Cisco Advanced Malware Protection for Endpoints

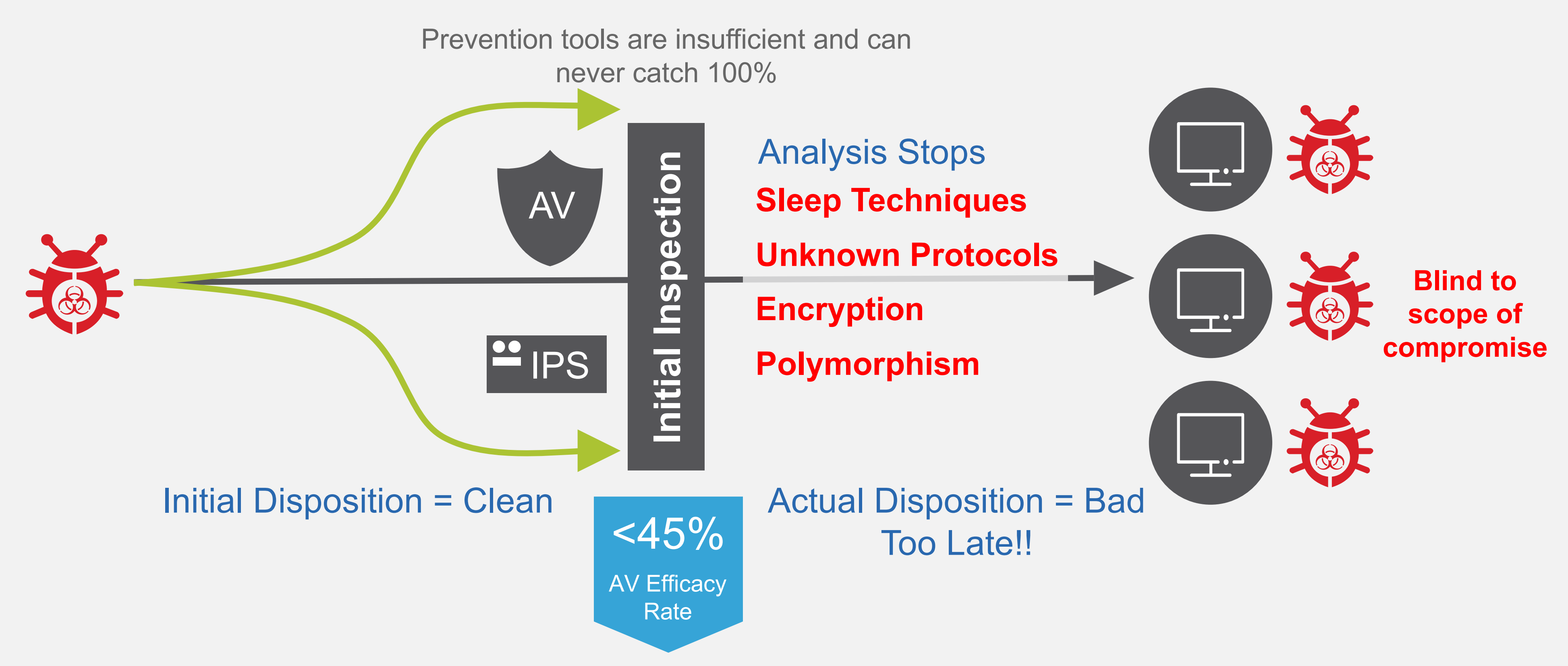
Donald J Case

BizCare, Inc.

Saturday, May 19, 2018

Every single attack that an organization experiences is either on an endpoint or it's headed there

Malware is getting in. Prevention tools alone can't catch everything and provide limited visibility into threats once inside



Prevention tools are insufficient and can never catch 100%

Analysis Stops

Sleep Techniques

Unknown Protocols

Encryption

Polymorphism

Blind to scope of compromise

Initial Disposition = Clean

<45%

AV Efficacy Rate

Actual Disposition = Bad
Too Late!!

Failing Prevention Tools and No Visibility on the Endpoint Means Increased Time to Detection

65%

of organizations say attacks evaded existing preventative security tools

55%

of organizations unable to determine cause of breach

100 Days

Industry average time to detection

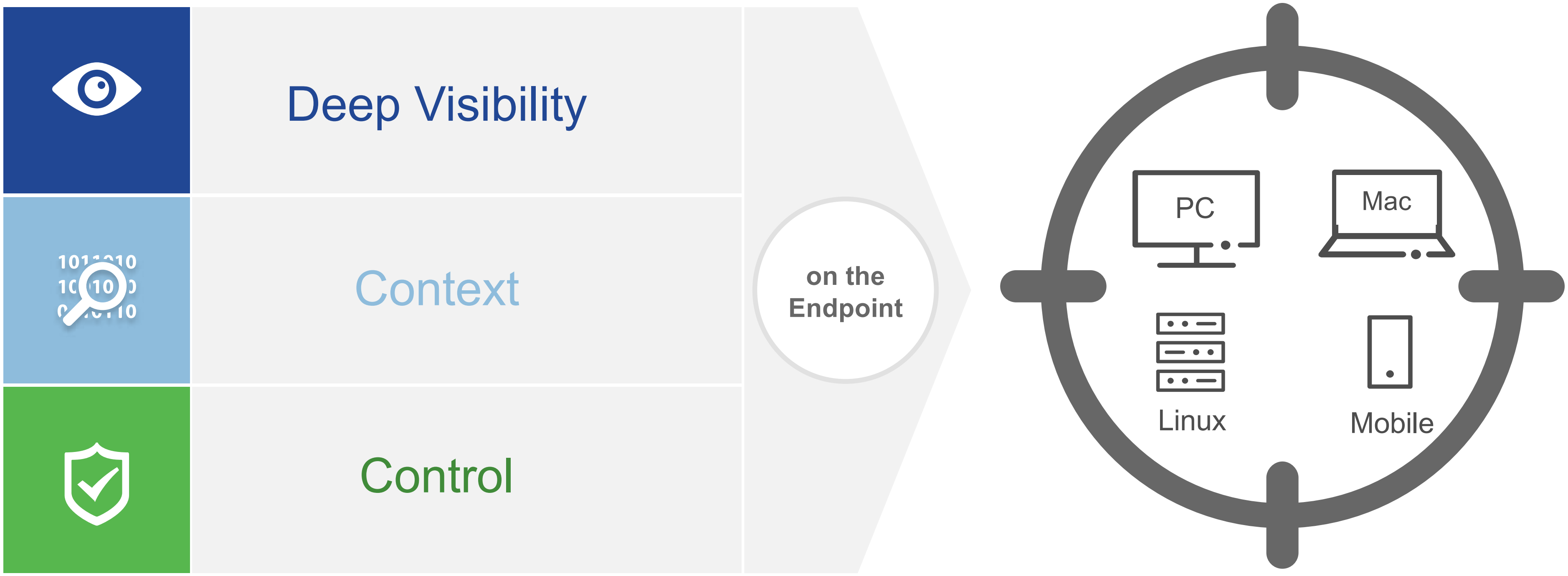
-Source: 2016 Cisco Midyear Security Report; 2014: A Year of Mega Breaches, Ponemon Institute

Complexity makes the problem worse. Juggling 40 to 60 disparate security point products slows you down, inhibits your ability to scope a compromise, and increases gaps in protection

	Overall Performance	Time to Detection	Cost
40 to 60 fragmented offerings across multiple vendors →	**Less communication** between disparate point products	**More lag** in finding threats	**Higher total cost** to build and run
vs.			
Integrated advanced security solution →	**Better communication** between components	**Faster** time to detection	**Lower** OpEx and easier to manage

Our Philosophy

Malware will get in. You must prevent what you can, but you can never prevent 100% of attacks. So what's needed to protect against threats that get in?



Deep Visibility

Context

Control

on the Endpoint

What Is Cisco AMP for Endpoints?

- Software as a service (subscription)
- Cloud managed
- Lightweight connector
- Protects Windows, Mac, Linux, and Android

AMP for Endpoints

Prevent

Prevent attacks and
block malware in real time

Monitor

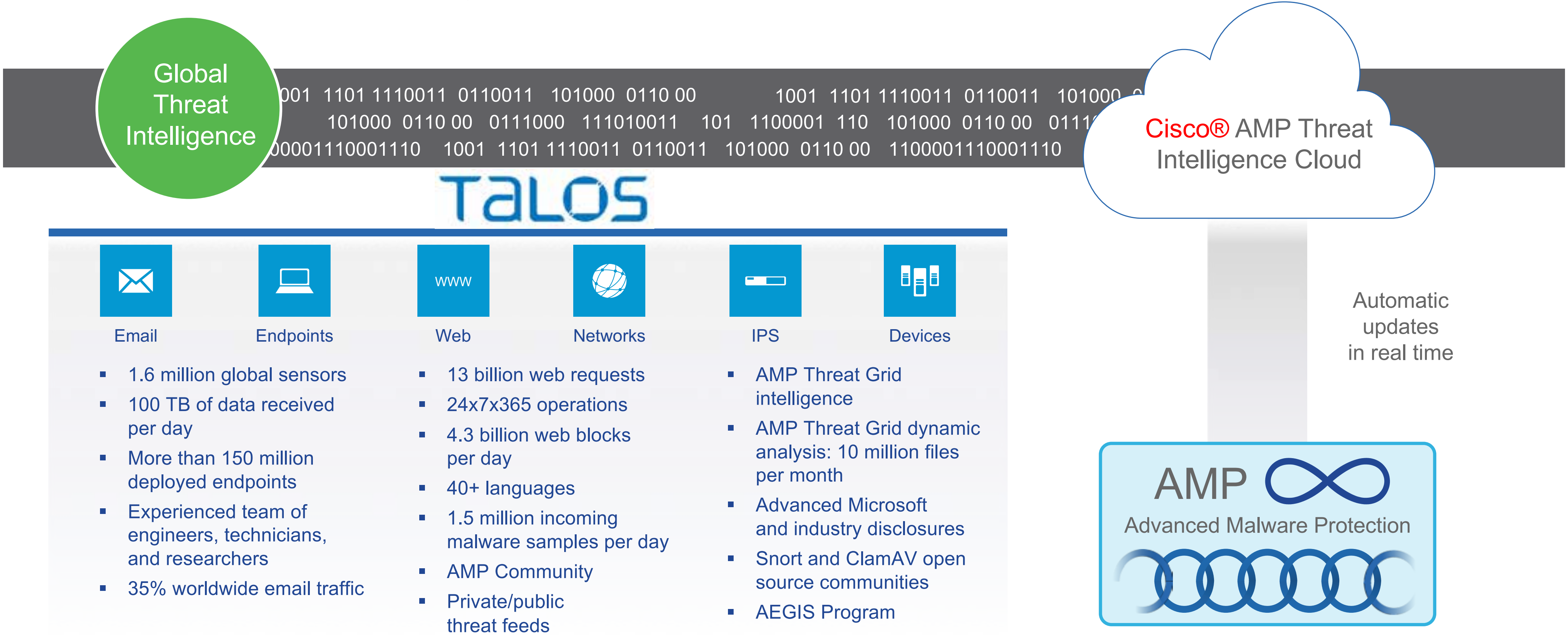
Continuously monitor for threats on your
endpoints to decrease time to detection

Respond

Accelerate investigations and
remediate faster and more effectively

Harden Your Defenses with the Best Global Threat Intelligence

Prevent



Global Threat Intelligence

Talos

Email

Endpoints

Web

Networks

IPS

Devices

- 1.6 million global sensors
- 100 TB of data received per day
- More than 150 million deployed endpoints
- Experienced team of engineers, technicians, and researchers
- 35% worldwide email traffic

- 13 billion web requests
- 24x7x365 operations
- 4.3 billion web blocks per day
- 40+ languages
- 1.5 million incoming malware samples per day
- AMP Community
- Private/public threat feeds

- AMP Threat Grid intelligence
- AMP Threat Grid dynamic analysis: 10 million files per month
- Advanced Microsoft and industry disclosures
- Snort and ClamAV open source communities
- AEGIS Program

Cisco® AMP Threat Intelligence Cloud

Automatic updates in real time

AMP

Advanced Malware Protection

Prevent

Block Attacks at Point of Entry

AMP Delivers the First Line of Defense, Blocking Known and Emerging Threats

Automatically stop as many threats as possible, known and unknown, using a combination of cloud- and system-based prevention technologies

- One-to-one signature
- Fuzzy fingerprinting
- Machine learning and rootkit scanning
- Built-in antivirus detection engine
- Static and dynamic analysis (sandboxing)

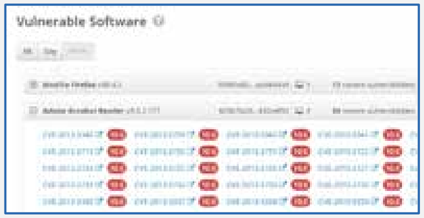
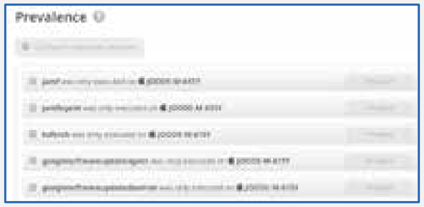
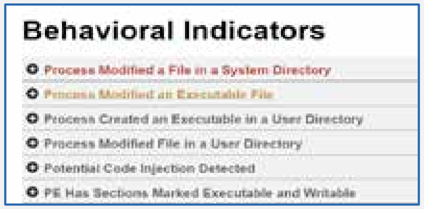
→

- Offer better accuracy and dispositioning
- Block known and emerging threats
- Protect your business with no lag

Prevent

Proactive Protection Tools

Close attack pathways, uncover stealthy malware, and reverse-analyze suspicious threats.

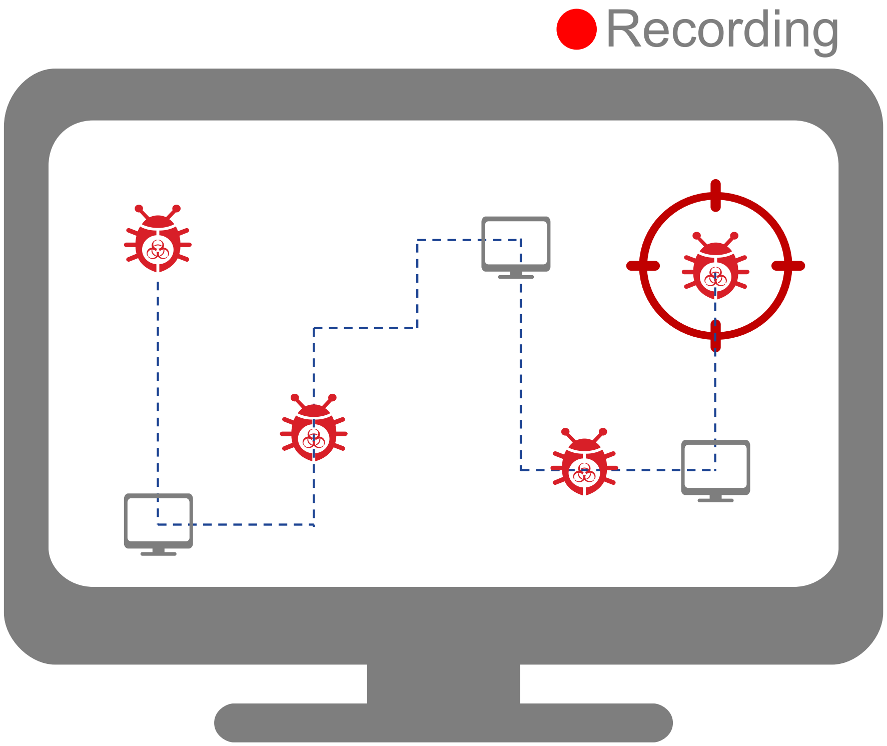
Vulnerabilities	Our vulnerabilities feature shows you, across all of your endpoints, all the software on your system that's vulnerable to malicious attacks, so you can patch them and close any potential attack pathway.	 Vulnerable Software
Low Prevalence	Our low prevalence feature shows you applications on endpoints that are flying under the radar, and lets you take a closer look to see if there's any malicious behavior happening.	 Prevalence
Built-In Sandboxing	Built-in sandboxing capabilities powered by Threat Grid let you submit a file for analysis against over 700 behavioral indicators so you can see what that file is trying to do and if it's bad. Then AMP will automatically block and quarantine the file.	 Behavioral Indicators Process Modified a File in a System Directory Process Modified an Executable File Process Created an Executable in a User Directory Process Modified File in a User Directory Potential Code Injection Detected PE Has Sections Marked Executable and Writable

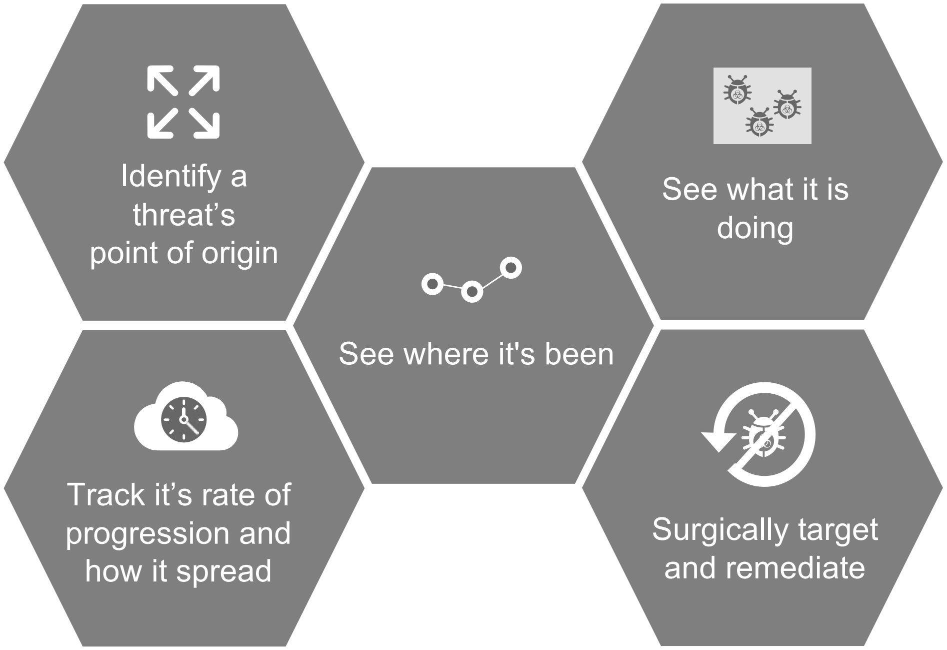
But Prevention Alone Will Never Be 100% Effective

Continuous Analysis and Retrospective Security

AMP for Endpoints Continuously Monitors, Records, and Analyzes All File Activity, Regardless of Disposition, to catch threats that got in

Monitor
+
Detect





Identify a threat's point of origin

See where it's been

See what it is doing

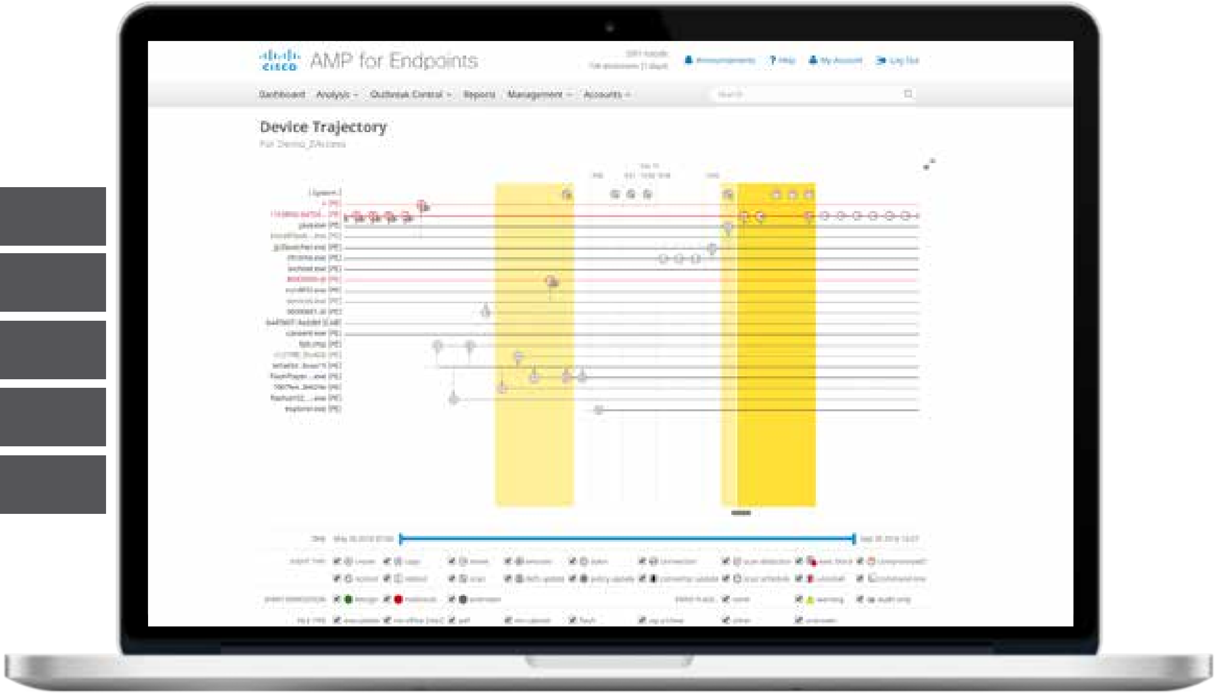
Track it's rate of progression and how it spread

Surgically target and remediate

If Something Gets in, Continuous Analysis and Retrospective Security Helps You Find Answers to the Most Pressing Security Questions

Monitor
+
Detect

- What happened?
- Where did the malware come from?
- Where has the malware been?
- What is it doing?
- How do we stop it?



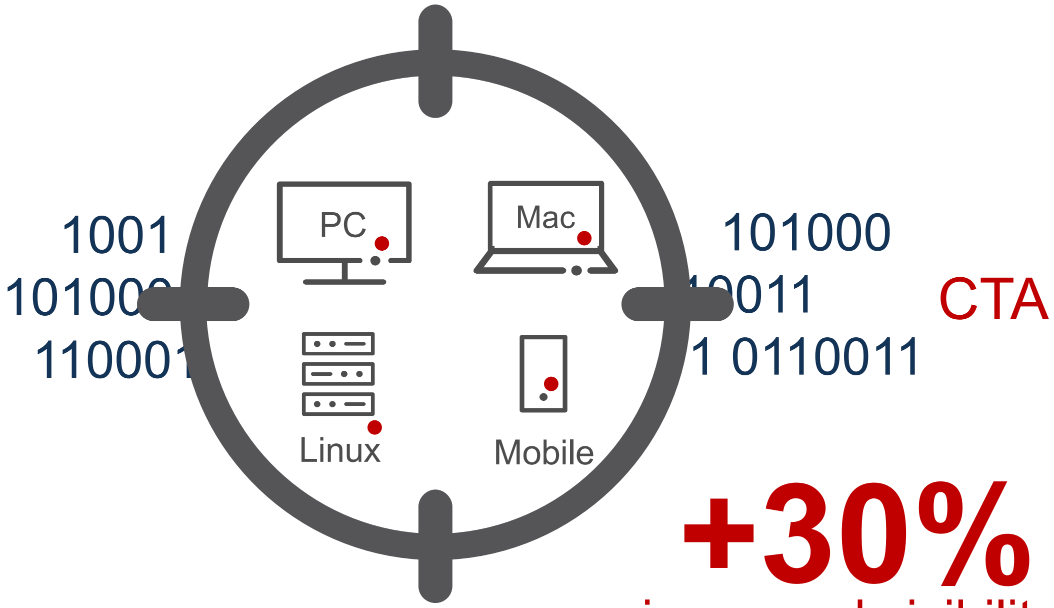
Agentless Detection

Our Cognitive Threat Analytics (CTA) Integration Helps You See Threats on Endpoints Without an Agent Installed

Monitor
+
Detect

- Get visibility into devices where you can't install an AMP for Endpoints connector
- See more malware than before, like fileless or memory-only malware and infections that live in a web browser only
- Catch malware before it compromises the OS level
- Investigations are easier and faster because all detections and threat information are shown in the AMP for Endpoints console

AMP for Endpoints



+30%
increased visibility

Recent Innovations

Cognitive Threat Analytics (CTA) Integration

Get agentless detection when AMP for Endpoints is deployed alongside a compatible web proxy, like Cisco WSA or Blue Coat ProxySG. See an average 30% more infections across your environment; uncover file-less or memory-only malware; catch malware before it compromises the OS-level; get visibility into devices with no AMP connector installed; all managed from the AMP for Endpoints management console.

Built-in AV Detection Engine

We've always provided malware blocking at point-of-entry inspection. Now we encourage customers to turn on our built-in AV engine to perform offline and system-based detections including rootkit scanning to complement Cisco's advanced endpoint protection capabilities. The engine can be enabled and used by customers that want to consolidate their antivirus and advanced endpoint protection in one agent.

New Dashboard UI

Our updated user interface allows customers to better assess the health and state of their security deployment, and ensures a more streamlined management, faster incident response, and improved workflow to triage, manage and respond to possible breaches.

Command Line Visibility

Get visibility into what command lines arguments are used to launch executables to determine if legitimate applications, including Windows utilities, are being used for malicious purposes. For instance, see if vssadmin is being used to delete shadow copies or disable safe boots; see PowerShell-based exploits; see into privilege escalation, modifications of access control lists (ACLs), and attempts to enumerate systems.

Improved Endpoint Search

A simple interface to easily and quickly search across all endpoints looking for artifacts left behind as part of the malware ecosystem, extending search capabilities beyond data stored in the cloud to the endpoint itself.

AMP for Endpoints Decreases Time to Detection

100 Days

to

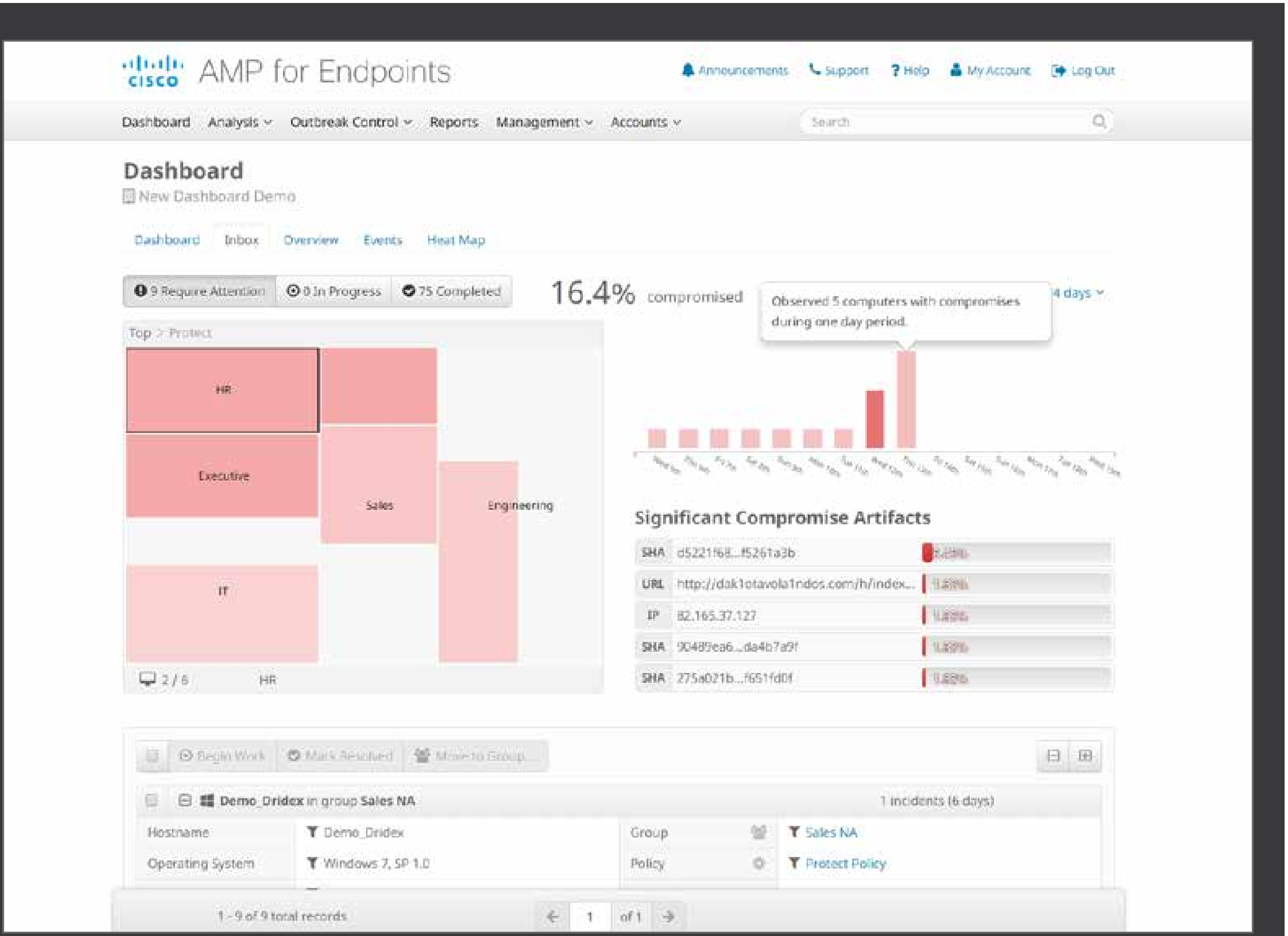
13 Hours or less

Industry average time to detection

AMP for Endpoints time to detection

Source: 2016 Cisco Midyear Security Report

Demo



Dashboard

New Dashboard Demo

9 Require Attention | 0 In Progress | 75 Completed

16.4% compromised

Observed 5 computers with compromises during one day period.

Significant Compromise Artifacts

SHA	d5221f68...f5261a3b	[illegible]
URL	http://dak1otavola1ndos.com/h/index...	[illegible]
IP	82.165.37.127	[illegible]
SHA	90485ea6...da4b7a9f	[illegible]
SHA	275a021b...f651fd0f	[illegible]

Demo_Dridex in group **Sales NA** — 1 incidents (6 days)

Hostname	Demo_Dridex	Group	Sales NA
Operating System	Windows 7, SP 1.0	Policy	Protect Policy

1 - 9 of 9 total records — 1 of 1

See More and Respond Faster with AMP Everywhere’s Integrated Threat Defense

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 security appliances (NGIPS).

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 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 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 Cloud Web Security (CWS) and get visibility and control to defend against advanced threats launched from the web.

Threat Grid

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

Private

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.

University Testimonial

"We received a malware alert. Within a few minutes in the AMP for Endpoints console we were able to determine the malware was using prohibited websites to mask its network traffic. AMP provides us the visibility and control on our endpoints to provide the IT security needs of the university without inhibiting academic freedom and research."

Tim McGuffin, Information Security Officer,
Sam Houston State University

[Video Testimonial]

Bank Testimonial

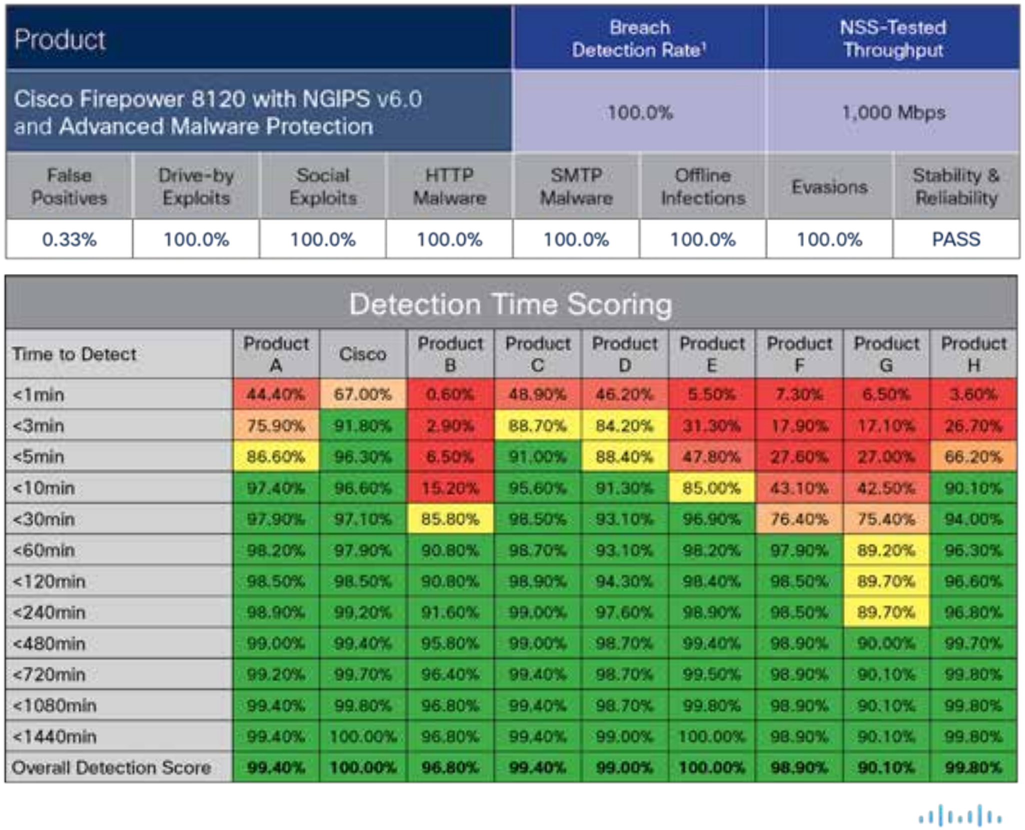
"One of the most successful stories we've had is AMP for Endpoints. We brought it in… and it immediately started solving problems for us."

Dan Polly, VP Enterprise Information Security Officer
First Financial Bank

[*Video Testimonial*]

Cisco AMP is the Leader in Security Effectiveness with Fastest Time to Detection

NSS Breach Detection and Time to Detection Test Results for Cisco



Product	Breach Detection Rate[1]	NSS-Tested Throughput
Cisco Firepower 8120 with NGIPS v6.0 and Advanced Malware Protection	100.0%	1,000 Mbps

False Positives	Drive-by Exploits	Social Exploits	HTTP Malware	SMTP Malware	Offline Infections	Evasions	Stability & Reliability
0.33%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	PASS

Detection Time Scoring

Time to Detect	Product A	Cisco	Product B	Product C	Product D	Product E	Product F	Product G	Product H
<1min	44.40%	67.00%	0.60%	48.90%	46.20%	5.50%	7.30%	6.50%	3.60%
<3min	75.90%	91.80%	2.90%	88.70%	84.20%	31.30%	17.90%	17.10%	26.70%
<5min	86.60%	96.30%	6.50%	91.00%	88.40%	47.80%	27.60%	27.00%	66.20%
<10min	97.40%	96.60%	15.20%	95.60%	91.30%	85.00%	43.10%	42.50%	90.10%
<30min	97.90%	97.10%	85.80%	98.50%	93.10%	96.90%	76.40%	75.40%	94.00%
<60min	98.20%	97.90%	90.80%	98.70%	93.10%	98.20%	97.90%	89.20%	96.30%
<120min	98.50%	98.50%	90.80%	98.90%	94.30%	98.40%	98.50%	89.70%	96.60%
<240min	98.90%	99.20%	91.60%	99.00%	97.60%	98.90%	98.50%	89.70%	96.80%
<480min	99.00%	99.40%	95.80%	99.00%	98.70%	99.40%	98.90%	90.00%	99.70%
<720min	99.20%	99.70%	96.40%	99.40%	98.70%	99.50%	98.90%	90.10%	99.80%
<1080min	99.40%	99.80%	96.80%	99.40%	98.70%	99.80%	98.90%	90.10%	99.80%
<1440min	99.40%	100.00%	96.80%	99.40%	99.00%	100.00%	98.90%	90.10%	99.80%
Overall Detection Score	**99.40%**	**100.00%**	**96.80%**	**99.40%**	**99.00%**	**100.00%**	**98.90%**	**90.10%**	**99.80%**

🟩	= > 90%
🟨	= 80 - 89%
🟧	= 60 - 79%
🟥	= 40 - 59%
🟥	= < 40%

- The leader for the 3rd year in a row in the BDS test – detecting 100% of malware, exploits & evasions.
- Faster time to detection than any other vendor - blocking 91.8% of attacks in < 3 minutes
- Products with faster detection rates get to green numbers faster moving from top to bottom.
- Products may have the same Overall Detection Score at the bottom, but those with the faster time to detection are more effective – giving attackers less time and space to operate.

Market Recognition

“Based on our (Breach Detection Systems) reports, Advanced Malware Protection from Cisco should be on everyone’s short list.”

NSS LABS

Gartner

2016 Vendor Rating for Security: Positive.

“So do any network security vendors understand data center and what’s needed to accommodate network security? Cisco certainly does.”

ESG

FORRESTER®

“… AMP will be one of the most beneficial aspects of the [Sourcefire®] acquisition.”

“Cisco is disrupting the advanced threat defense industry.”

“The AMP products will provide deeper capability to Cisco's role in providing secure services for the Internet of Everything (IoE).”

BizCare
SECURE.IT™

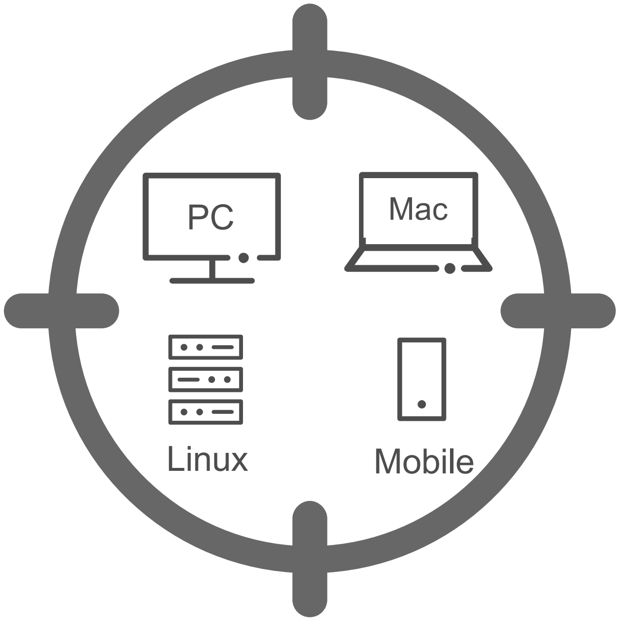
CISCO

bizcare.com/security

Appendix Slides

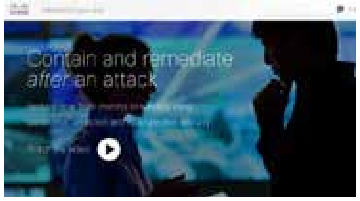
AMP for Endpoints

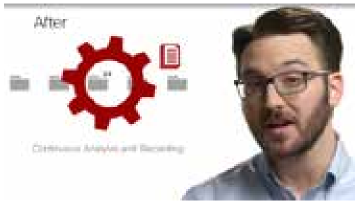
in summary



- Prevention, Monitoring + Detection, Response
- Deep Visibility, Context, and Control if something gets in
- Continuous Analysis of File Behavior and Retrospective Security
- Turn on our AV detection engine in AMP for Endpoints to consolidate agents
- Containment and quarantine on endpoint
- Built-in sandbox powered by Threat Grid
- Open APIs for seamless integration
- Agentless protection via CTA
- More than just endpoint, it’s the integrated security architecture of AMP Everywhere

AMP Assets to Learn More





AMP Webpages

www.cisco.com/go/amp
www.cisco.com/go/ampsolution
www.cisco.com/go/ampendpoint
www.cisco.com/go/ampnetwork

www.cisco.com/go/ampprivatecloud
www.cisco.com/go/amptg

- Cloud deployment
- On-premises deployment

AMP Solution Overview Videos

AMP for Endpoints Overview Video
AMP for Endpoints Continuous Analysis
AMP for Endpoints Threat Intelligence
Cisco Executive Perspectives on Security

AMP for Endpoints Integration with CTA
AMP for Endpoints Integration with CTA Demo
AMP Overview in 4 Minutes: Meet Tom, the IT Security Guy
Solving the Security Patchwork Problem

Demos

5-minute AMP Demo, with Threat Grid integration
AMP Threat Grid for Incident Response

AMP and Threat Grid Full Demo on Techwise TV June 2015
AMP Threat Grid: Portal overview and API demo

Customer Testimonials

Playlist of all Customer Testimonials on AMP
First Financial Bank

SHSU.uses AMP for Endpoints
Center for Internet Security uses AMP Threat Grid

AMP Assets to Learn More

Average Cost of a Breach
$5.4MM
$5.9MM
2013
2014
Average Time To Resolve a Cyber-attack
32 days
45 days
2013
2014

Data Sheets, At-a-Glances, Infographic, Whitepapers

AMP Solution Overview

AMP for Networks: Data Sheet

AMP for Endpoints: Data Sheet | AAG

AMP Private Cloud: Data Sheet

Security Everywhere Whitepaper (direct link)

AMP Threat Grid Solution Overview

AMP Threat Grid - Appliance: Data Sheet | AAG

AMP Threat Grid - Cloud: Data Sheet

Continuous Endpoint Protection in a Point-in-Time World

Third Party Validation

Gartner Video-on-Demand: Strategies to Combat Advanced Threats featuring Cisco AMP

2016 NSS Labs Breach Detection Test Results

The Business Value of Endpoints Security by IDC

Next Generation Endpoint Security Infographic

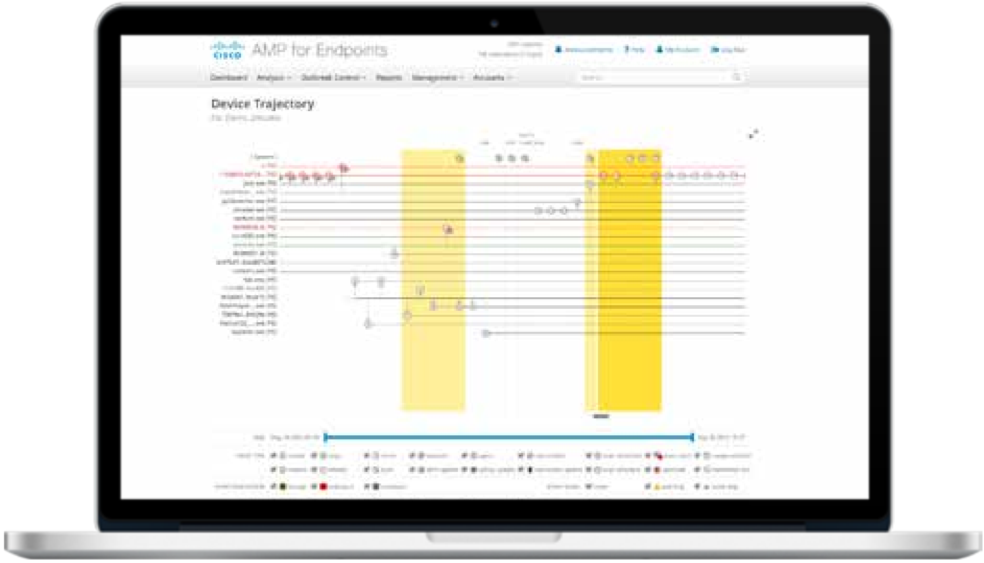
“65% of CEOs say their risk management approach is falling behind. In a **new reality where security breaches come at a daily rate**, we must move away from trying to achieve the impossible perfect protection and instead **invest in detection and response. Organizations should move their investments from 90 percent prevention and 10 percent detection and response to a 60/40 split.**”

— Peter Sondergaard,
Senior VP and Global Head of Research
Gartner

Gartner®

What Do You Get with AMP for Endpoints over AMP for Networks?

- Visibility into executables and file operations
- Device trajectory
- Visibility into and control of off-network endpoints
- Remediation vs. just containment
- Prevalence feature for threat hunting
- See lateral movement between endpoints
- Sharing info between endpoint and network
- Robust tool for incident response teams
- Lightweight connector; no impact on users
- Widest selection of AMP features for visibility and control



Before

Block Threats Before They Breach

A U.S. Bank Case Study

Challenge	An experienced security team of 7 supporting more than 120 locations needed greater intelligence to quickly identify and stop threats. Current defenses alerted personnel and logged details but did nothing to aid the investigation of the situation.
Solution	Augmented intrusion prevention systems with Cisco® AMP for Endpoints.
Result	After installation of AMP for Endpoints, a targeted attack was identified and remediated in half a day. Seven days after the initial attack, new business processes and intelligences implemented by AMP for Endpoints resulted in the immediate mitigation of a second targeted attack.

During

Defend Against Threats During the Attack

FVC Case Study

Challenge

A previous bulky malware solution was not centrally managed, so it was difficult for IT to monitor and troubleshoot the network effectively.

Solution

Installed Cisco® AMP for Endpoints for a lighter footprint, central monitoring, and real-time, remote visibility.

Result

The AMP for Endpoints dashboard helped the team find and stop threats much faster than previous methods. What used to take them hours now requires only 2 or 3 minutes. With remote management, the team is also able to solve many problems remotely and keep employees productive.

Identify Scope and Remediate Impact After Breach

After

Power Utility Case Study

Challenge	The company is a frequent victim of spear-fishing campaigns, with indications of infection emanating from multiple sources.
Solution	Added Cisco® AMP for Endpoints to a system already using a Cisco FirePOWER™ NGIPS to enable the company to track and investigate suspicious file activity.
Result	The company gained complete visibility into its malware infections, determined the attack vector, assessed the impact on the network, and made intelligent surgical decisions for remediation in a fraction of the time that it would take to respond manually.

Business Impact Summary

→ Better protection: Before, during, and after

→ Better visibility, context, and control

→ Better intelligence

→ Faster response

→ Save money and time

→ Protect resources and maintain business-critical functions

→ Highest security leadership (NSS Labs)

Customer Challenges

- Prevention tools are not enough
- Malware still getting in

- No visibility into file activity on endpoints once malware gets in
- If I can't see malware, I can't detect it or respond quickly

- Complexity: too many tools, too much to manage.
- Complexity is slowing us down