Advanced threats call for Advanced Malware Protection (AMP)

Why prevention tools alone are not enough!

Dale Long-Consulting Security Engineer-Advanced Threat Solutions, Cisco Systems
Cisco Knowledge Network - Service Provider Webinar Series

February 13, 2019
Today’s Presenters

John Malzahn
Senior Manager, Service Provider Solutions Marketing
Cisco Systems

Dale Long
Consulting Security Engineer, Advanced Threat Solutions
Cisco Systems
Attending MWC This Month?
Come See Us

Mobile World Congress
Barcelona, February 25 – 28
Cisco Booth Located in Hall 3 Booth #3E30
Agenda

• Managed Security Market Trends
• Why Cisco Security
• AMP Endpoints Overview
• AMP Endpoints MSSP/GSP Solution
• Additional Resources
Managed Security Trends

ask-mssp-amp@cisco.com
Customers Need Help with Endpoint Security

Organizations lack the resources necessary to respond to advanced threats on the endpoint

Lack of Available Security Talent

(ISC)² estimates that the number of unfilled cybersecurity jobs will rise to 1.8 million by 2022

Lack of Available Budget

Over half of the security professionals named cost efficiency and unbiased insight as the top reasons to outsource security

Evasion Techniques Advancing

Today’s threats employ advanced evasion techniques designed specifically to get around preventative security tools

Diverse Endpoint Ecosystems

Mobile and flexible workforces have introduced a diverse set of endpoint types and increased complexity of environment
Increasing Demand for Managed Security Services

Outsourcing security enables organizations to concentrate on what matters most

Q: Have you engaged with a security services provider for Cloud Managed SaaS-security?
MSSP Market Transitioning to Cloud

Cloud-based security service revenue totaled $9.1B in CY16

- 13% up from $8.1B in CY15
- 43% growth over the next 5 years to $13.1B in CY21
- 7.5% CY16 to CY21 CAGR
## Needs and Challenges MSSPs Face

<table>
<thead>
<tr>
<th>Challenges</th>
<th>Needs</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Inefficient service creation and ongoing operations</td>
<td>• Improved management and visibility/interoperability</td>
</tr>
<tr>
<td>• Increasingly competitive environment</td>
<td>• Vendors who are easy to do business with</td>
</tr>
<tr>
<td>• Differing customer needs</td>
<td>• Flexible licensing models</td>
</tr>
<tr>
<td>• Flexibility to adjust services quickly and efficiently</td>
<td>• Minimal upfront capital investments</td>
</tr>
</tbody>
</table>
Why Cisco Security?

ask-mssp-amp@cisco.com
Why Cisco?

- Drive monetization of new services
- Offer fast and agile deployment
- Integrate products seamlessly
- Manage customers efficiently
- Prove your ongoing value to customers
- Protect customers from advanced threats
The Cisco difference for MSSPs is that no other company combines...

- Threat intelligence from Talos
- An end to end security portfolio
- Security market leadership
- Multiple cloud security offerings
Stop global threats more effectively with integrated threat intelligence

Cloud – Public, Private

MASSIVE VOLUME

- 20 billion
  Threats blocked daily

- 1.5 million
  Daily malware samples

- 16 billion
  Daily web requests

UNPARALLELED EXPERTISE

- 250+
 threat intel researchers;
  24 – 7 – 365

- Over 100
  Threat intelligence partners
Differentiate with a Comprehensive Architecture of Security Solutions

Better together:
- Integration
- Scale
- Efficacy
AMP Architecture - See once, block everywhere

Shared intelligence across network, web, email, and endpoints to see once, block everywhere.
Cisco Advanced Malware Protection delivers...

- Point in Time Protection
- Protection Lattice + Threat Grid (sandbox)

- Retrospective Security
- Continuous Analysis
Cisco's Next Gen Endpoint Security

- 10M+ Endpoints
- 4,200+ Customers
- Apple Partnership
- Gartner MQ “Visionary”
- Global Customer Success
- Architecture: Network, Endpoint, Cloud
- MSLA
- 1100+ AMP - Certified Partner Engineers
- Incident Response Services
- Protection, Detection & Response in a Single Agent
- Talos
- NSS Labs “Recommended”

Simple, Open, Automated
What Is Cisco AMP for Endpoints?

→ Software as a service (subscription)
→ Cloud managed
→ Lightweight connector
→ Protects Windows, Mac, Linux, Android, New! iOS
Holistic view of endpoints
Regardless of operating system – from servers to desktop to mobile devices
Uncover the 1% with Cisco AMP for Endpoints

Stop Malware
Using multiple detection and protection mechanisms

Eliminate Blind Spots
The network and endpoint, working together across all operating systems

Discover Unknown Threats
With proactive threat hunting
Stop Malware

Using multiple detection and protection mechanisms
How we...

Prevent
- Antivirus
- Fileless malware detection
- Cloud lookups (1:1, 1:many)
- Client Indicators of Compromise

Detect
- Static analysis
- Sandboxing
- Malicious Activity Protection
- Machine learning
- Device flow correlation
- Cloud Indicators of Compromise

Reduce Risk
- Vulnerable software
- Low prevalence
- Proxy log analysis
Discover Unknown Threats

With proactive threat hunting
How does that 1% get through?

Advanced evasion techniques:

• Fileless malware
• Environmentally-aware malware
• Polymorphism
• Exploit legitimate processes
• Multi-Stage Vector Exploits/
The question is no longer if malware will get into your network
It’s how quickly you can detect the infection, understand scope, and remediate the problem

- Where do I start?
- How bad is the situation?
- What systems were impacted?
- What did the threat do?
- How do we recover?
- How do we keep it from happening again?
AMP Endpoint Continuous Monitoring

What happened?
Where did the malware come from?
Where has the malware been?
What is it doing?
How do we stop it?
Dynamic Analysis and Sandboxing

Execute, analyze, and test malware behavior in order to discover previously unknown zero-day threats.

AMP for Endpoints

Suspicious File

Analysis Report

Threat Grid
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
Prospective MSSP Services

Single Solution Enables Multiple Managed Security Service Offerings

Next Generation Endpoint Security (NGES) with extensive visibility & threat analytics

- Endpoint Protection (EPP) + Endpoint Detection & Response (EDR) combined capability = Managed Detection and Response (MDR) which is now tracked by industry analysts

Single agent promotes Anti-Virus (A/V) Replacement opportunities

- PCI & HIPAA compliant solution

Ransomware Defense Solution

- AMP Endpoint + Umbrella + AMP for Email (separate licensing/pricing dynamics)

Incident Response / Breach Readiness Services

- i.e. Incident Response – Security Consulting

Mobile Cisco Security Connector for iOS (Clarity)

- Highly differentiated iOS offering with upsell path to Umbrella and Meraki-SM

AMP & Threat Grid Everywhere Architecture attach Opportunities

- “Detect Once – Protect Everywhere” across NGFW, NGIPS, E-Mail, Web, Meraki, ISR
AMP Endpoint MSSP/GSP Capabilities

Multitenancy
Add, move, and change customers while keeping client environments separate

Comprehensive Reporting
Keep customers informed through automated, customizable reports

API integrations
Easily integrate Cisco solutions with your portfolio and management systems

Easy service creation
Deploy advanced cloud-based security solutions quickly
Customer Service Creation in Multi-Tenant AMP Endpoint Cloud

AMP Endpoints
MSSP Console

- Cloud Based
- Multitenant
- Provisioning
  - Licensed
  - Trials / Evaluations
  - NFR (Not-for-resale)
- Reporting
- API key management
- MSLA support
- Term Licensing Support

© 2017 Cisco and/or its affiliates. All rights reserved.
Managed AMP Endpoint Customer Deployments

AMP MSSP Portal

AMP Public Cloud

Customer 1

Customer 2

Customer 3

MSSP AMP Solutions

AMP MSSP (customer) REST API

MSSP SOC

Customer AMP Endpoint ThreatGrid File Analysis Submission and Reports

AMP Endpoint Management Services
Provisioning Users
Connector Deployment
Management & Monitoring
Response
Ongoing Support

MSSP Provides A4E Connector download link and/or installation package to individual customers
Software Buying Then and Now with MSLA
Managed Service License Agreement

**Then**
- High-Watermark Acquisition
- Perpetual licensing
  - You shoulder all the risk -- buy up front and then monetize over time
  - Lack of portability
- Term licensing
  - Term starts before you can monetize -- "lost" revenue
  - Must track multiple license termination periods across customers
- POs issued for every customer opportunity

**Now**
- ONE: Contract & Order
- FIXED: Term & Price
- MATCH: Revenue & Cost
- MORE: Portability & Flexibility
- PAY: Monthly & After Use

Partner Scenario:
MSP wants to launch managed AMP Endpoint security service

- High-Watermark Acquisition
- Perpetual licensing
- Term licensing
- POs issued for every customer opportunity
MSLA Economical: Matching of Revenue with Cost

A Utility-Based Buying Program - Shared Risk, Shared Success

- Initial three-year term
- Accommodates reuse and upgrades
- Greater licensing flexibility

- Utility pricing with monthly postpaid billing
- Shared risk with lower barrier to entry
Summary of Benefits from MSLA
What Services Does MSLA Enable You to Offer Your Customers?

- **Simplicity**
  - No more thousand line co-terms & complicated license management
  - Drastically reduce build/rollout costs and match costs with revenue
  - Create services quickly without opportunity-killing financial analysis paralysis

- **Lower risk**
- **Greater business agility**
## AMP for Endpoints MSSP/GSP Benefits

- No hardware, all cloud managed from a multi-tenant portal
- Supports the Managed Service Licensing Agreement (MSLA) which is a post-paid, OPEX, utility based pricing with *no up-front CapEx investment required*
- Next Generation Endpoint Security capabilities and service offerings
- Simply deploy software solutions as needed (trials and NFR’s supported as well)
Additional Resources

ask-mssp-amp@cisco.com
AMP Endpoint MSSP
Partner Media Release / References

"Even the Odds" with Advanced Endpoint Protection

Hackers constantly come up with new cyber attacks to cause trouble or profit from your business’s vulnerabilities.

CompuCom’s endpoint security solutions provide multiple layers of effective protection. The antivirus in our Endpoint Management package blocks traditional online threats, while our Anti-Malware as a Service detects and removes today’s more advanced menace such as ransomware.

Anti-Malware as a Service

CompuCom’s Anti-Malware as a Service (AMP) combines our 30 years of experience in management services to ensure total endpoint protection support and elimination of all malware. Learn how to protect your business.

https://www.compucom.com/services/endpoint-security-services

Get malwares
Continuously monitor malicious behavior and quickly detect malicious programs
Prevent infections and detect malware
From 3.9 € per month

Secure all your devices and block malware in real time

A protection solution based on technology:


Advanced malware protection & detection service

NetDefend Malware Protector provides an extra layer of defense against known and emerging threats. Our malware protection is designed to software, endpoints, and applications used to run malware. It provides comprehensive protection for users, applications, and the network infrastructure. It performs in real-time to protect against known and unknown malware to keep your environment safe and secure.


“AMP’s multitenant, cloud-based delivery model has made it easier than ever to introduce enhanced security services to our customers with no upfront costs.”

- Rick Chapman, CTO, InterVision Systems LLC
For more information

Visit
www.cisco.com/go/mssp
www.cisco.com/amp

or contact your Cisco account representatives
Questions?
Compliance

• Cisco AMP for Endpoints meets and exceeds the capabilities of a traditional antivirus solution required for PCI and HIPAA compliance

• Detailed white paper available outlining how AMP exceeds the requirements of PCI DSS v3.2 and the HIPAA Security Rule

• Covers Windows, Mac, Linux, Android, and iOS

“AMP undeniably meets and exceeds PCI and HIPAA requirements.”

- Qualified Security Assessor
Accolades

- Cisco named a ‘Visionary’ in 2018 Magic Quadrant for Endpoint Protection Platforms
- NSS Labs provides ‘Recommended’ rating in 2018 Advanced Endpoint Protection test
- NSS Labs finds AMP has fastest time to detection 3 years in a row, Breach Detection Test
- IDC names AMP for Endpoints a Leader in Endpoint Specialized Threat Analysis and Protection, 2017 vendor assessment
Customers Love AMP for Endpoints
Techvalidate Customer Survey

The Response

- Recipients: 8,500 AMP for Endpoints users
- Responses: 1047
- Response Rate: 13%
- Volunteer References: 113

https://www.techvalidate.com/collections/amp-for-endpoints-survey-results

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Partner Confidential
See how we stack up against the competition

<table>
<thead>
<tr>
<th>Detection</th>
<th>Cisco AMP for Endpoints</th>
<th>Carbon Black Endpoint Security</th>
<th>CrowdStrike Falcon</th>
<th>CylancePROTECT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of integrated detection techniques</td>
<td>13</td>
<td>4</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>Continuous analysis and retrospective detection</td>
<td>✔</td>
<td>Limited</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Device trajectory</td>
<td>Continuous</td>
<td>🟢</td>
<td>✗</td>
<td>Limited</td>
</tr>
<tr>
<td>Detection measures</td>
<td>Multiple</td>
<td>Multiple</td>
<td>Multiple</td>
<td>Multiple</td>
</tr>
<tr>
<td>Dynamic file analysis</td>
<td>Threat Grid</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
</tbody>
</table>


© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Partner Confidential