Pervasive Cybersecurity in the Digital Era

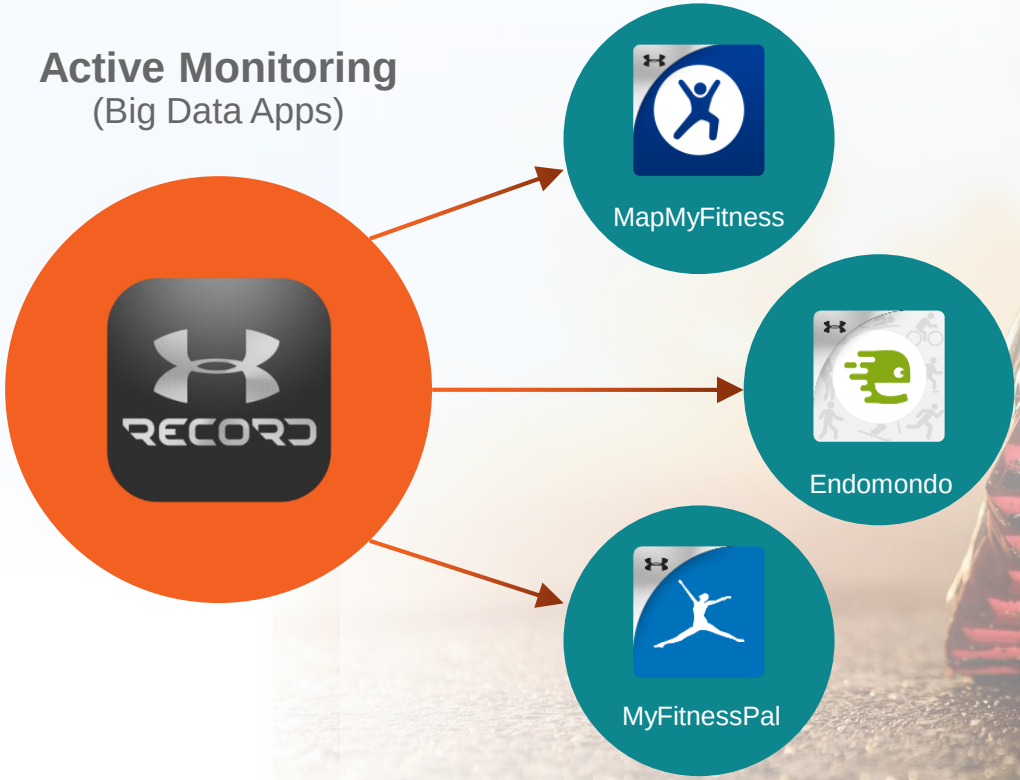
Securely Connecting Everything

Steve Martino
VP, Chief Information Security Officer

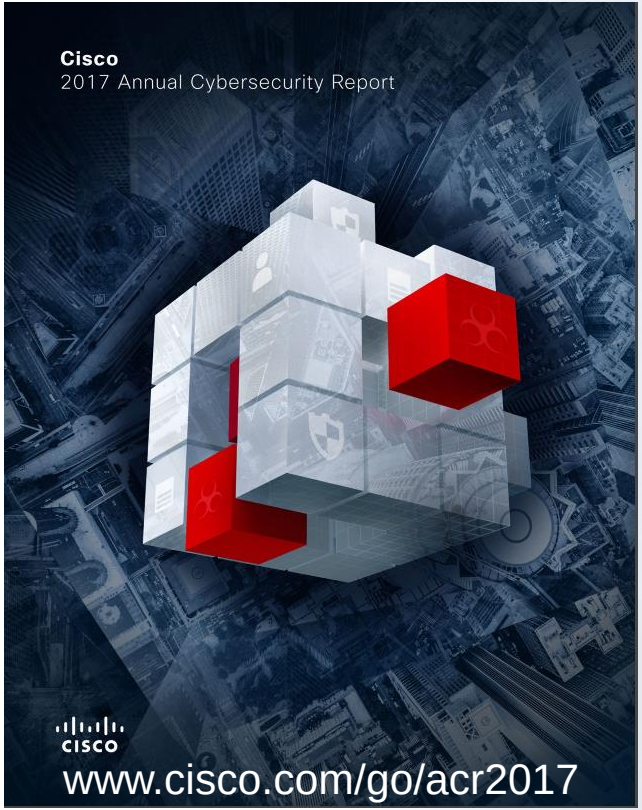
February 12, 2017

Fitness Going Digital

From Active Wear to Digital Coaching



Cisco Telemetry



- 16 billion web requests a day
- 600 billion emails a day
- In aggregate, block almost 20 billion threats per day
  - More than 1.5 million unique malware samples daily
- 18.5 billion AMP queries

TALOS

250 Threat Researchers

Study Included 13 countries

~3000 Respondents

Losses After an Attack are Real for Organizations

Opportunity

23%

44% were losses >20%

Revenue

29%

63% were losses >20%

Customers

22%

61% were losses >20%

IT Security Personnel (n=2,912)

Source: Cisco Annual Security Report, January 2017

IT/Security is not Keeping Pace

Cisco Security Report Findings

Increasing Vulnerabilities

Avg. Increase/Month

Aging Infrastructure

Devices Running Known Vulnerabilities

Weak Operational Practices

Human Errors
Lack Security Personnel

Security Complexity

Many Vendors
Many Tools

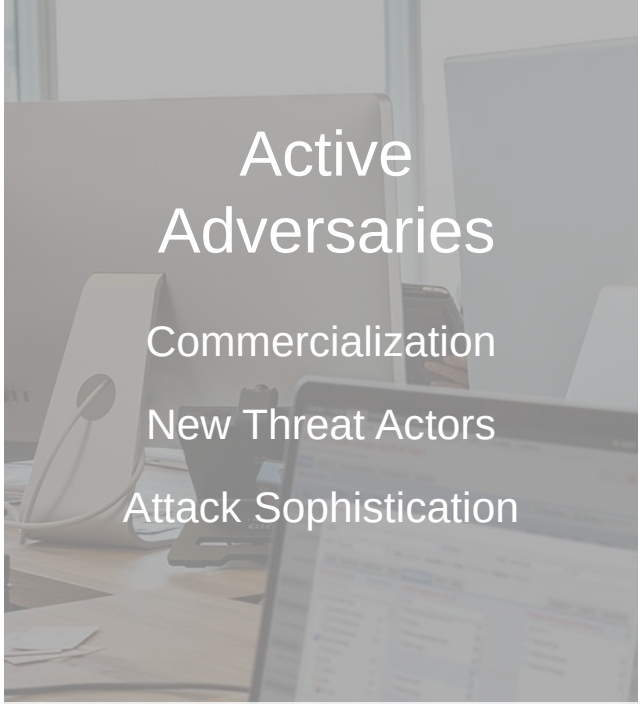
Source: Cisco Mid-Year Security Report, June 2016 & Cisco Annual Security Report, January 2017

A Growing Digital Economy

Change in Social Behavior

500B Devices Connected by 2030

Changing Business Models

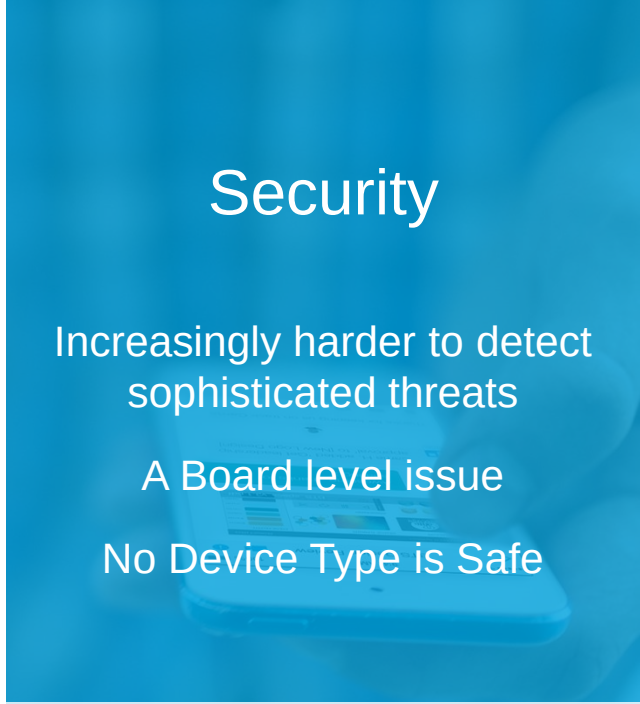


Active Adversaries

Commercialization

New Threat Actors

Attack Sophistication



Security

Increasingly harder to detect sophisticated threats

A Board level issue

No Device Type is Safe

Security Challenges

Trust is Critical to Growing the Digital Economy

Trust is Under Attack

Pervasive Security is Imperative

Defending Cisco: What We Must Protect

300 partner extranet connections
500 Cloud ASPs

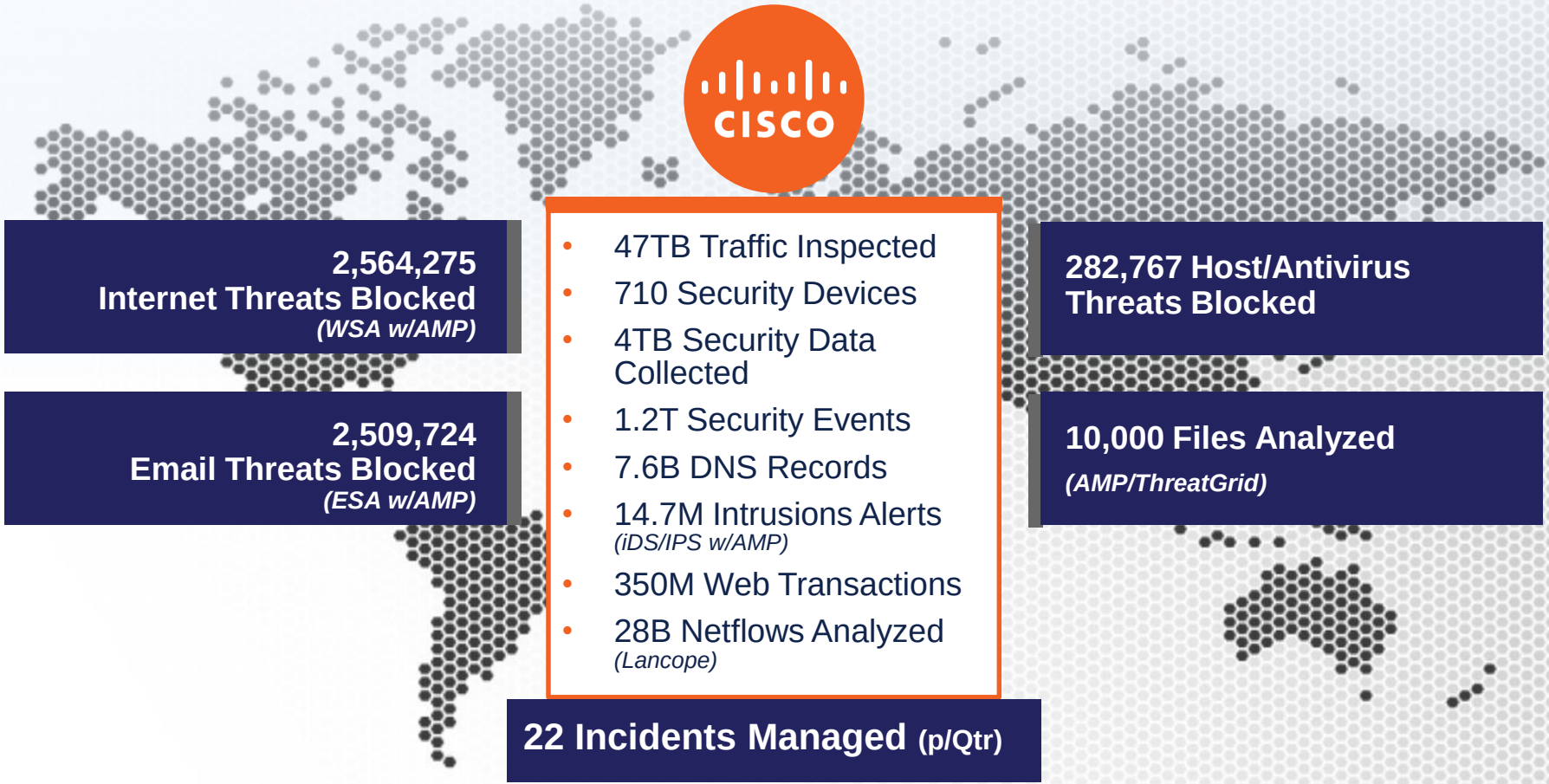
WebEx, Meraki, OpenDNS and Growing Portfolio of Offers

- 122K Workforce
- 170 Countries
- ~3M IP Addresses
- 215K Infra Devices
- 275K Total Hosts
- 2500+ IT Applications
- 26K Connected Cisco Virtual Offices

16 major Internet connections
~47 TB bandwidth used daily

1350 Labs
180+ Acquisitions

Defending Cisco: A Day in Security



2,564,275
Internet Threats Blocked
(WSA w/AMP)

2,509,724
Email Threats Blocked
(ESA w/AMP)

- 47TB Traffic Inspected
- 710 Security Devices
- 4TB Security Data Collected
- 1.2T Security Events
- 7.6B DNS Records
- 14.7M Intrusions Alerts *(iDS/IPS w/AMP)*
- 350M Web Transactions
- 28B Netflows Analyzed *(Lancope)*

282,767 Host/Antivirus Threats Blocked

10,000 Files Analyzed
(AMP/ThreatGrid)

22 Incidents Managed (p/Qtr)

Pervasive Security Framework

Threats/Risks

Regulatory Requirements

Governance & Operational Excellence

- Standards & Policies
- Risk Assessments
- Privacy Engineering
- Architecture Reviews
- Vulnerability Management
- Analytics, Metrics & Reporting

People

Users

- COBC
- Targeted Awareness
- Security Training (Ninja, SKE, EMS)

Accountability

- Security Primes & Advocates
- Partner Security Architects
- Business Partnerships

Validated Identity

Identity

- Federated (Inbound/outbound)
- Strong Multi-Factor
- Separation (User<->Admin)

Contextual Access Control

Location, Time, Role

Endpoint

- Profiling
- Registration
- Posture Assessment

Trusted Resources (Private/Third Party/Hybrid Cloud)

Network

- ESA/WSA
- AnyConnect
- NGFW/IPS
- AMP
- ISE
- ACI

Service

- Application
- Endpoint
- Host
- XaaS

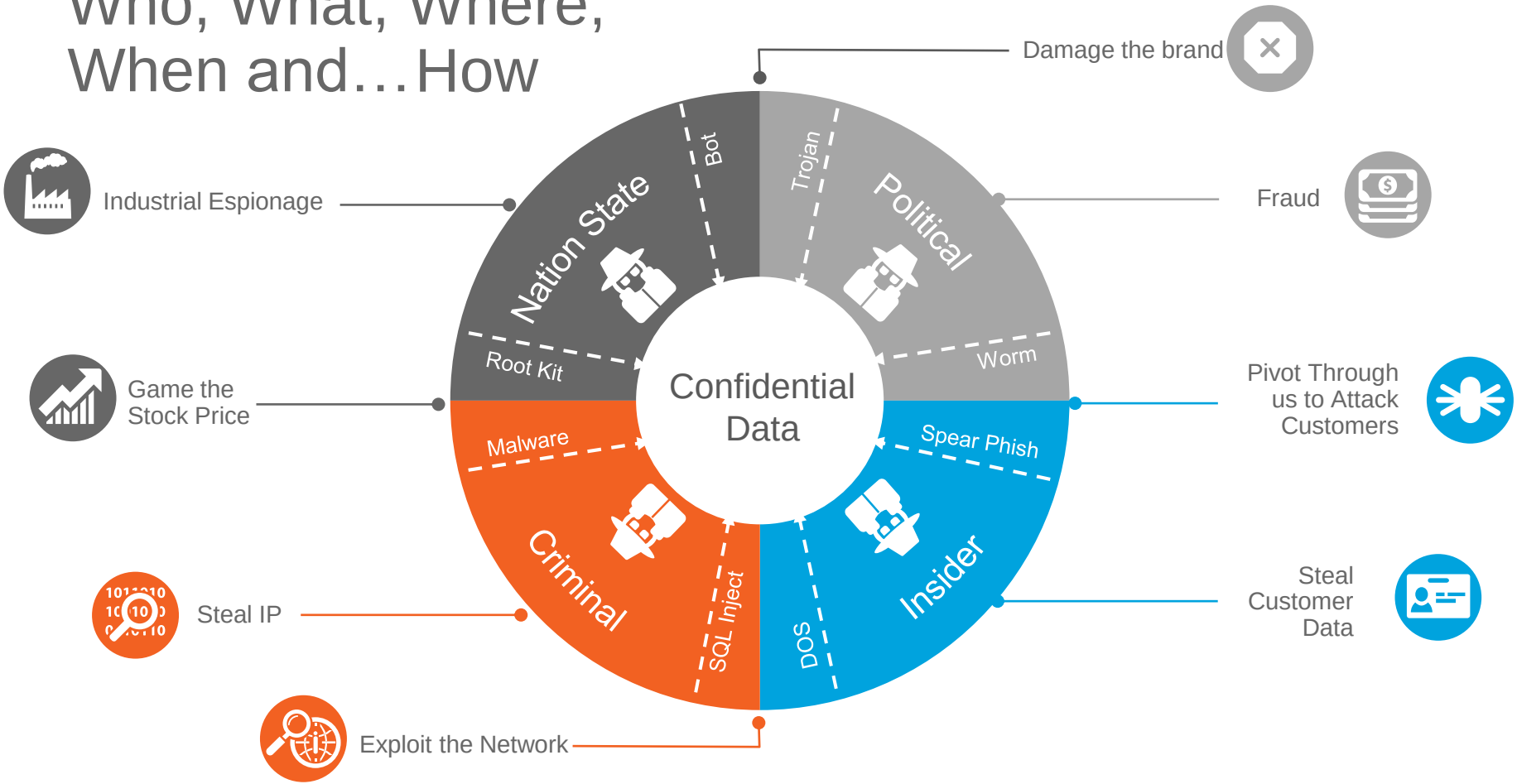
Data

- Ownership
- Accountability
- Visibility
- Pervasive Protection
- Adaptive Access & Control

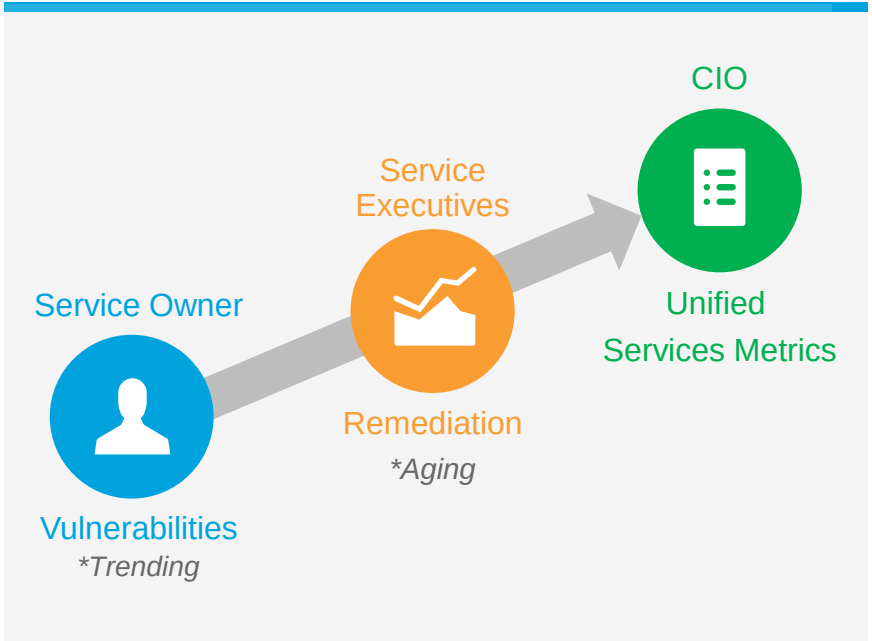
Adaptive Defense (Detect, Respond, Mitigate)

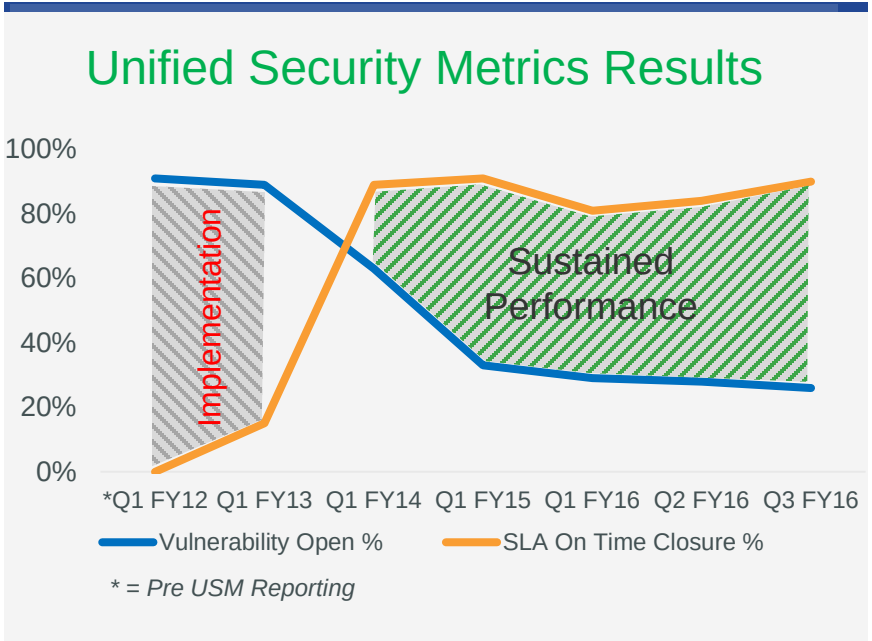
Comprehensive Telemetry, Integrated Intelligence, Pervasive Detection, Playbooks

Who, What, Where, When and…How



Balancing Features vs Operational Efficacy





Vulnerabilities Declined 64% – On-time Closure Increased to 86%

Security Education Campaign – Phishing

- Phishing is #1 source of endpoint compromise
- Different levels of sophistication and difficulty each quarter
- Remember it only takes one Phish to compromise YOU

All Employees	Qrtly Phish 1 Financial Restrictions	Qrtly Phish 2 Message Notification	Qrtly Phish 3 Account Closing	Qrtly Phish 4 Final Version
Targeted Employees	IT-Admins, Finance, HR, Exec Admins…			

Expanding Accountability

Service Executive

1 or more primes

Service Owner

1 or more primes

Service Security Prime

- CSO of the Service
- Single point of accountability
- Increase communication and awareness around security

- Security SMEs
- Security architecture reviews
- Trusted advisors

InfoSec Team

- Establishes security technology baselines
- Formal approval for exceptions
- Establishes corporate security policies and guidelines

Key Elements of Data Protection Program

Taxonomy

Identification and Classification

Data Risk and Organizational Maturity

Awareness and Education

Oversight and Enforcement

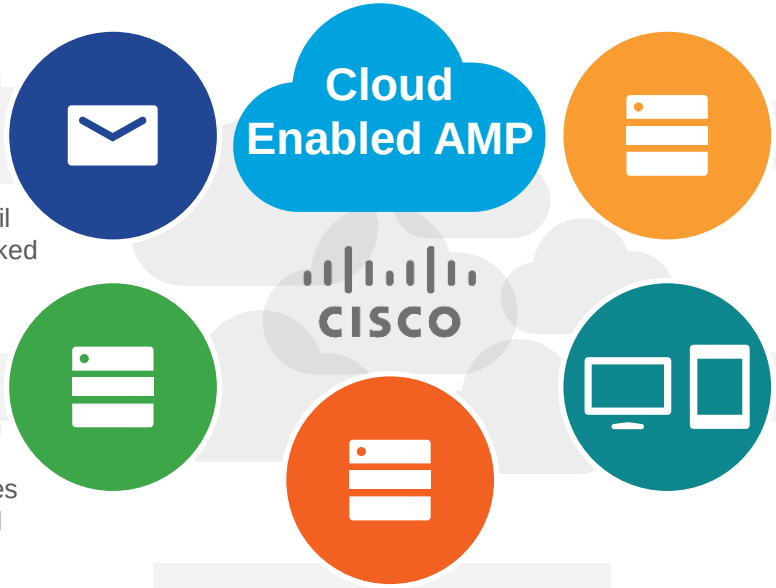
Privacy by Design

Security by Design

Incident Management

Integrated Threat Defense

13 iPOP's Globally



AMP'd Web and Email
100%**

1% of all WSA transactions blocked

80 WSAs/ 30 ESA Deployed

3K+ email files blocked by AMP monthly

AMP for Networks
50%**

Passive and Inline capabilities

25K+ quarterly alerts

NG-IPS 83xx and VM series deployed

Threat Grid/AMP
100%**

On-Prem Sandboxing

10K+ files analyzed every 24hrs.

14 TG appliances Deployed

AMP for Endpoints
10%**

Machine Learning Engine

10K+ agents deployed

Analytics Engine

FireSIGHT Management Center
100%**

Eight Global Appliances Deployed

****Deployment Progress Completion**

Playbook Defense

Enabling Active Response to Threats

Playbook Defense
Enabling Active Response to Threats

What are we trying to protect?	What are the threats?	How do we detect them?	How do we respond?
Collect/Analyze Cisco.com **1.2T** events throughout network **47TB** traffic inspected Active Directory Servers **28B** NetFlows analyzed/day **7.6B** DNS records **4TB** data collected and analyzed End User Laptop **~200** Plays	DoS attack SQL Injection Directory Traversal Information Sharing	NetFlow monitoring IPS/IDS detection System Logs	Engage ISP Investigate
	Lateral Movement Account Compromise Malware Network Services	NetFlow alerts User Activity HIPS logs Playbook	P1 incident Investigate Mitigate Remediate
	Malware Phishing Attacks Driveby Download Detection Tools	HIPS/AV logs ESA logs WSA logs	Reimage Investigate

Key Takeaways – Drivers Minimizing Risk

Make Security a Business Priority
Leadership must own, evangelize, invest in security.

Measure Operational Discipline
Review security practices, control access points, patch.

Test Security Effectiveness
Validate, improve security practices.

Adopt Integrated Defense Approach
Implement architectural approach to security, automate processes to reduce time to react to, stop attacks.

Attack Preparedness Plan

Source: Cisco Annual Security Report, January 2017


Cisco 2017
Annual Cybersecurity Report
Download the Cisco 2017 Annual Cybersecurity Report
www.cisco.com/go/acr2017

Thank You