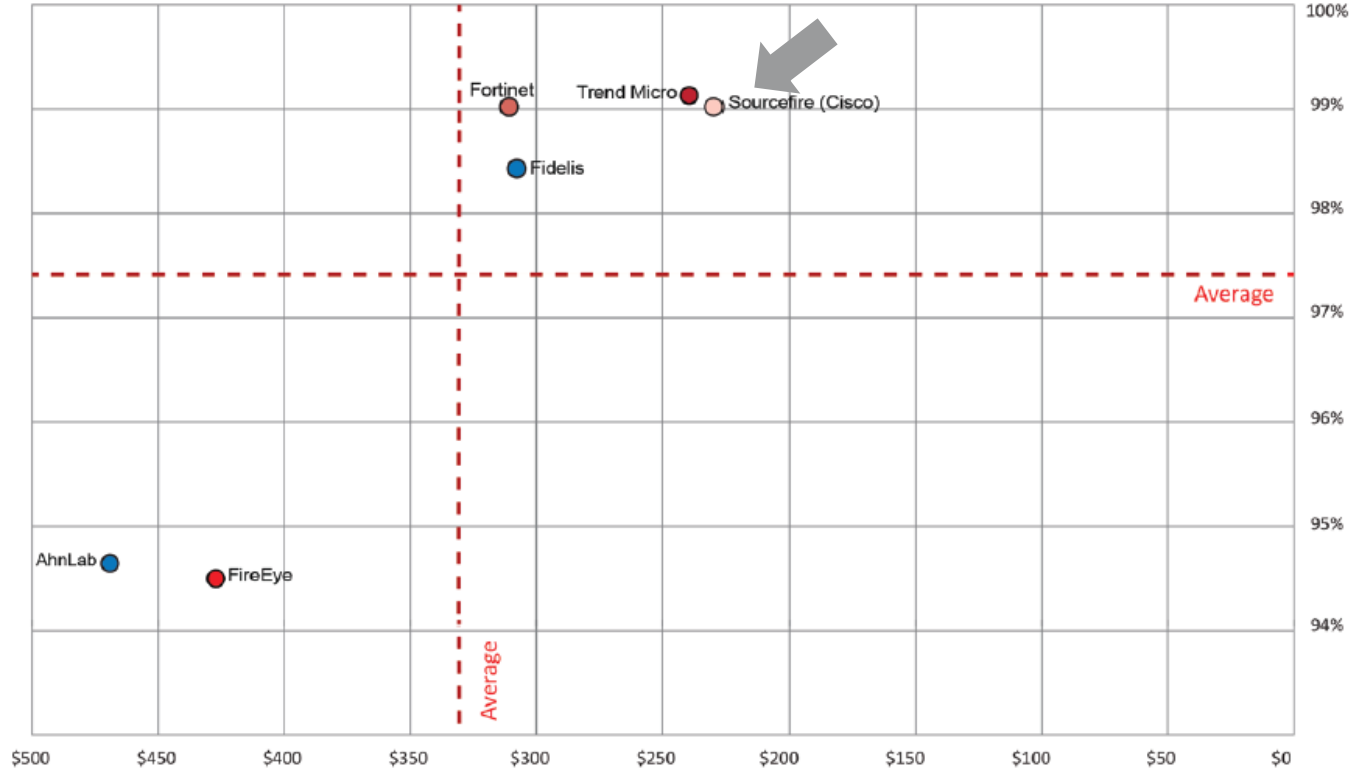
Cisco Advanced Malware Protection

Best Protection Value

99.0% Breach Detection Rating

Lowest TCO per Protected-Mbps

Other Products Do Not Provide Retrospective Security After a Breach



Thank you.





CISCO