Cisco Customer Education

Malware, Malware Everywhere – Battle 21st Century Security Threats with Cisco

This session was recorded via Cisco WebEx! You can watch the live session recording via the following URL:

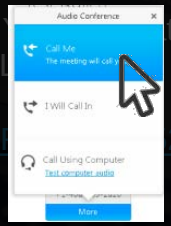
https://acecloud.webex.com/acecloud/lsr.php?RCID=9179b646be6a4f03a3480b1a1db8d72b

Cisco Customer Education

Malware, Malware Everywhere – Battle 21st Century Security Threats with Cisco

Connect using the audio conference box or you can call into the meeting:

1. Toll-Free: (866) 432-9903
2. Enter Meeting ID: 201 146 961
3. Press “1” to join the conference.



Presentation Agenda

- Welcome from Cisco
- Security in the 21st Century
- Talos and Advanced Malware Protection
- Next Generation Threat Protection
- Mid-Year Security Report
- Conclusion

About Your Host

Brian Avery

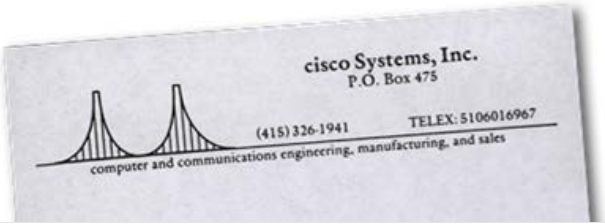
Territory Business Manager
Cisco Systems, Inc.

bravery@cisco.com

Priors:
Cisco Sales and Channels (11 yrs)
President and CEO (6 yrs) - Cisco Premier Partner
Director of Sales (2 yrs) - Cisco Silver Partner
Financial Analyst (7 yrs) - Sprint Corporation

Who Is Cisco?

1984



Computer scientists,
Len Bosack and Sandy Lerner
found Cisco Systems

Bosack and Lerner run network cables between two different buildings on the Stanford University campus

A technology has to be invented to deal with disparate local area protocols;
the multi-protocol router is born

Leading for Nearly 30 Years

Internet of Everything

1990 – 1995	1996 – 2000	2001 – 2007	2008 – Today	2016
WellFleet	Bay Networks	Siemens	Juniper	The Landscape is Constantly Changing
Proteon	ACC	Alcatel	HP	
	Ascend	Extreme	Microsoft	
SynOptics	3Com	Ericsson	Checkpoint	
	Newbridge	Nortel	Arista	
3Com	DEC	Foundry	Aruba	
	Fore	Riverstone	Riverbed	
IBM	Cabletron	NEC	Avaya	
	Xylan	Lucent	ShoreTel	
		Juniper	Dell	
		Redback	F5	
			Huawei	
			Fortinet	
			Brocade	
			Polycom	

Who Is Cisco?

- Dow Jones Industrial Average
  Fortune 100 Company (AAPL, CSCO, INTC, MSFT)
- $117B Market Capitalization
- $49.6B in Revenue
- $10B in Annual Net Profits
- $34B More Cash than Debt
- $6.3B in Research and Development

http://finance.yahoo.com/q/ks?s=CSCO+Key+Statistics

Chuck Robbins,
CEO, Cisco

Market Leadership Matters

No. 1
Routing
Edge/Core/
Access
47%

No. 1
TelePresence
50%

No. 1
Wireless LAN
50%

No. 1
Switching
Modular/Fixed
65%

No. 1
Voice
41%

No. 1
Web Conferencing
43%

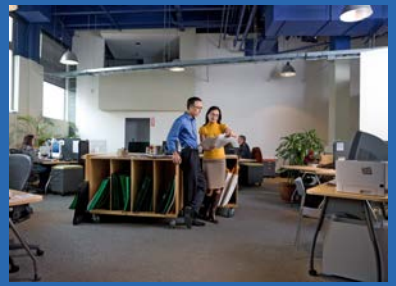
No. 2
x86 Blade Servers
29%

No. 1
Storage Area Networks
47%

No. 1
Security
31%

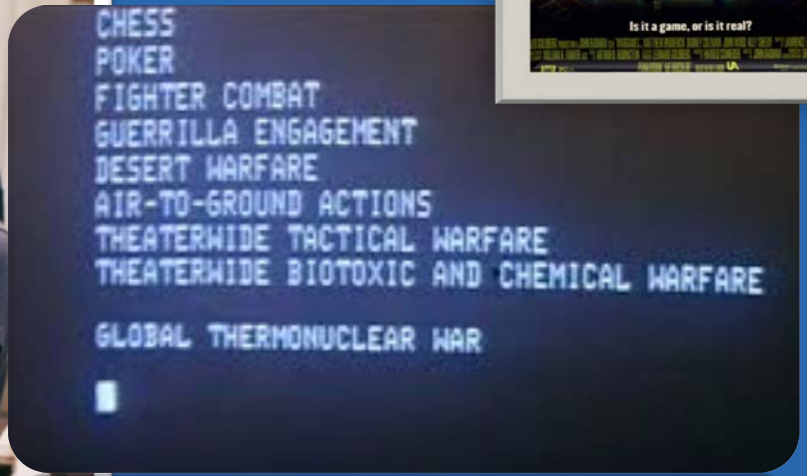
What Is the Cisco Customer Education Series?

- CCE is an educational session for current and prospective Cisco customers
- Designed to help you understand the capabilities and business benefits of Cisco technologies
- Allow you to interact directly with Cisco subject matter experts and ask questions
- Offer assistance if you need/want more information, demonstrations, etc.




Security in the 21st Century

Remember This Movie?



http://www.imdb.com/title/tt0086567/

It's All About The Money

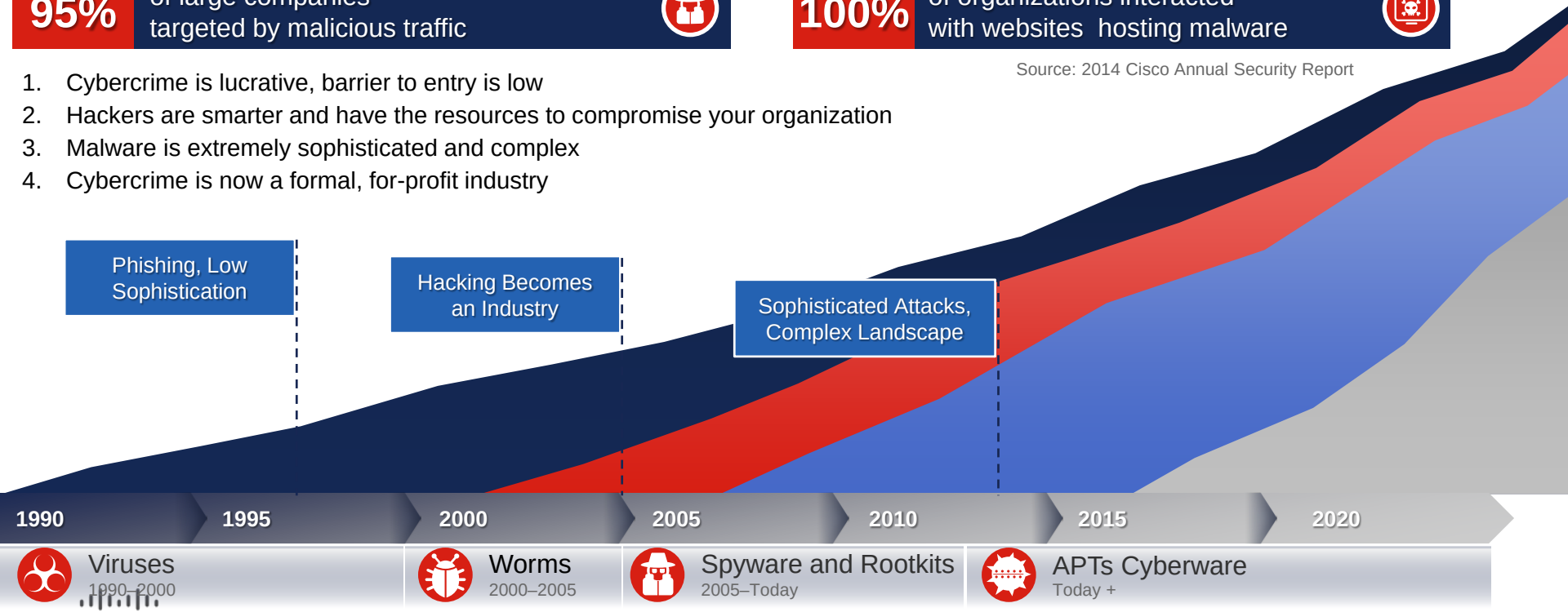
Industrial Hackers Are Making Big Money with Innovative Tactics

95% of large companies targeted by malicious traffic

100% of organizations interacted with websites hosting malware

Source: 2014 Cisco Annual Security Report

1. Cybercrime is lucrative, barrier to entry is low
2. Hackers are smarter and have the resources to compromise your organization
3. Malware is extremely sophisticated and complex
4. Cybercrime is now a formal, for-profit industry



High Profile Breaches

CHASE 1,000,000

THE HOME DEPOT 56,000,000

TARGET 70,000,000

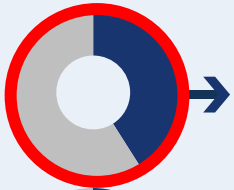
Michaels Where Creativity Happens 2,600,000

Neiman Marcus 1,100,000

STAPLES 1,160,000

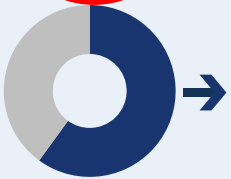
And Yet…

Organizations of every size are targets



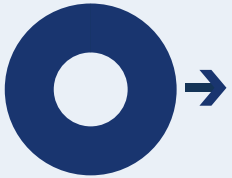
41% of targeted attacks are against organizations with fewer than 500 employees

(*July 2014 The National Cyber Security Alliance (NCSA)*



60% of UK small businesses were compromised in 2014

(2014 Information Security Breaches Survey)

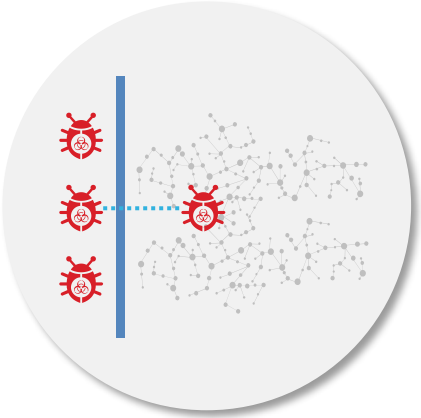


100% of corporate networks examined had malicious traffic

(Cisco 2014 Annual Security Report)

As of 12/31/2014 http://www.idtheftcenter.org/images/breach/DataBreachReports_2014.pdf

Today’s cyber-threat reality



Your environment will get breached – it’s not an “IF” it’s a “WHEN”

Why? Because you’ll never be able to prevent 100% of attacks.

If you know you are going to be compromised, how should you do security differently?

The Attack Surface

Attack surface – web browsers

More than

85%

of the companies studied were affected each month by malicious browser extensions

Attack surface – user error on web

Users becoming complicit enablers of attacks

Untrustworthy sources

Clickfraud and Adware

Outdated browsers

10% vs **64%**

IE requests running latest version

Chrome requests running latest version

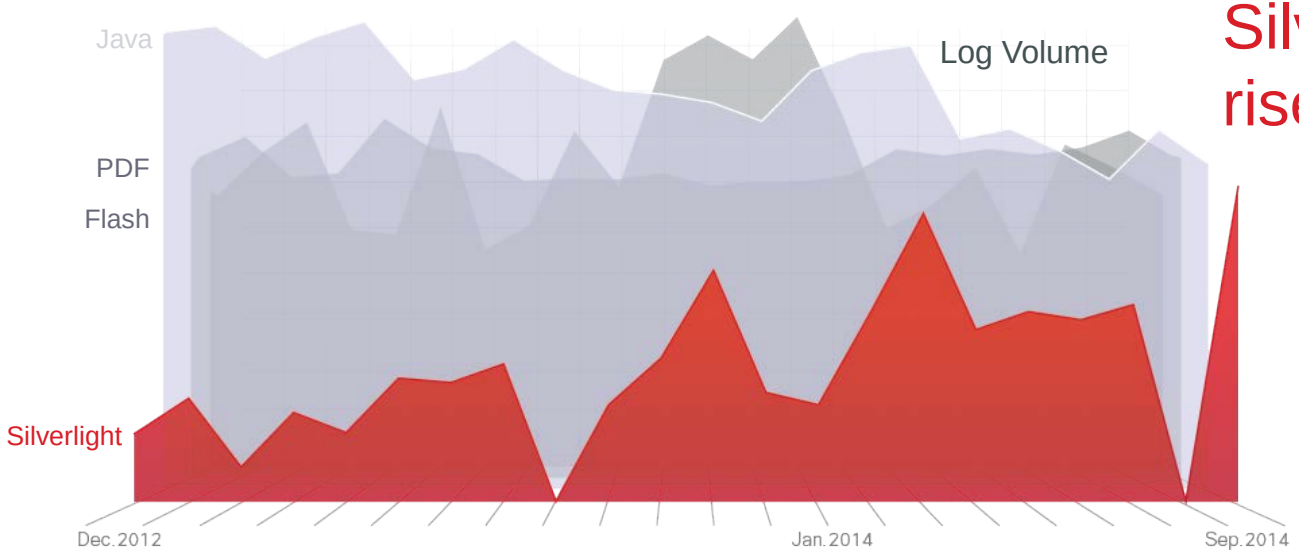
Attack surface – web applications

Attackers:

Shifts in the attack vectors

PDF and Flash steady

Java drop 34%



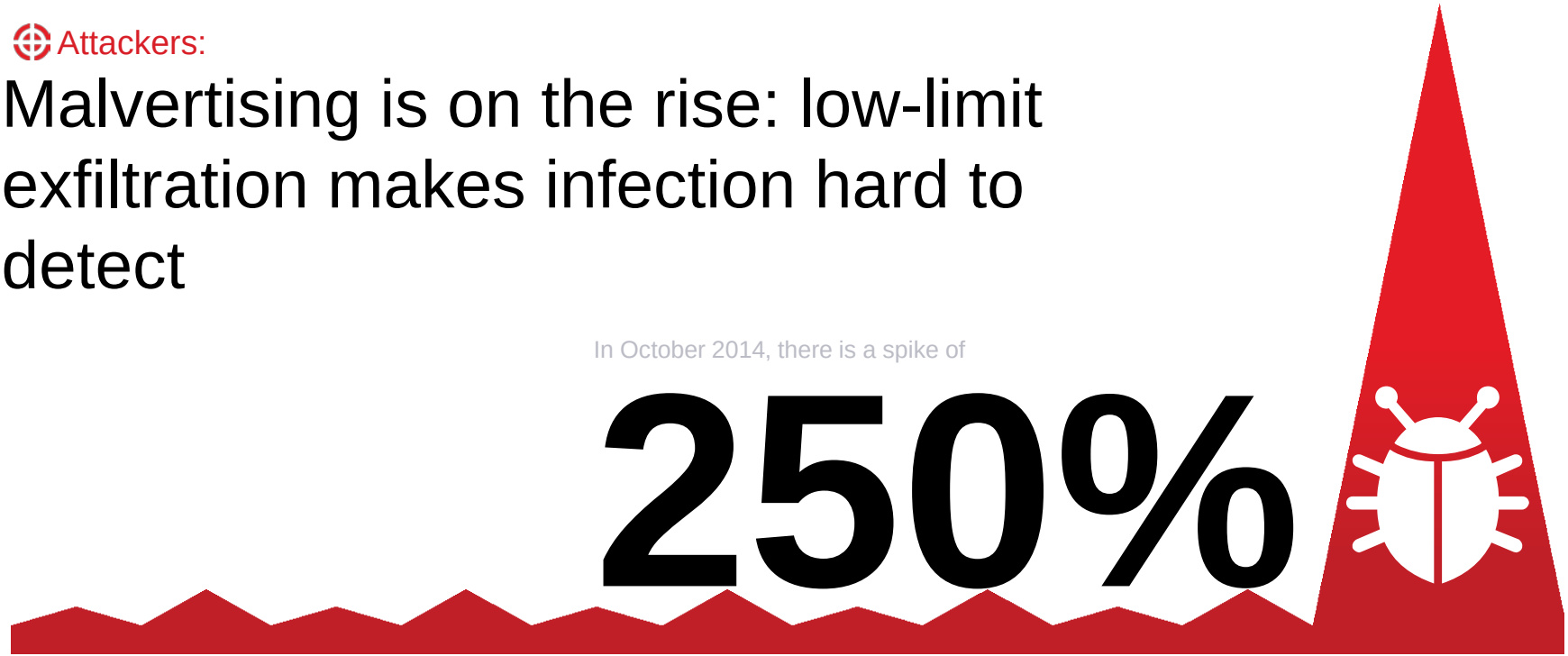
Silverlight rise 228%

2015 Cisco Annual Security Report

Compromising without clicking

Attackers:

Malvertising is on the rise: low-limit exfiltration makes infection hard to detect



Ransomware and Exploit Kits, e.g. Cryptowall version 4

Encryption technique allows per-target customization

Using Bitcoin for anonymous payment

Marking systems and files have already been encrypted

Dual deadlines for:
1.Cost increase
2.Deleting data

Phishing and Social Engineering

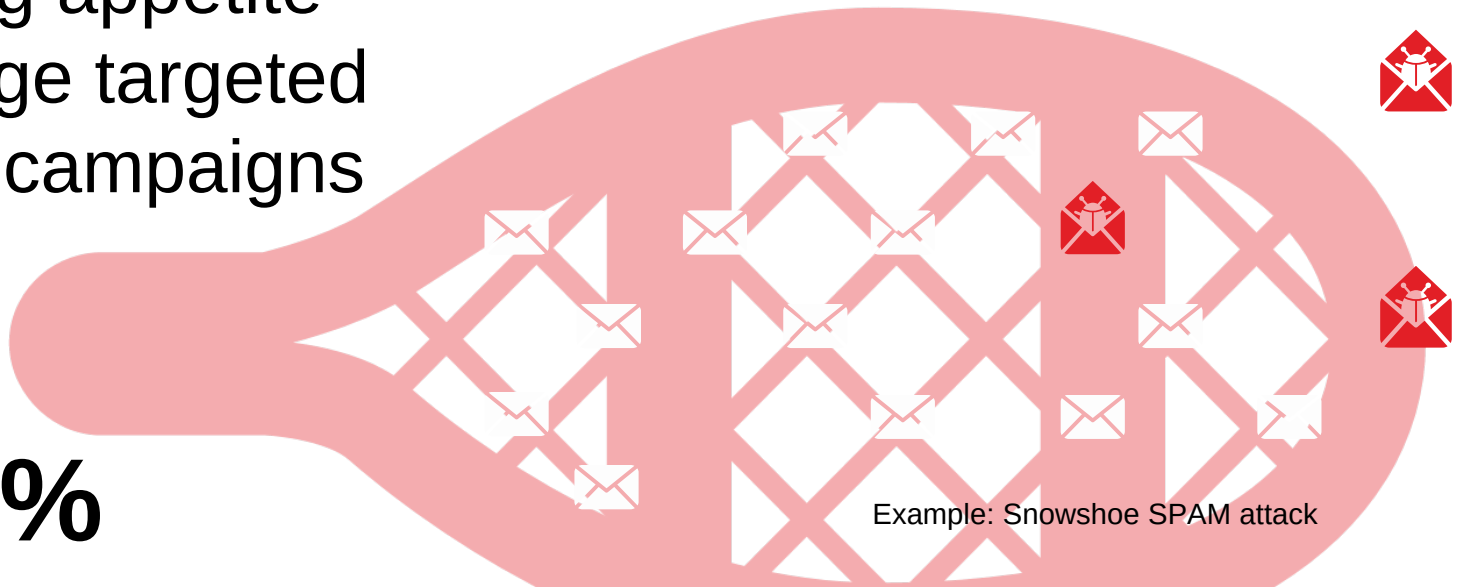
Attack surface - email

Attackers:

A growing appetite to leverage targeted phishing campaigns

SPAM up

250%



Example: Snowshoe SPAM attack

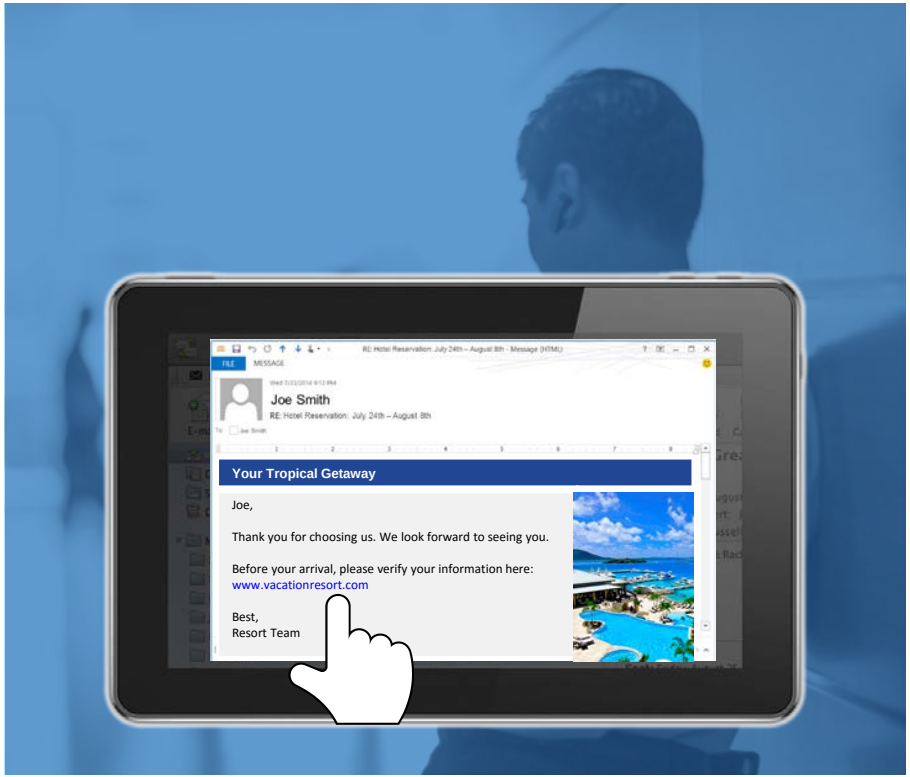
Social Engineering

Meet Brian, an employee at Sysco (not Cisco).

He is catching up on life using the public Wi-Fi at Starbucks prior to a meeting.

Brian decides to check on Facebook where his Mom had posted pictures of her vacation.

Social Engineering



Brian then gets an email from his mom.

The email says she's having a great vacation and took a video she wants him to see. In the email is a link to what looks to be a normal video link.

No problem, right? Everything looks normal. After all, his mom IS on vacation.

And the video site has an https: so it looks trustworthy, so he clicks the link.

Social Engineering

Brian opens the link and a video of the resort plays.

Although he doesn't know it, Brian's device has been compromised by a Silverlight based video exploit.

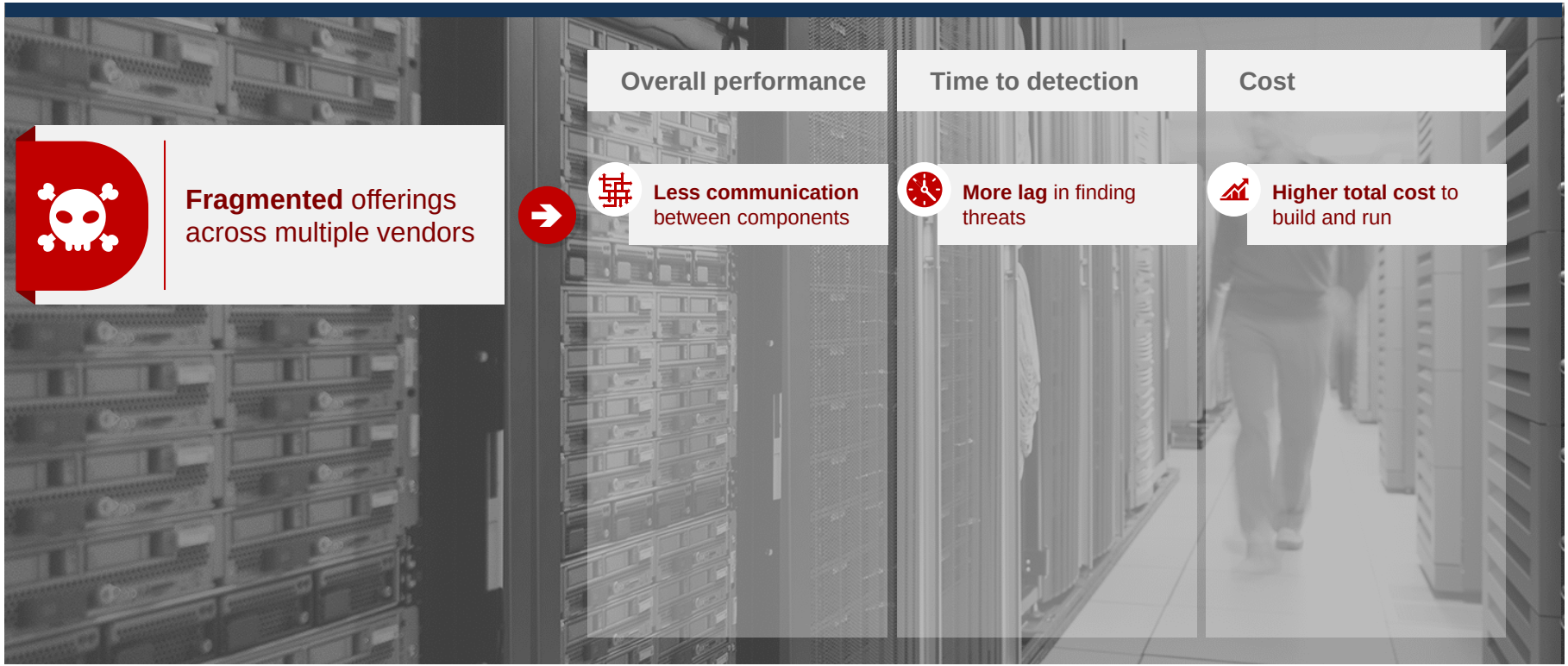
The malware now starts to harvest Brian's confidential information:

- Passwords
- Credentials
- Company access authorizations

Why did the cybercriminal target Brian?

Cisco Security Overview

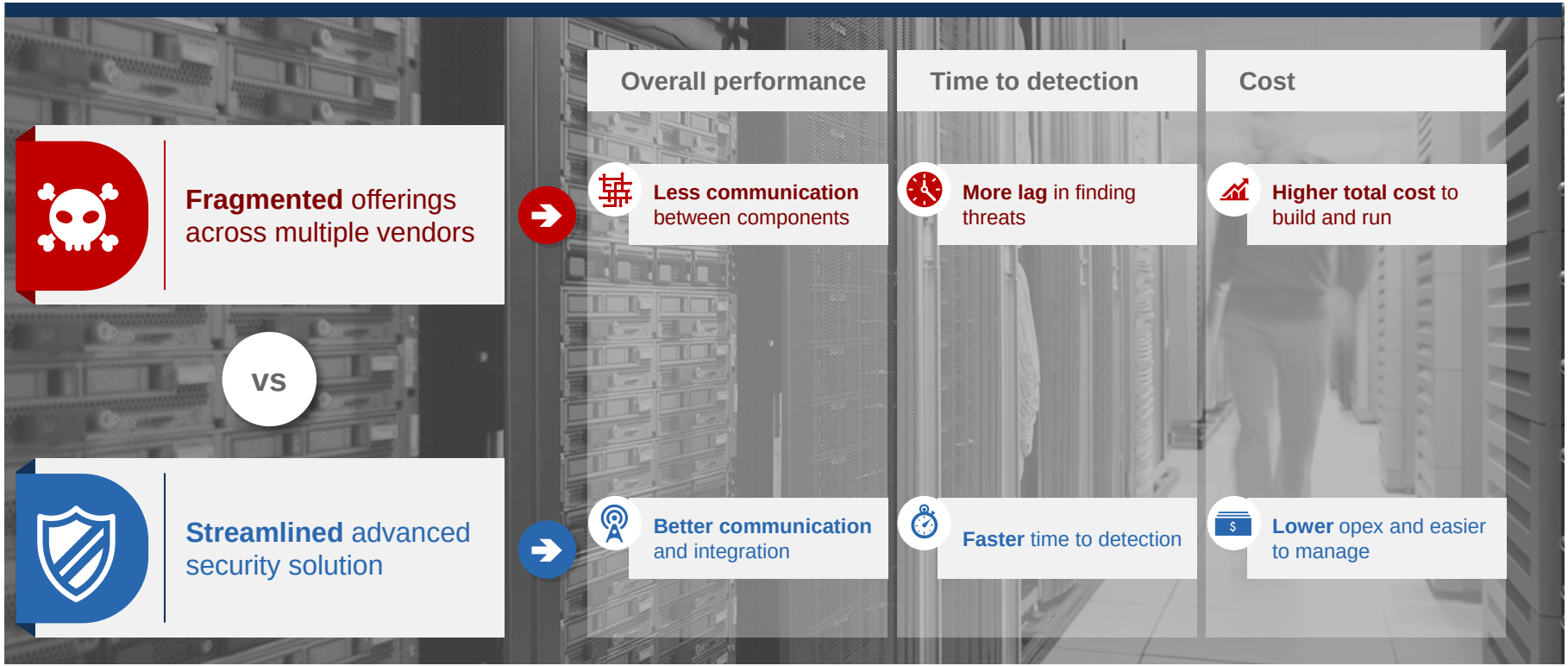
Too Many Disparate Security Products Mean Gaps in Protection



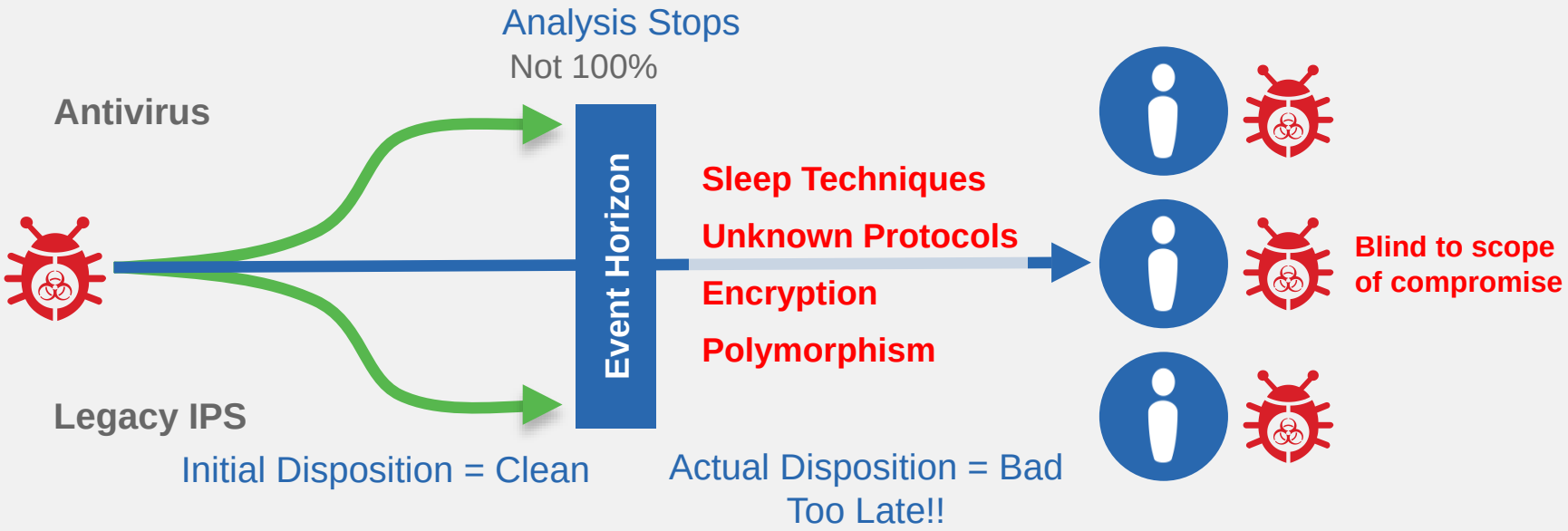
Fragmented offerings across multiple vendors

Overall performance	Time to detection	Cost
Less communication between components	**More lag** in finding threats	**Higher total cost** to build and run

Too Many Disparate Security Products Mean Gaps in Protection



Point-in-Time Detection Tools Alone Are Insufficient and Provide Limited or No Visibility Into Threats Once They Get in




I'm going for fearsome here, but I just don't feel it!
I'm think I'm just coming off as annoying.
Competitors
JURASSIC PARK

What's Needed to Protect Against Advanced Threats That Manage to Slip by Your Front-Line Defenses?

Deep Visibility

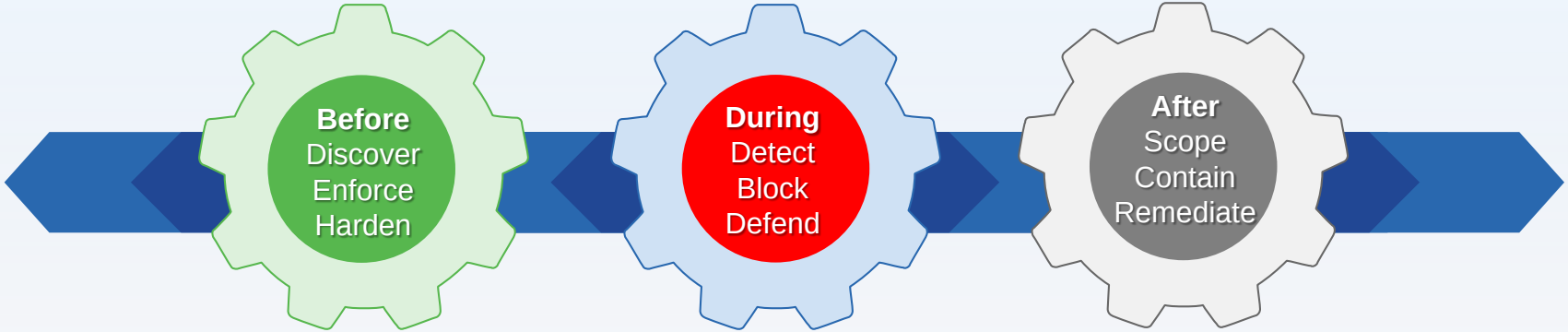
+

Control

Defending Against These Advanced Threats

Requires Greater Visibility and Control Across the Full Attack Continuum

Attack Continuum



Threat intelligence and analytics

Point-in-Time detection

Retrospective security and continuous analysis

Email and Web

Data Center/Servers

Network

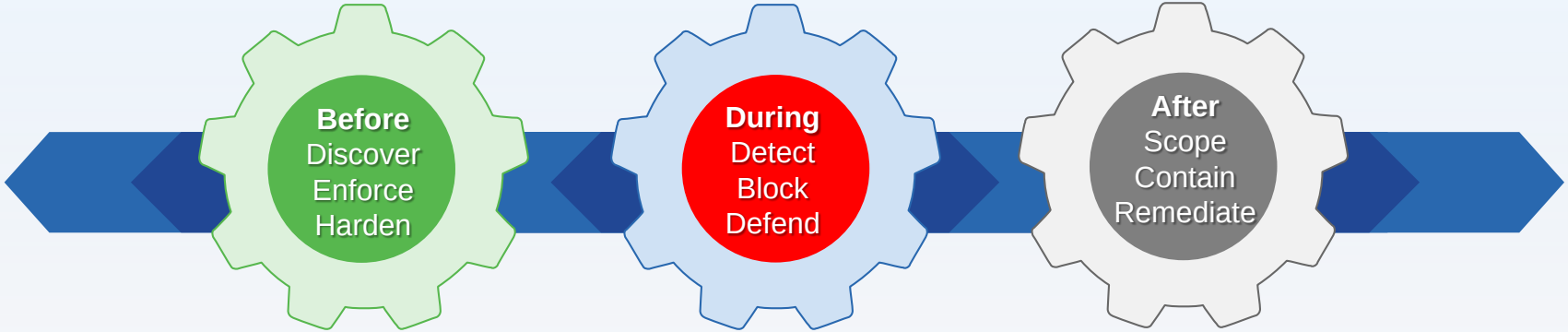
Endpoints

Mobile

Defending Against These Advanced Threats

Requires Greater Visibility and Control Across the Full Attack Continuum

Attack Continuum



ASA	VPN	NGIPS	Advanced Malware Protection
OpenDNS	Meraki	ESA/WSA	Network as Enforcer
Secure Access + Identity Services		CWS	ThreatGRID

FireSIGHT and pxGrid

AMP

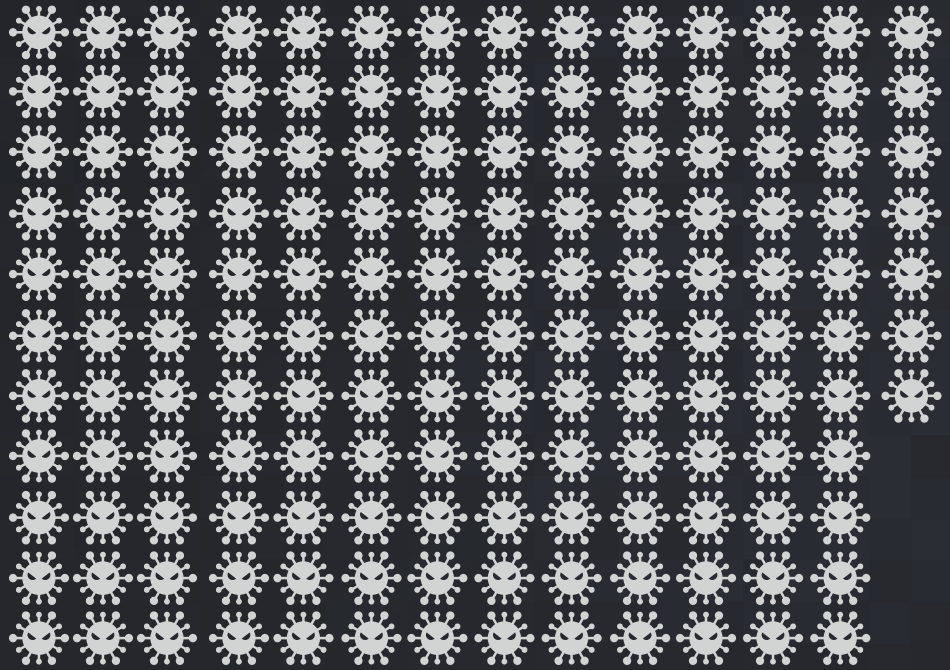
Cisco Advanced Malware Protection

Cisco Advanced Malware Protection

Software-as-a-Service
Cloud Managed
Subscription Based


TALOS

THREAT LANDSCAPE



= 10,000

1.5 Million

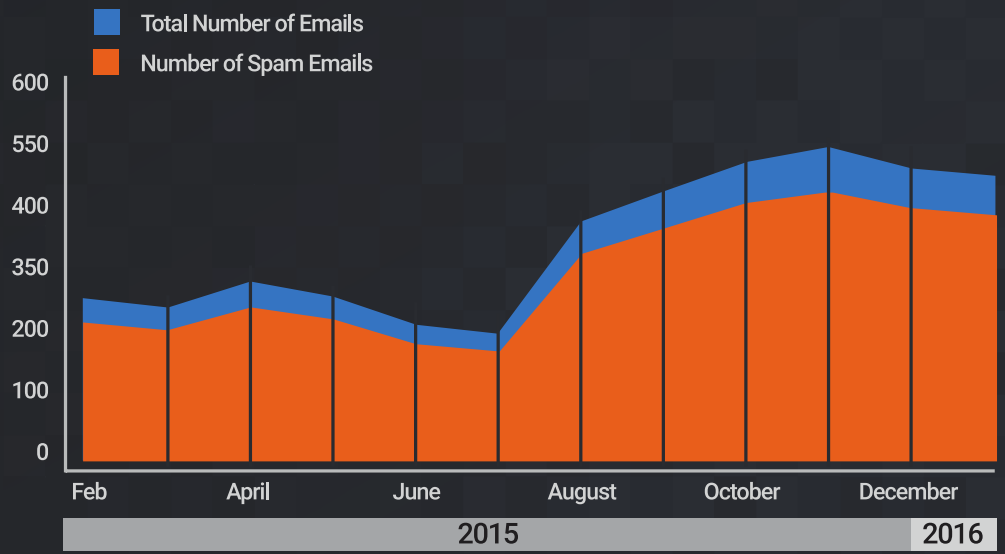
Malware Samples

DAILY

TALOS

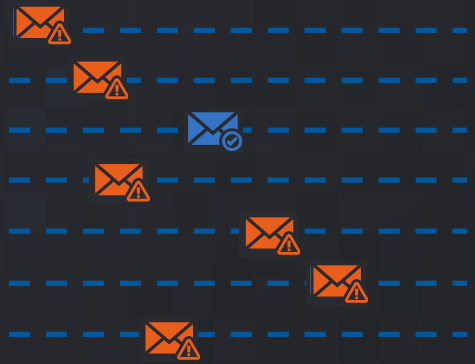
THREAT LANDSCAPE

Talos Billions of Emails Daily



SPAM MAKES UP

86% of ALL email traffic



TALOS

TALOS

Cloud to Core
Coverage

WEB

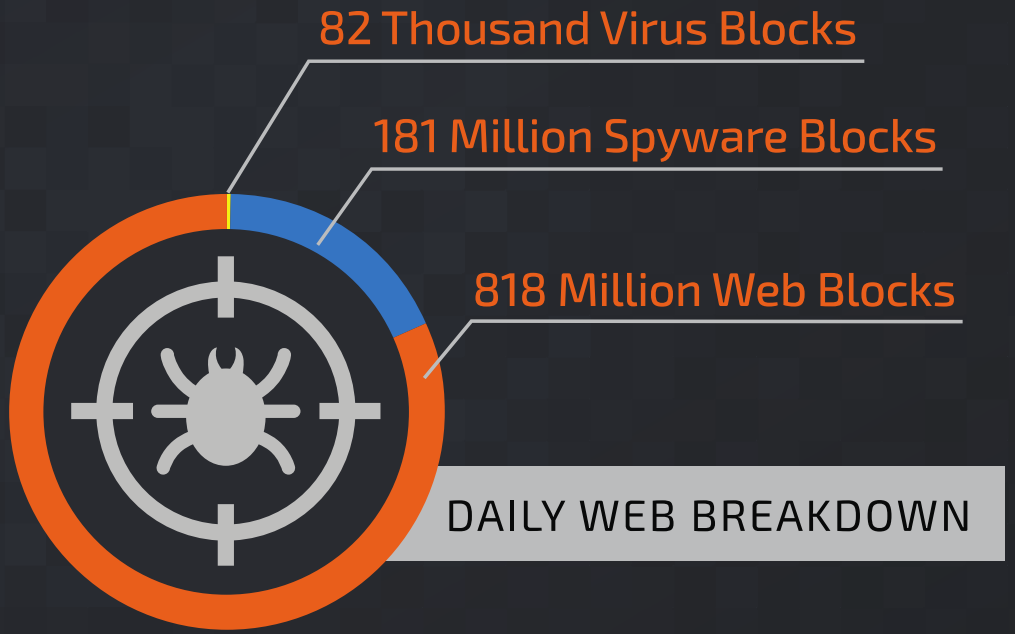
TALOS

THREAT LANDSCAPE

19.7 Billion
TOTAL THREAT BLOCKS
DAILY

=

7.2 Trillion
YEARLY



TALOS

Cisco Security Decreases Time to Detection

Current Industry Average (TTD)

100 days

- Source: 2016 Cisco Annual Security Report

Cisco Security Decreases Time to Detection

100 days to 13.8 hours

- Source: 2016 Cisco Annual Security Report

TALOS

Point in Time Protection

Point-in-Time Detection

AMP Delivers the First Line of Defense, Blocking Known and Emerging Threats with Point-in-Time Defenses

Automatically stop as many threats as possible, known and unknown

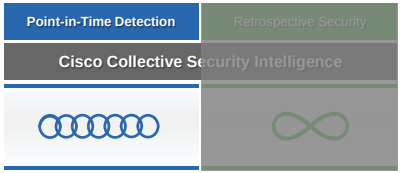
- One-to-one signature
- Fuzzy finger-printing
- Machine learning
- Advanced analytics
- Static and dynamic analysis (sandboxing)

Offer better accuracy and dispositioning

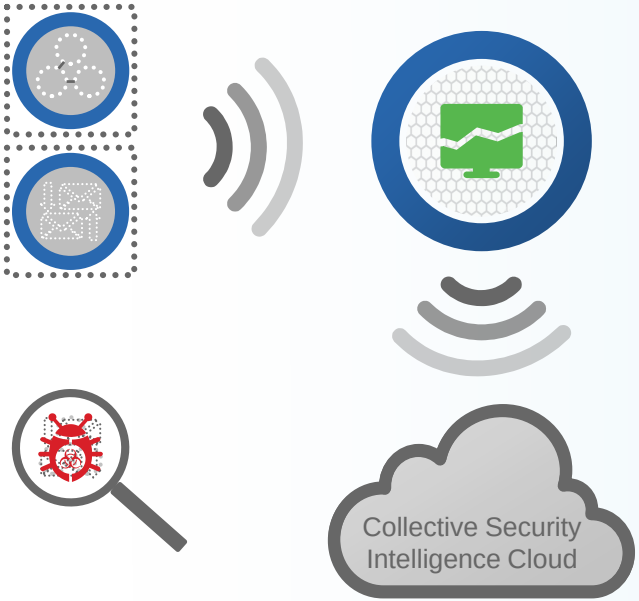
Block known and emerging threats

Protect your business with no lag

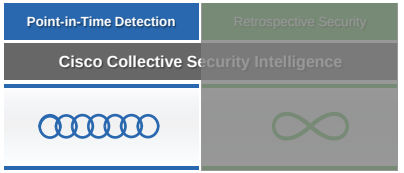
Behavioral Detection: Example



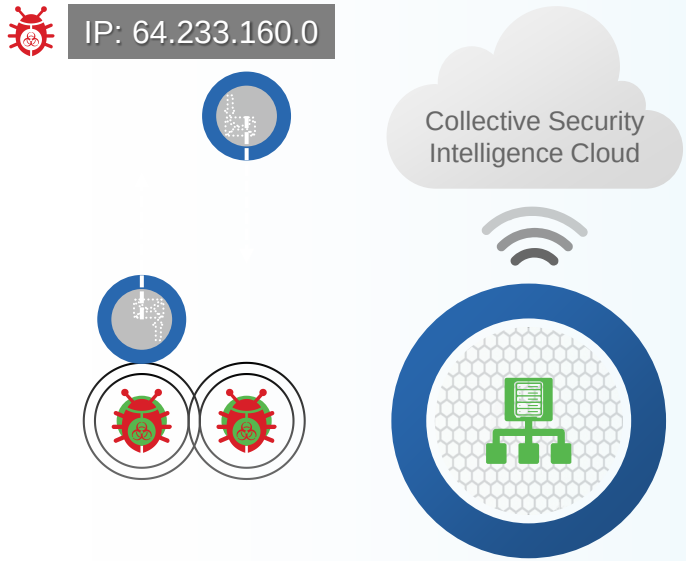
1. File of unknown disposition is encountered
2. File replicates itself and this information is communicated to the cloud
3. File communicates with malicious IP addresses or starts downloading files with known malware disposition
4. Combination of activities indicates a compromise and the behavior is reported to the cloud and AMP client
5. These indications are prioritized and reported to security team as possible compromise



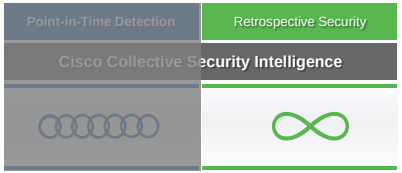
Behavioral Detection: Example



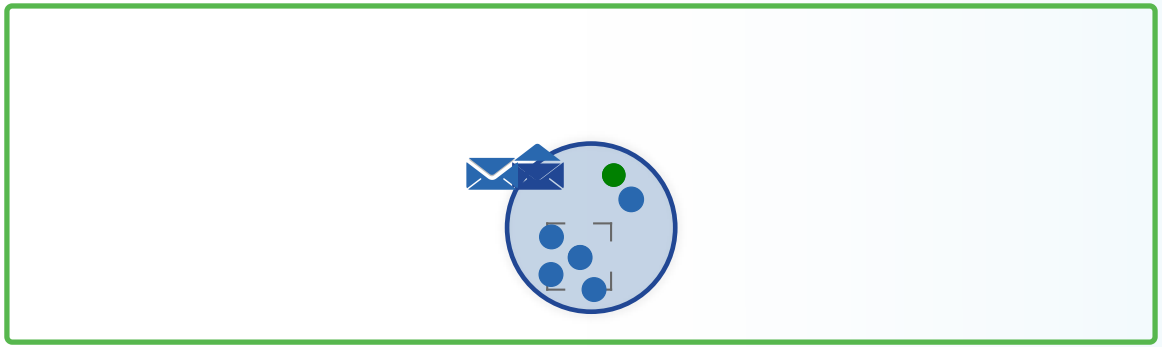
1. Device Flow Correlation monitors communications of a host on the network
2. Two unknown files are seen communicating with a particular IP address
3. One is sending information to the IP address, the other is receiving commands from the IP address
4. Collective Security Intelligence Cloud recognizes the external IP as a confirmed, malicious site
5. Unknown files are identified as malware because of the association



Behavioral Indications of Compromise: Example



Behavioral Indications of Compromise uses continuous analysis and retrospection to monitor systems for suspicious and unexplained activity… not just signatures!

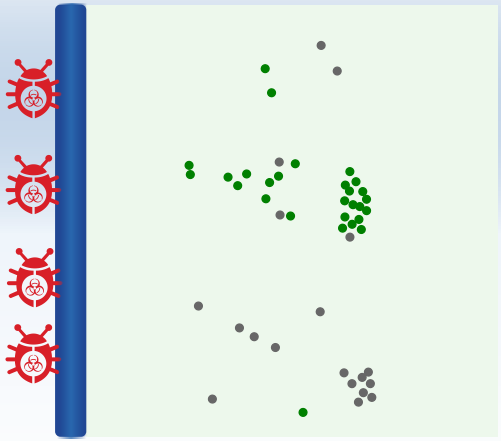


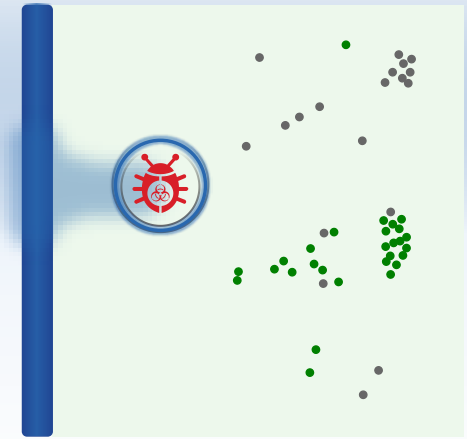
1. An unknown file is admitted into the network
2. The unknown file copies itself to multiple machines
3. Duplicates content from the hard drive
4. Sends duplicate content to an unknown IP address

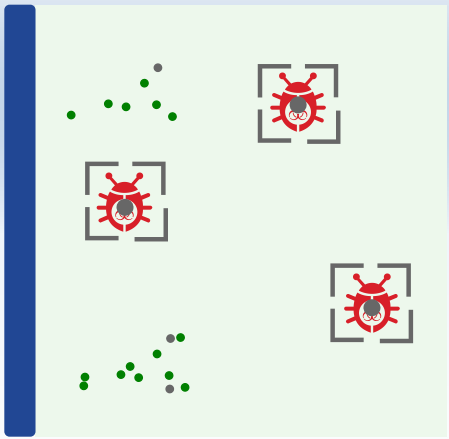
Using the power of Attack Chain Weaving, Cisco® AMP is able to recognize patterns and activities of a given file, and identify an action to look for across your environment rather than a file fingerprint or signature

How Malware Gets In to Your Network

Breach Prevention	Rapid Breach Detection, Response, Remediation	Threat Intelligence







But Point-in-Time Detection Alone Will Never Be 100% Effective

Continuous Analysis and Retrospective Security

Only AMP Continuously Monitors and Analyzes All File Activity, Regardless of Disposition

Across all control points


Email

Web


Network


Endpoints


Mobile

Take advantage of key capabilities


Identify a threat's point of origin


Track it's rate of progression and how it spread

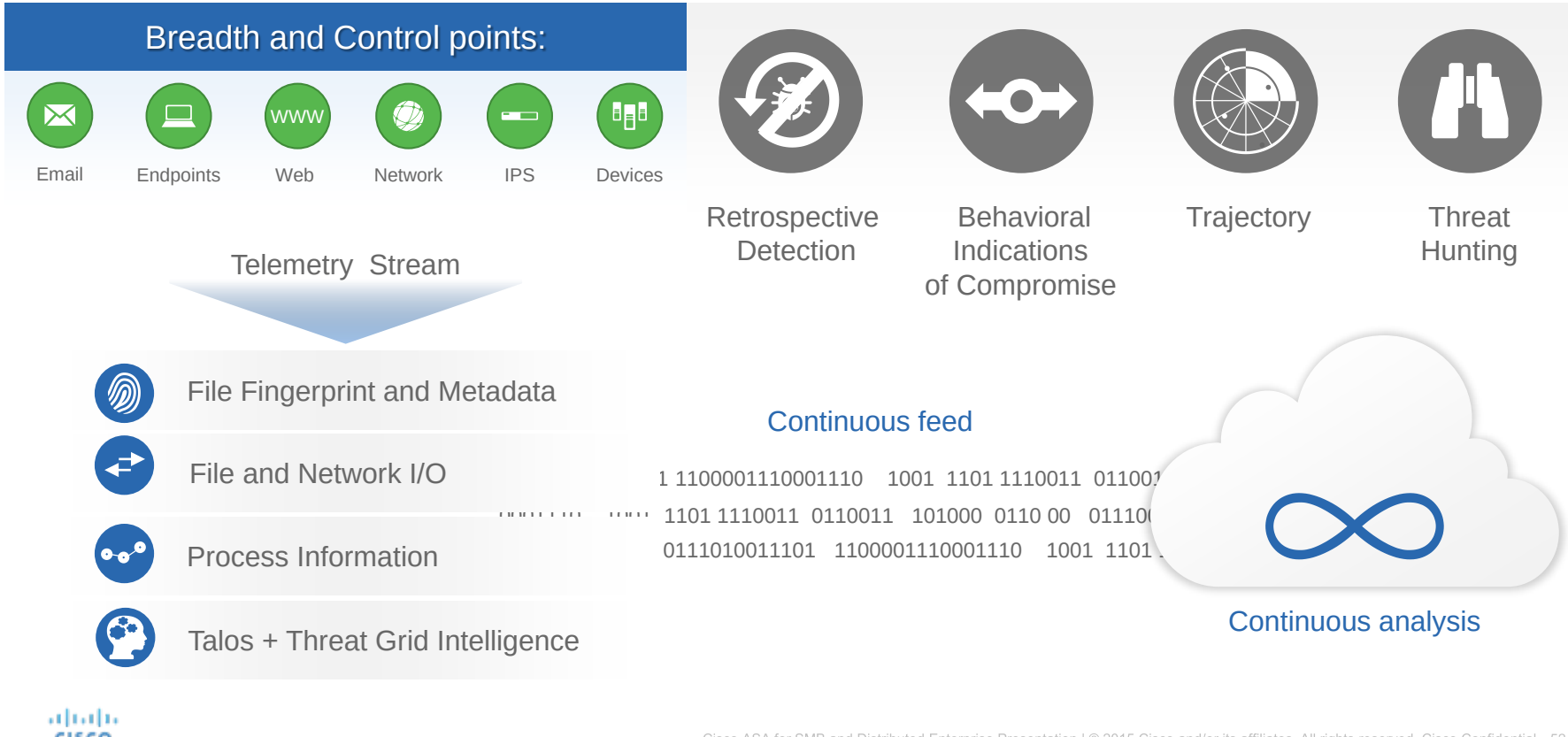

See where it's been


See what it is doing


Surgically target and remediate

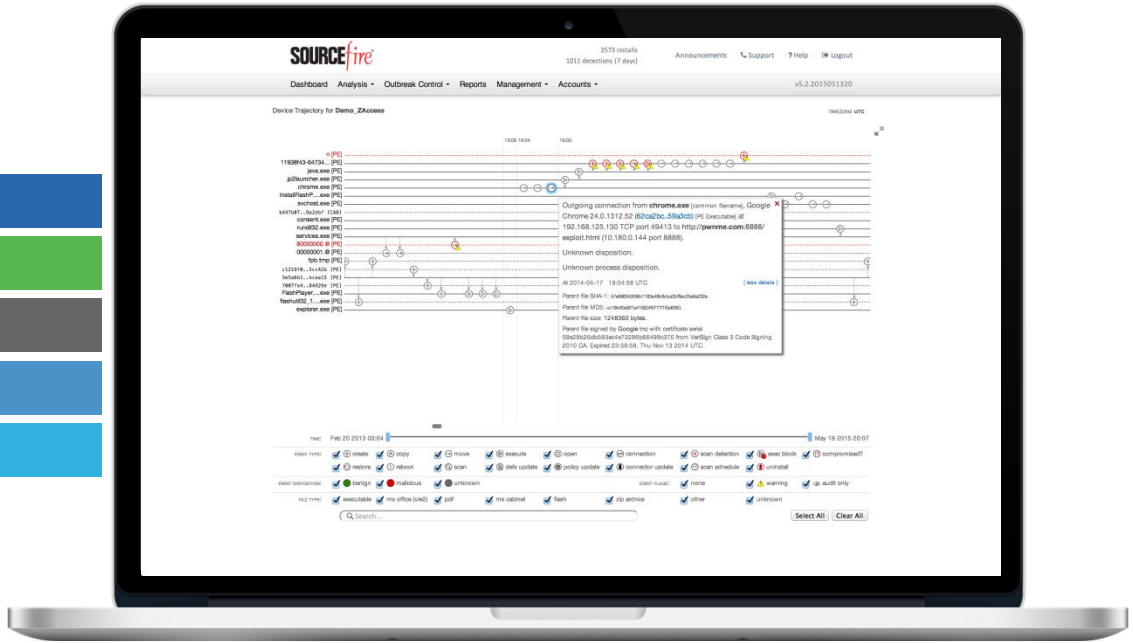
To answer the questions that matter…

Continuous Analysis and Retrospective Security



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

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



See AMP in Action!

See Where It Entered the System

What happened?

Where did the malware come from?

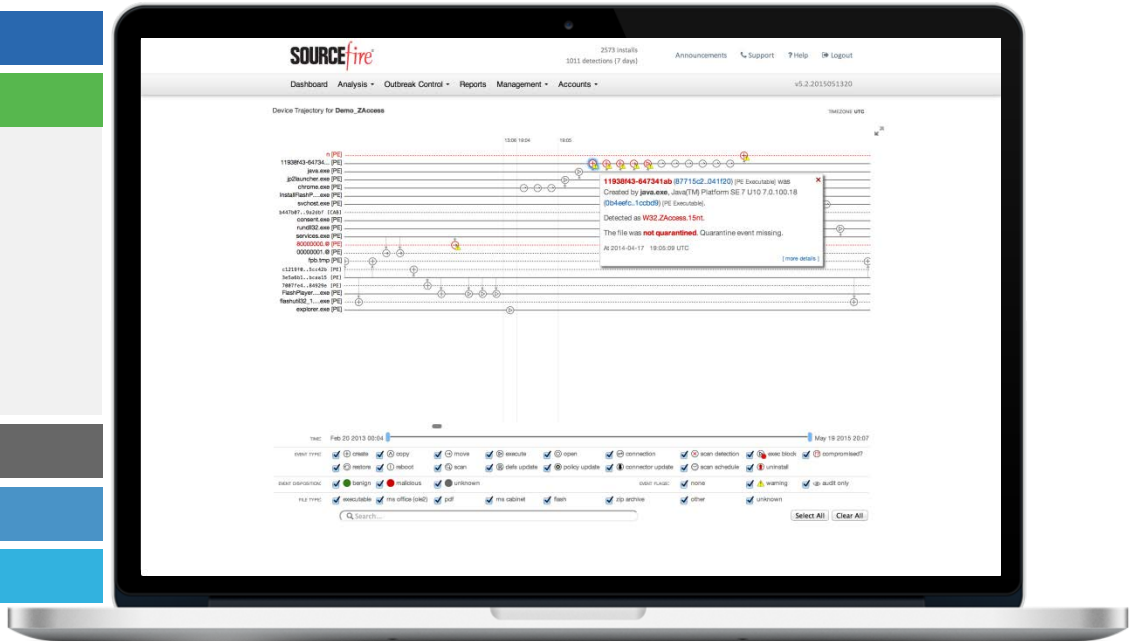
Track threat's origin and progression:

- How did it get into the system
- What is the point of origin
- What was the attack vector

Where has the malware been?

What is it doing?

How do we stop it?



See AMP in Action!

See Everywhere That It Has Been

What happened?

Where did the malware come from?

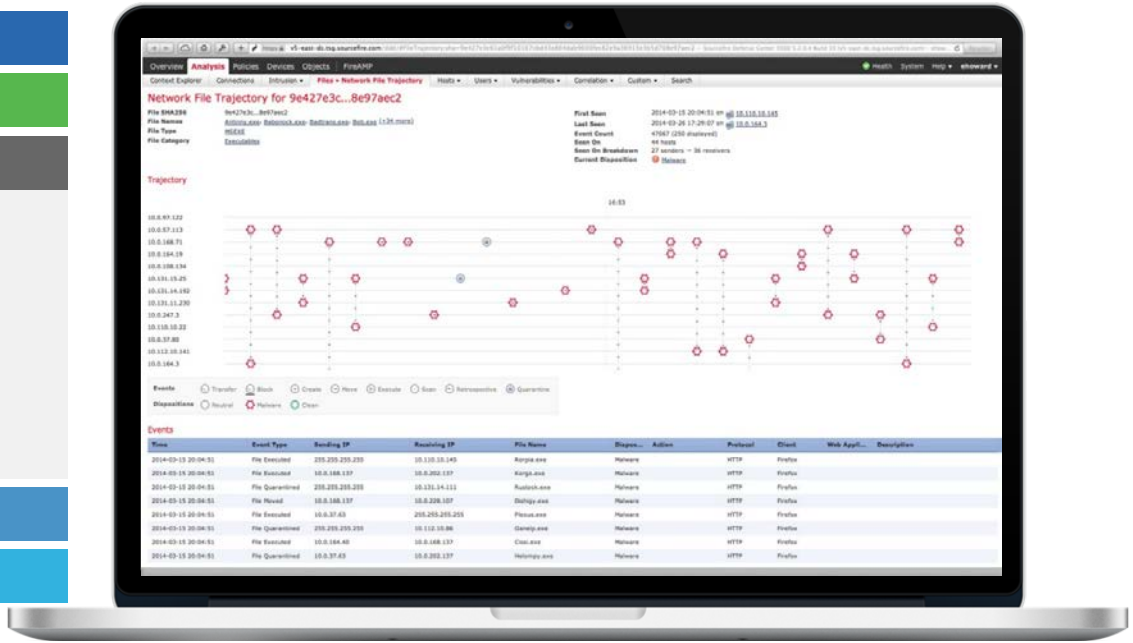
Where has the malware been?

Track infected areas in the system:

- Where is the attack now
- What other endpoints have seen it
- Where should I focus my response
- Where is still safe

What is it doing?

How do we stop it?



See AMP in Action!

Determine What the Malware Is Doing

What happened?

Where did the malware come from?

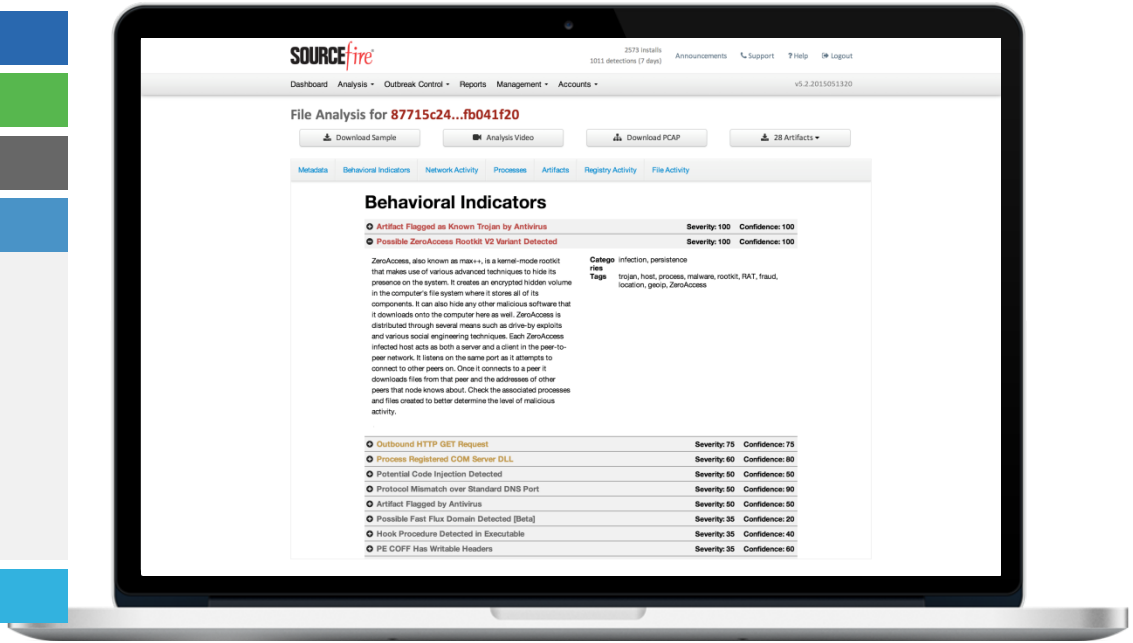
Where has the malware been?

What is it doing?

Understand the details of how the malware works:

- What is it trying to do, in plain English
- How does the malware behave
- Get detailed information vital for incident response

How do we stop it?



See AMP in Action!

Stop It with a Few Clicks

What happened?

Where did the malware come from?

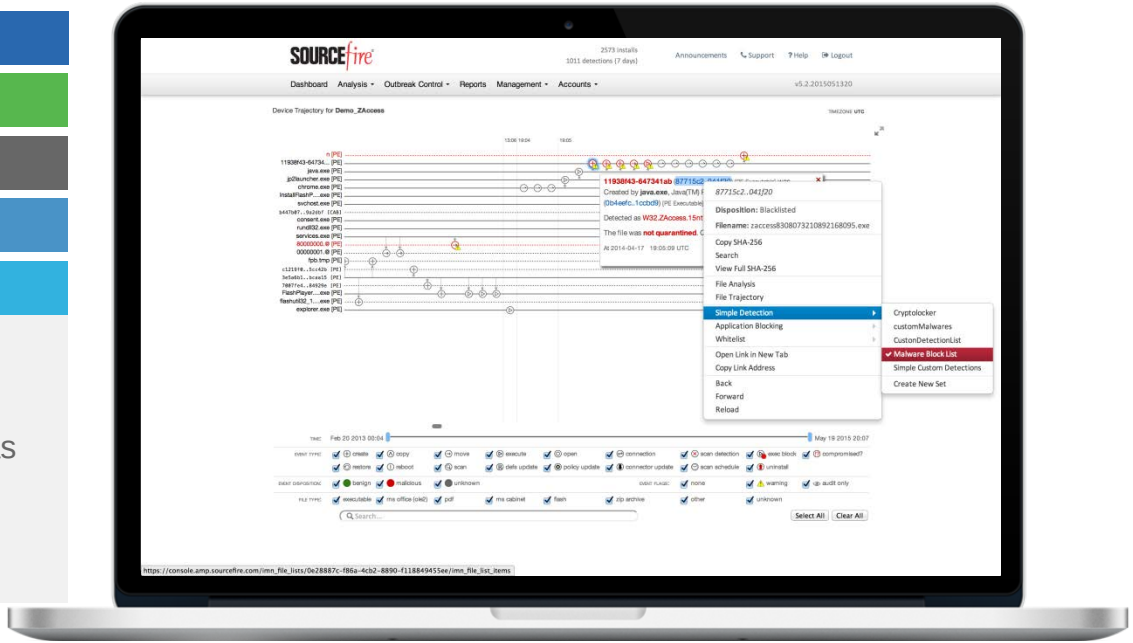
Where has the malware been?

What is it doing?

How do we stop it?

Knowing the details above, surgically remediate:

- Stop it at the source and all infected areas
- Simply right click, add to a blocklist, and remediate the malware from the entire system

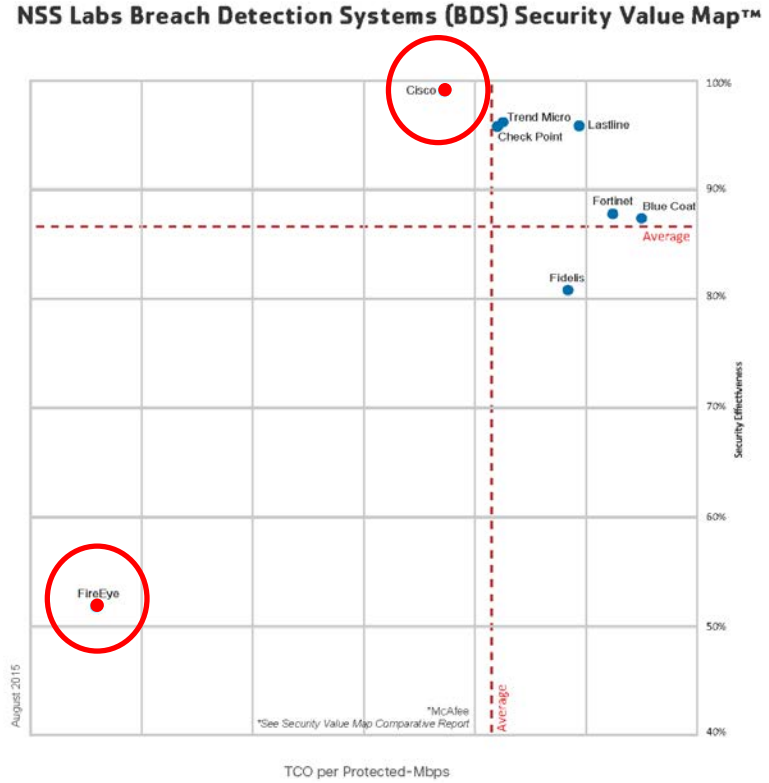


See AMP in Action!

The Leader in Security Effectiveness

Cisco AMP offers superior security effectiveness, excellent performance, and provides security across more attack vectors than any other vendor

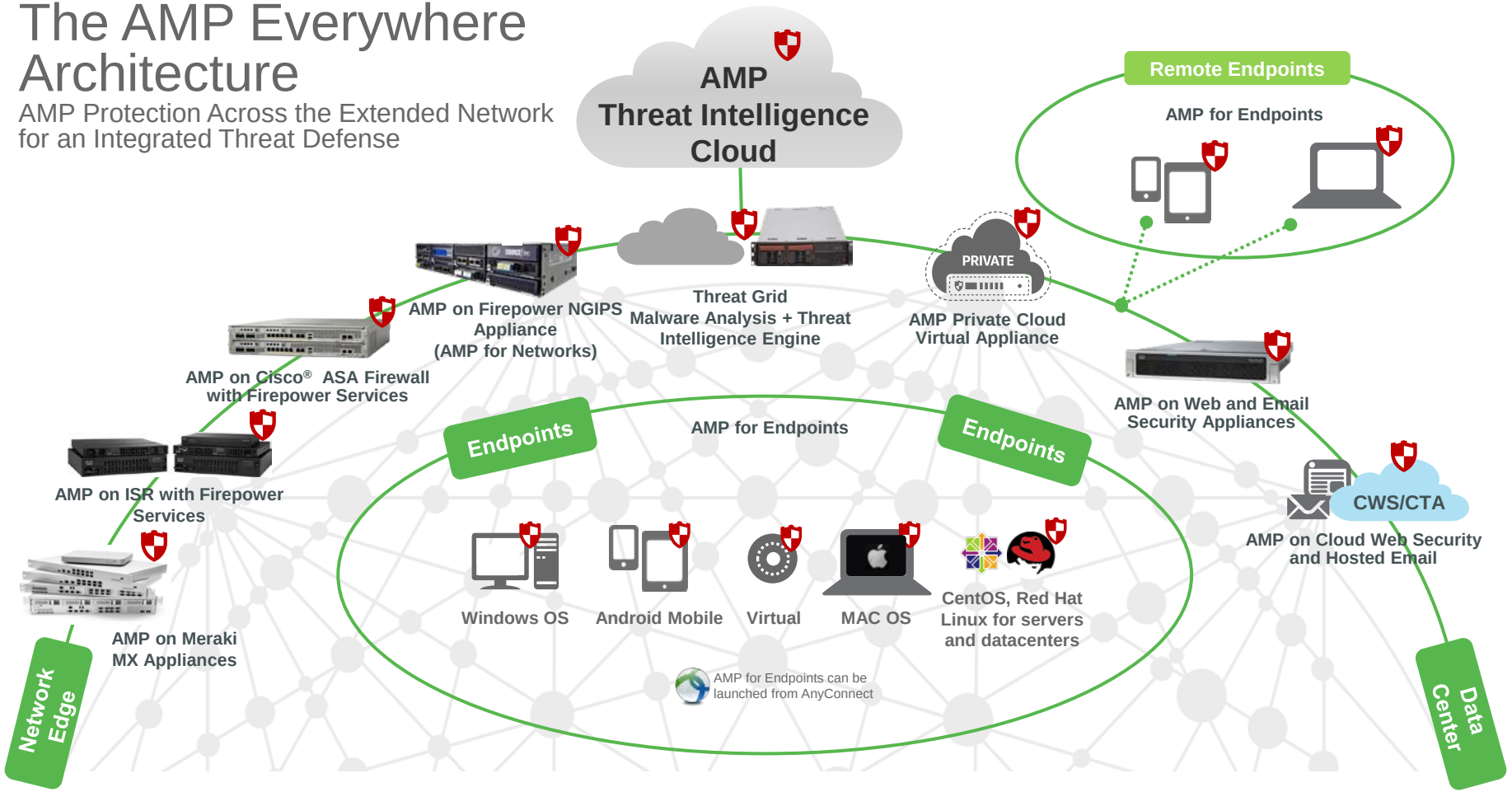
- **99.2%** Security Effectiveness rating in BDS testing, the highest of all vendors tested.
- Only vendor to block 100% of evasion techniques during testing.
- Excellent performance with minimal impact on network, endpoint, or application latency.
- Download the flysheet and full report here.



Next-Generation Security

The AMP Everywhere Architecture

AMP Protection Across the Extended Network for an Integrated Threat Defense



Introducing Cisco Adaptive Security Appliances

Industry's First Threat-Focused NGFW

Cisco ASA with FirePOWER Services Next-Generation Firewall (NGFW)

Proven Cisco ASA firewalling

+

Industry leading NGIPS and AMP

=

Cisco ASA with FirePOWER Services

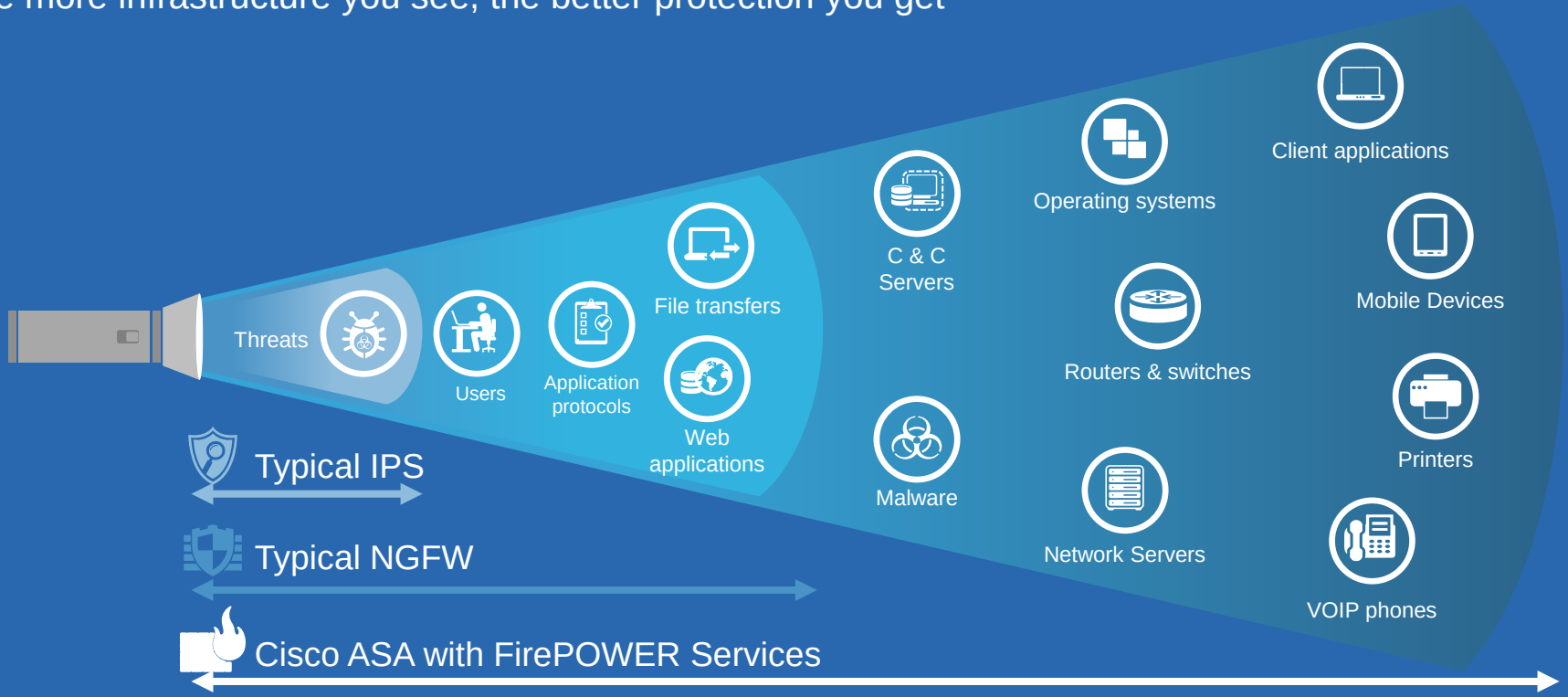
- *Integrating* defense layers helps organizations get the best visibility
- Enable dynamic controls to automatically adapt
- Protect against advanced threats across the entire attack continuum

Superior Integrated & Multilayered Protection

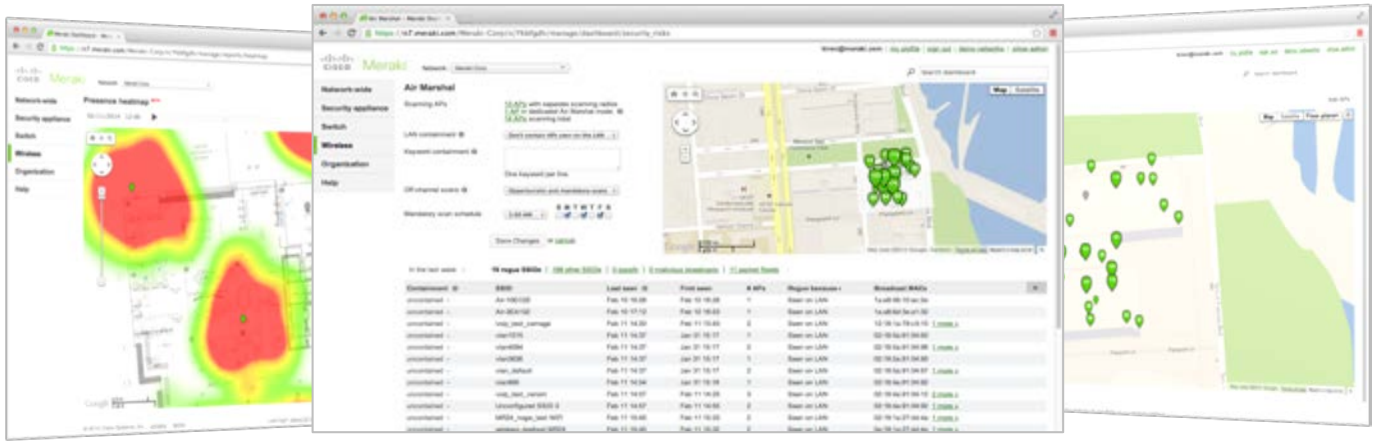
- World's most widely deployed, enterprise-class ASA stateful firewall
- Granular Cisco® Application Visibility and Control (AVC)
- Industry-leading FirePOWER next-generation IPS (NGIPS)
- Reputation- and category-based URL filtering
- Advanced malware protection

No other NGFW offers this level of visibility

The more infrastructure you see, the better protection you get



Cisco Meraki - Cloud Managed Networking



Meraki MR
Wireless LAN

Meraki MS
Ethernet Switches

Meraki MX
Security Appliances

Meraki SME
Enterprise Mobility Management

MC Communications

MX Security Appliance Features

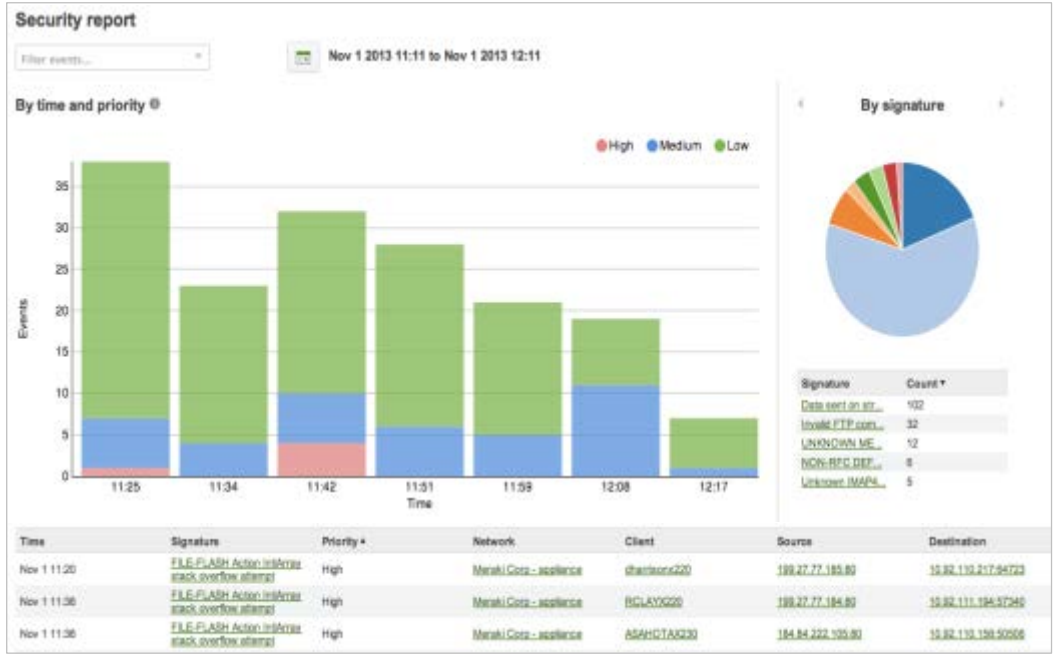
Security
NG Firewall, Client VPN,
Site to Site VPN, IDS/IPS

Networking
NAT/DHCP, 3G/4G Cellular,
Static Routing, Link Balancing

Application Control
Traffic Shaping, Content
Filtering, Web Caching

Ironclad security

Best IPS	SOURCEfire IDS / IPS, updated every day
Anti-Malware	Advanced Malware Protection powered by Cisco Sourcefire and Talos
Content Filtering	4+ billions URLS, updated in real-time
Geo-based security	Block attackers from rogue countries
AV / anti-phishing	Kaspersky AV, updated every hour
PCI compliance	PCI L1 certified cloud-based management



MX Security Appliance Features

Enterprise License

- Stateful firewall
- Site to site VPN
- Branch routing
- Internet load-balancing (over dual WAN)
- Application control
- Web caching
- Intelligent WAN (IWAN)
- Client VPN

Advanced Security License

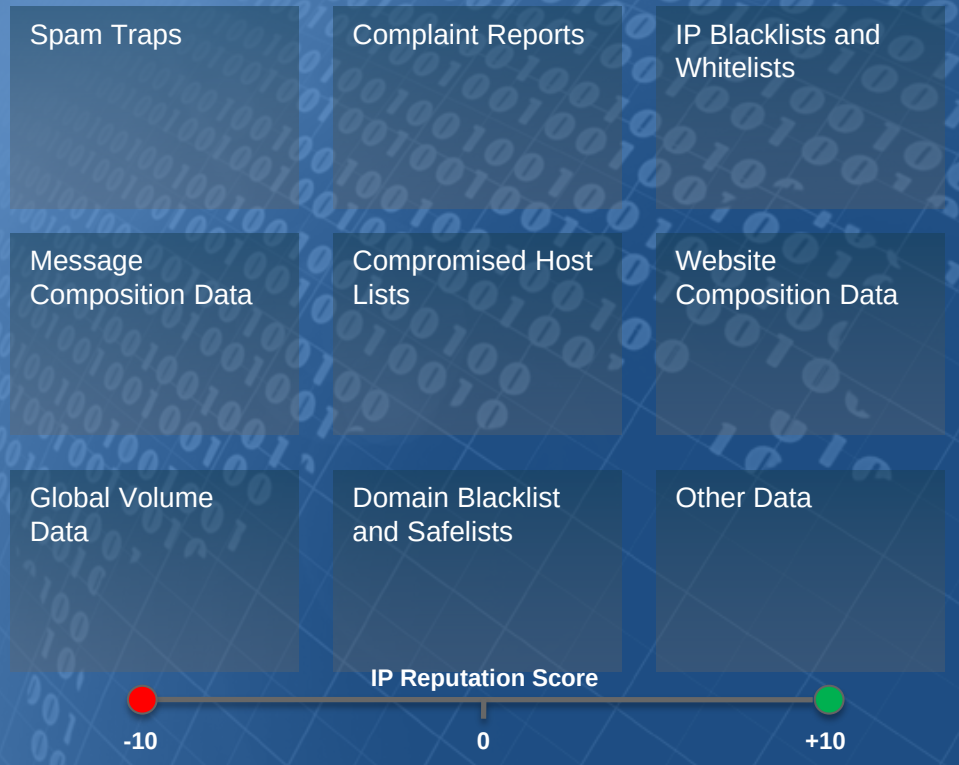
All enterprise features, plus

- Content filtering (with Google SafeSearch)
- Kaspersky Anti-Virus and Anti-Phishing
- SourceFire IPS / IDS
- Geo-based firewall rules
- Advanced Malware Protection (AMP)

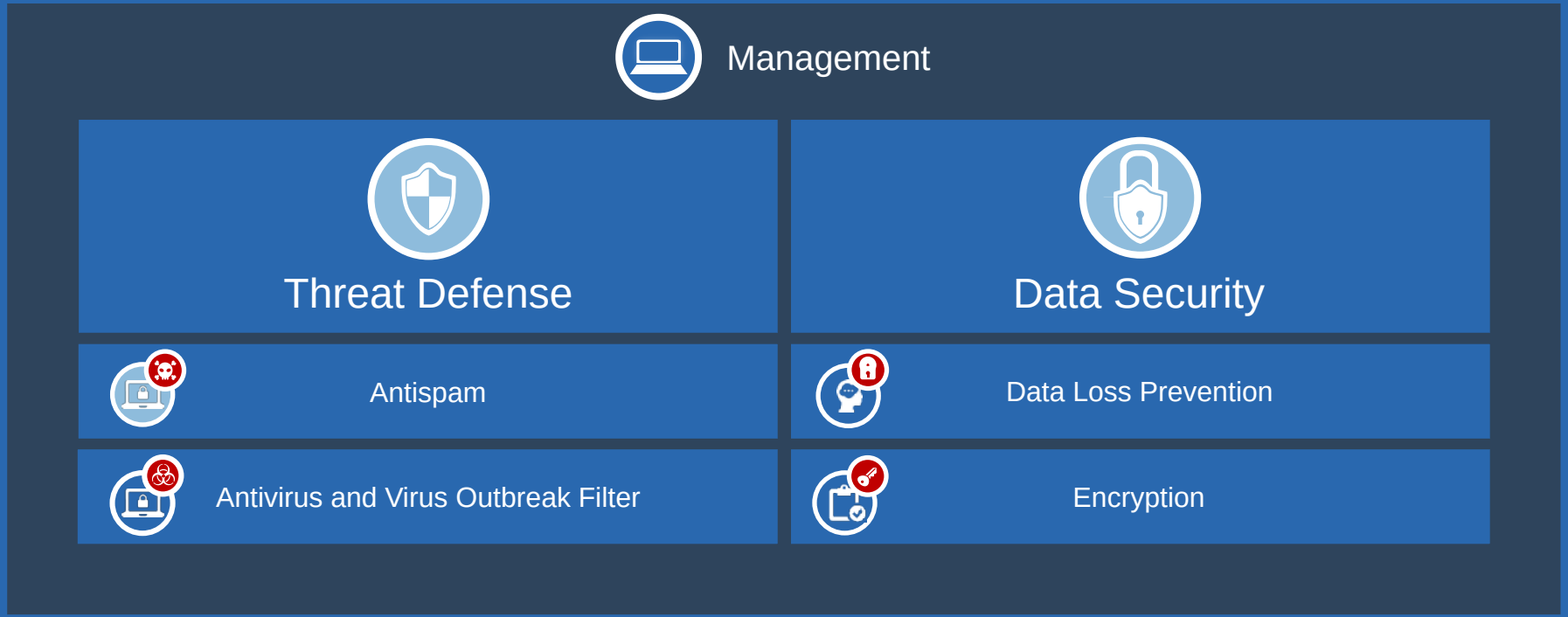
Cisco Email Security

Cisco SensorBase: Email Reputation Database

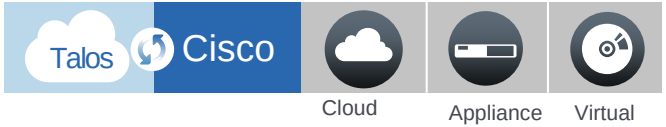
Breadth and quality of data make the difference

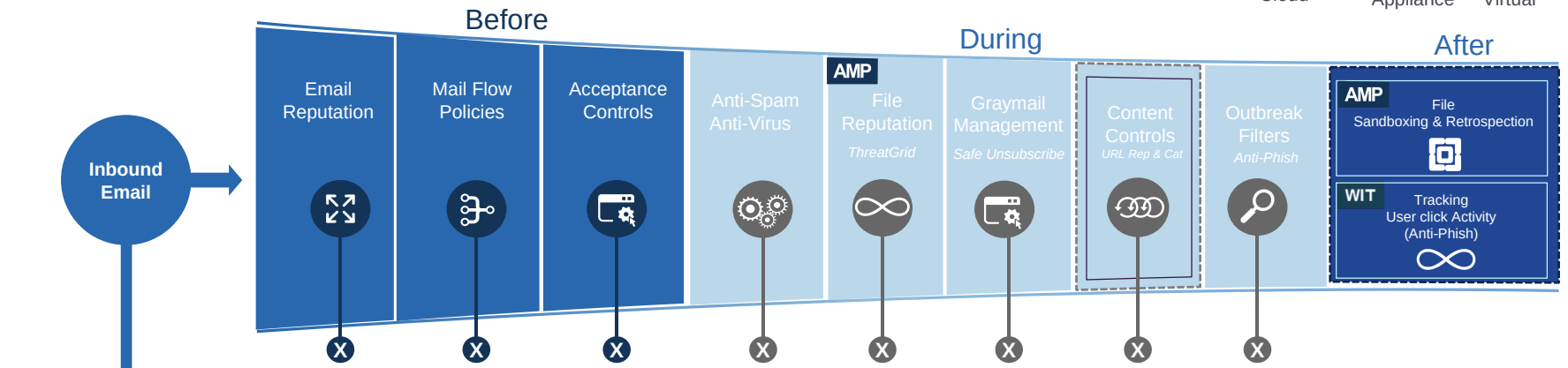


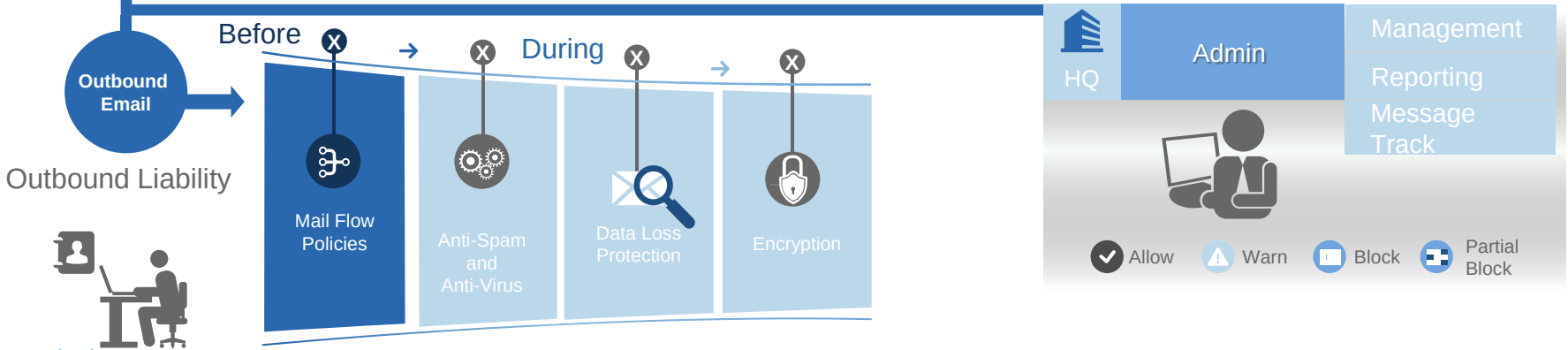
Cisco Email Security Architecture



Cisco Email Security







Cisco Security and OpenDNS

What is DNS?

Domain Name System

- A system for relating names and numbers
- Domain = IP Address
- Amazon.com = 205.251.242.103
- Like a library of phone books

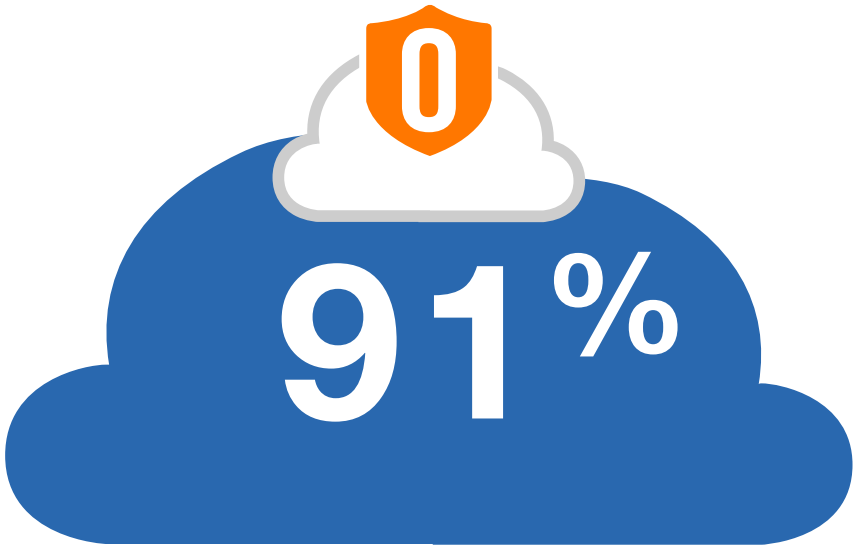
Types of DNS

DOMAIN REGISTRAR
Maps and records names to #s in “phone books”

AUTHORITATIVE DNS
Owns and publishes the “phone books”

RECURSIVE DNS
Looks up & remembers the #s for each name

DNS and Malware

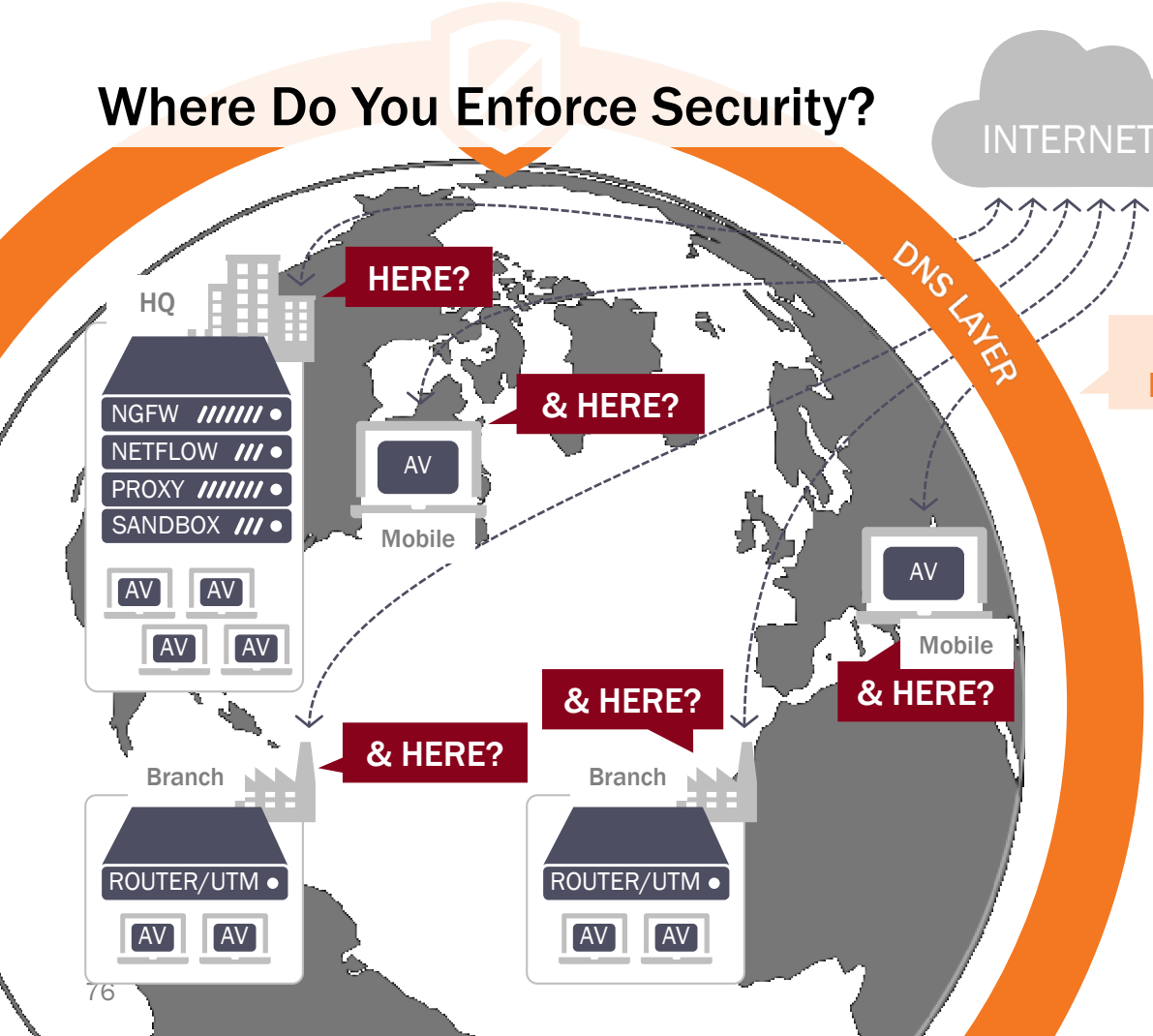


Malware validated as “known bad” – 91% of all malware - use the Domain Name Service in one of these three ways:

- To gain command and control
- To exfiltrate data
- To redirect traffic

Few companies are monitoring DNS for security purposes (or monitoring DNS at all).

Where Do You Enforce Security?



BENEFITS

Alerts Reduced 2x; Improves Your SIEM

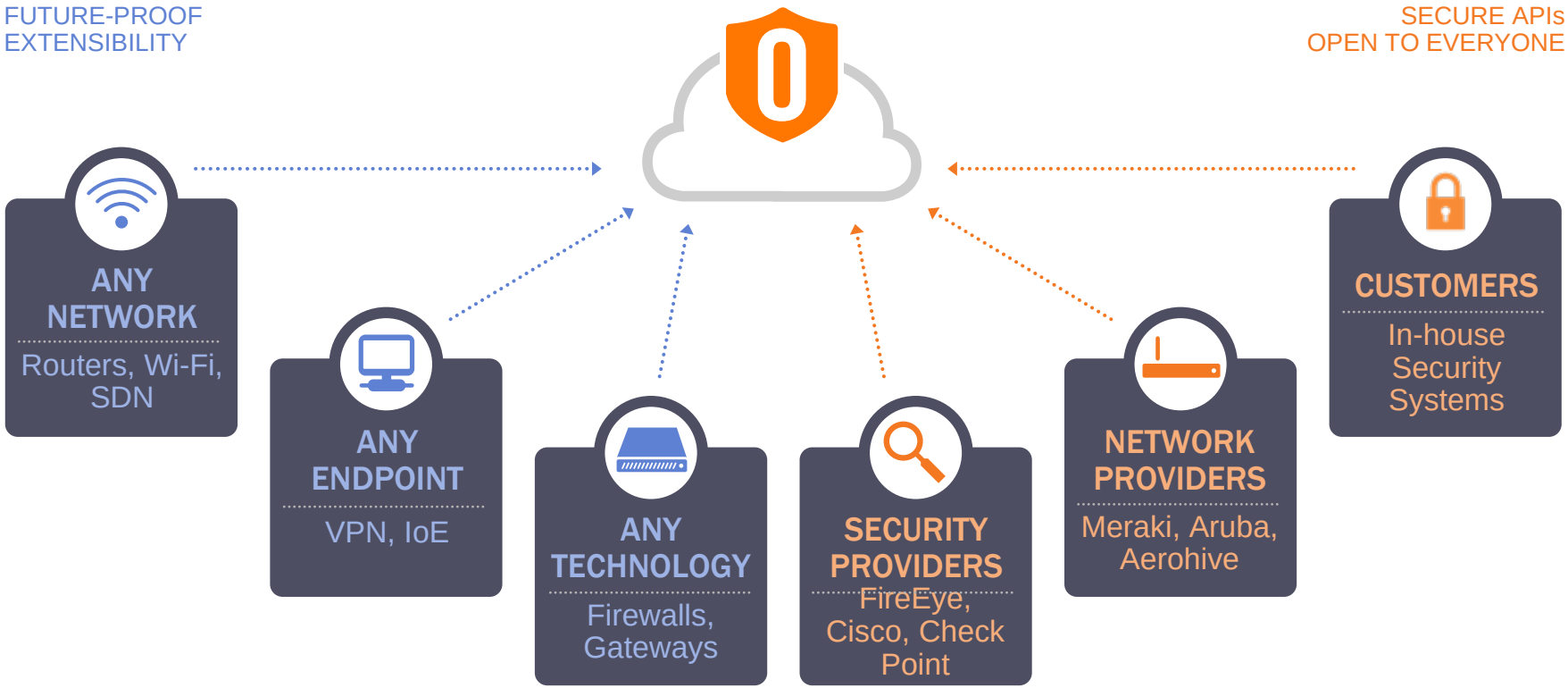
Traffic & Payloads Never Reach Target

Internet Access Is Faster; Not Slower

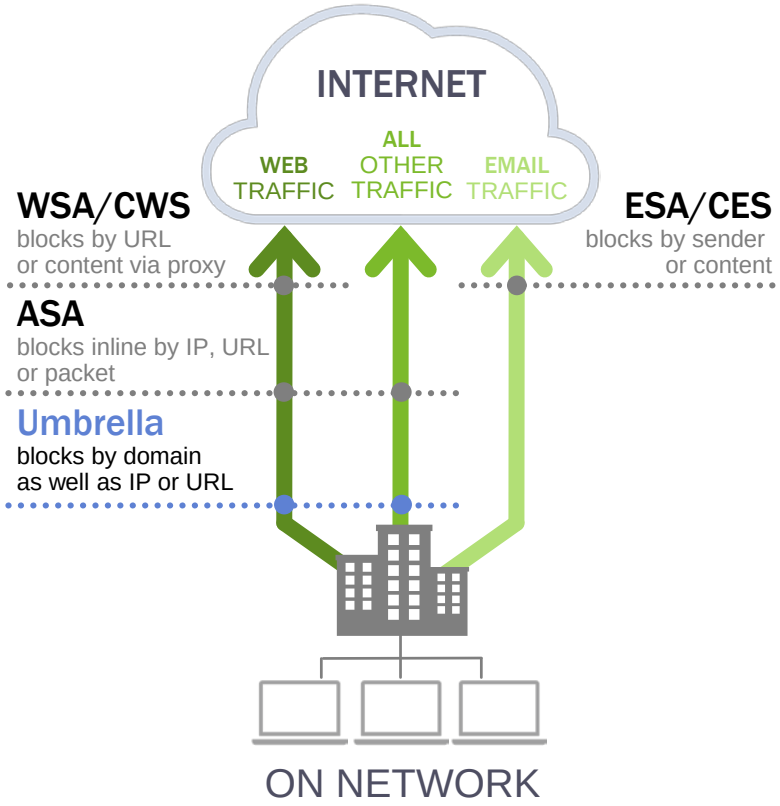
Provision Globally in UNDER 30 MINUTES

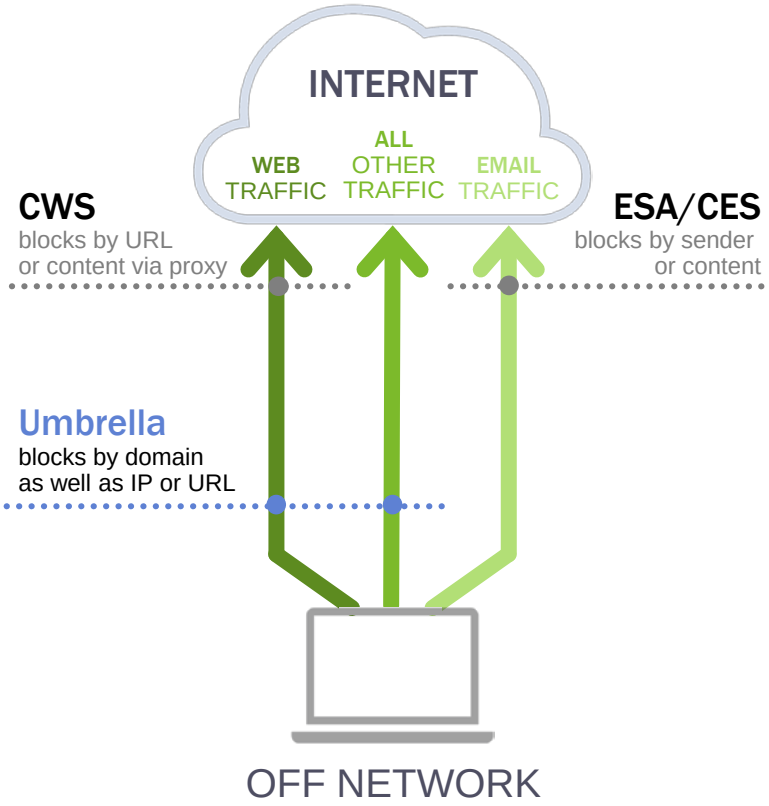
OpenDNS

OpenDNS Works With Everything You Use



Where Does Umbrella Fit?





Network As A Sensor
Nework As An Enforcer

Insider Threats

One out of four breaches are caused by malicious insiders

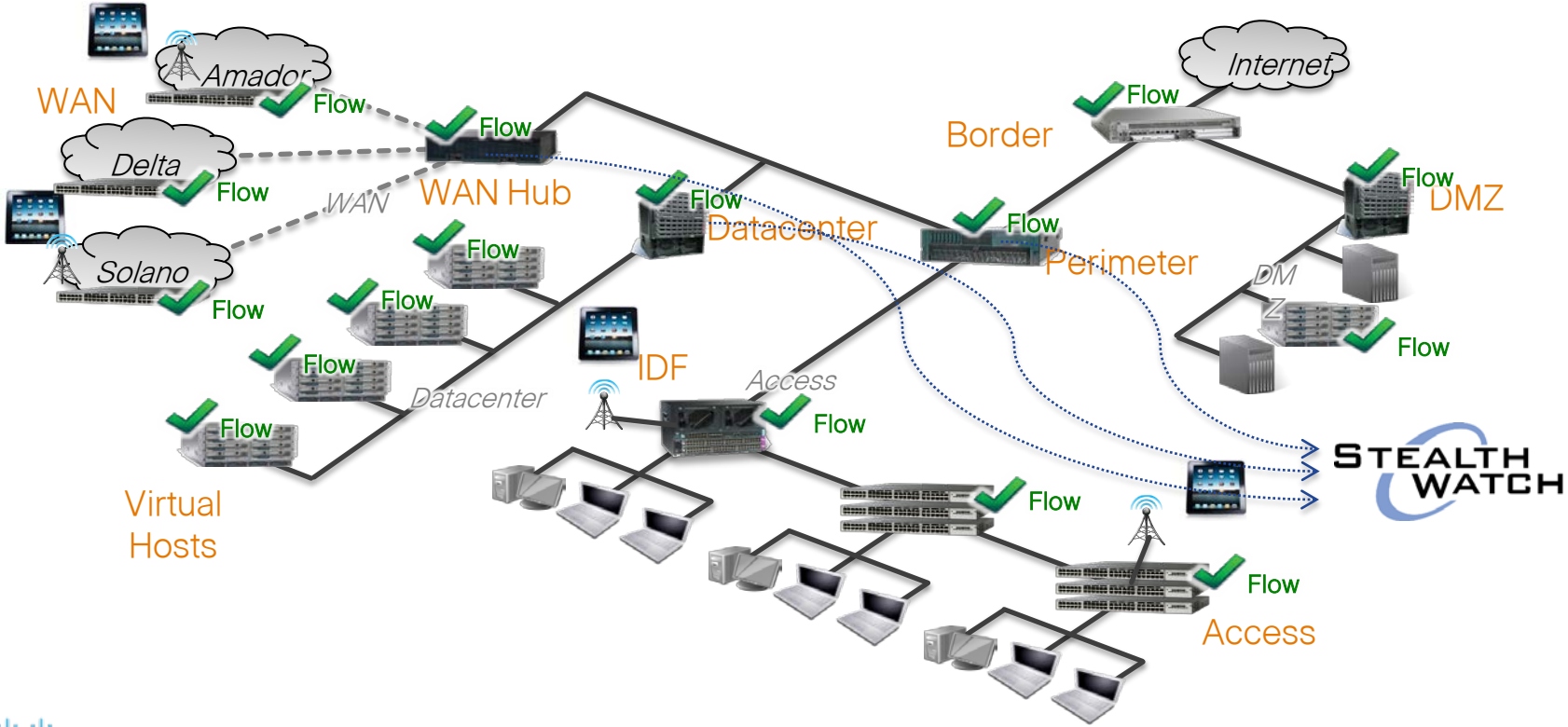
95% of all cybercrime is user-triggered by disguised malicious links

Two out of three breaches exploit weak or stolen passwords

With lateral movement of advanced persistent threats, even external attacks eventually become internal threats

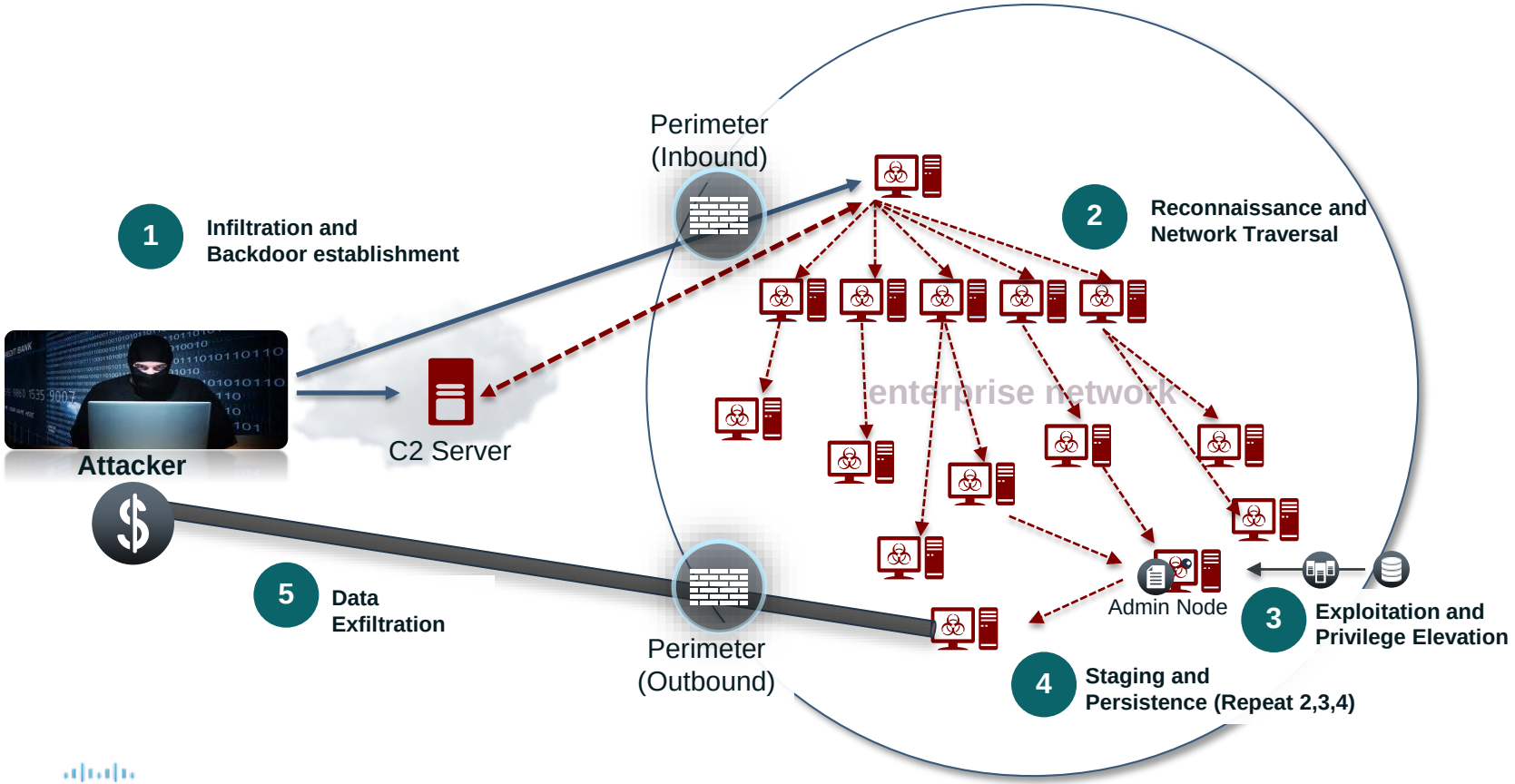
Cisco Stealthwatch: Ubiquitous visibility via flow telemetry

… your infrastructure is the source:



81

Anatomy of a Data Breach



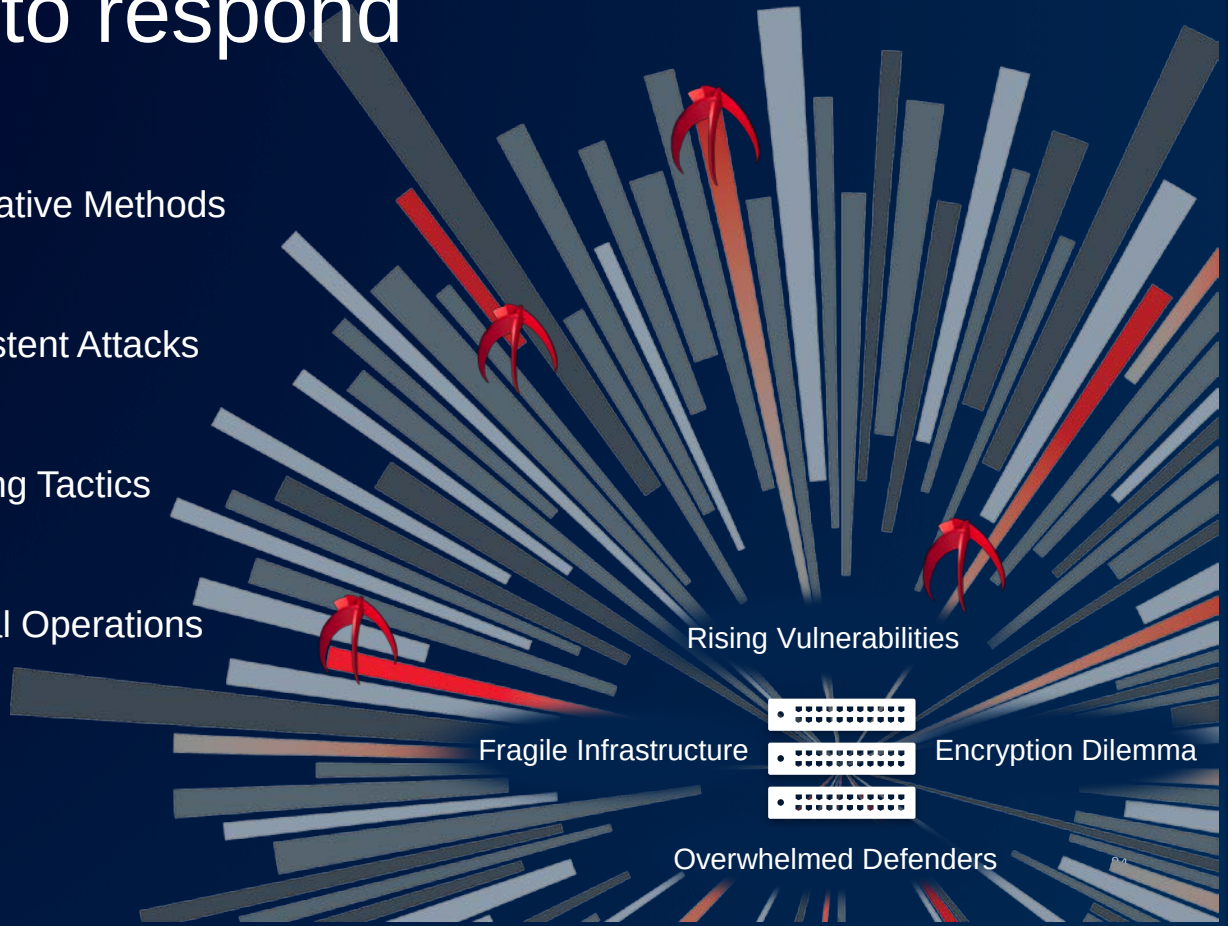
Cisco 2016

Midyear Cybersecurity Report Highlights

July 2016

Asymmetric battles are greater than our ability to respond

- Innovative Methods
- Persistent Attacks
- Shifting Tactics
- Global Operations



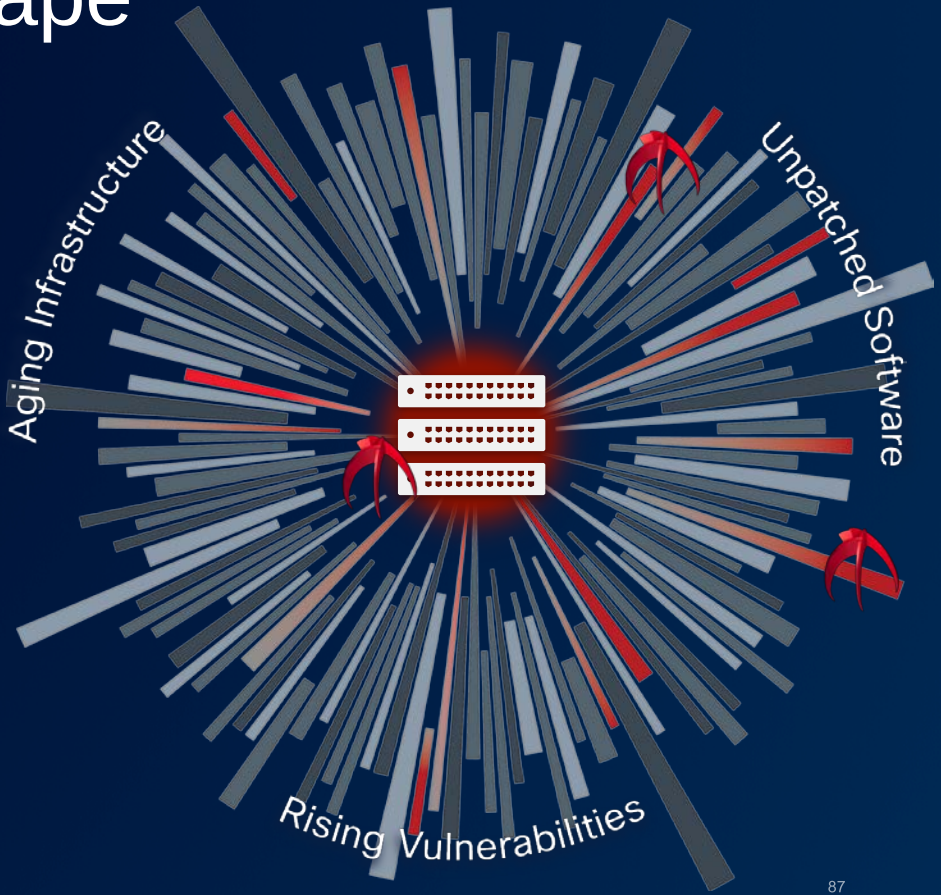
cisco


STAR TREK
BEYOND

Security practitioners need to identify and constrain the operational space of the adversaries

Current Threat Landscape

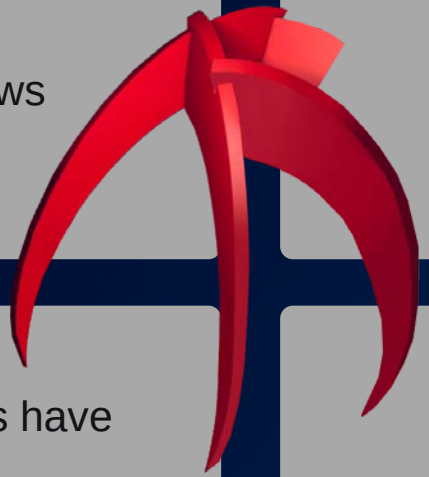
- Evolution of Ransomware
- Advances in Malicious Tradecraft
- Questionable Network Hygiene



Ransomware

Encryption technique allows per-target customization

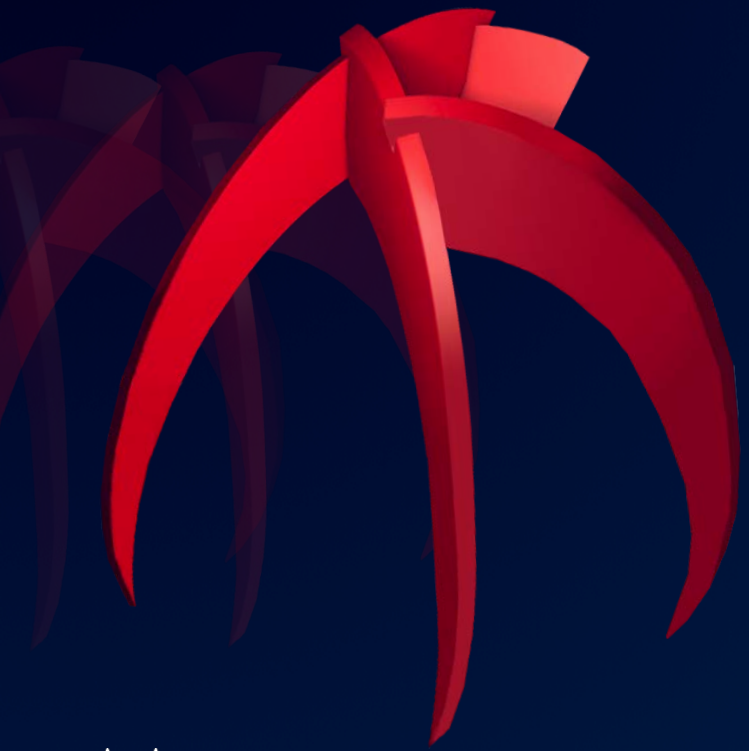
Using Bitcoin for anonymous payment



Marking systems and files have already been encrypted

Dual deadlines for:
1.Cost increase
2.Deleting data

Ransomware 2.0



Self-propagating

- Utilization of a vulnerability in a widely deployed product
- Replication to all available drives
- File infections
- Limited brute-force activity
- Resilient command and control
- Use of other backdoors

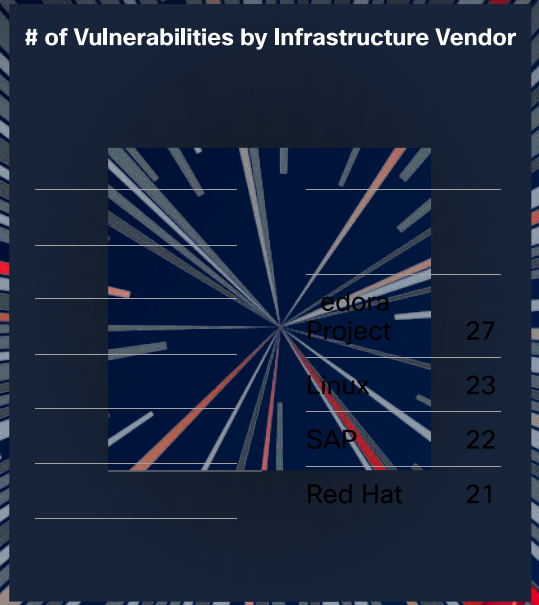
Modular

- Autorun.Inf/USB Mass Storage Propagation
- Authentication Infrastructure Exploits
- Command and Control/Reporting Infections
- Rate Limiter
- RFC 1918 Target Address Limiter

Attack Vectors: Servers on the Horizon

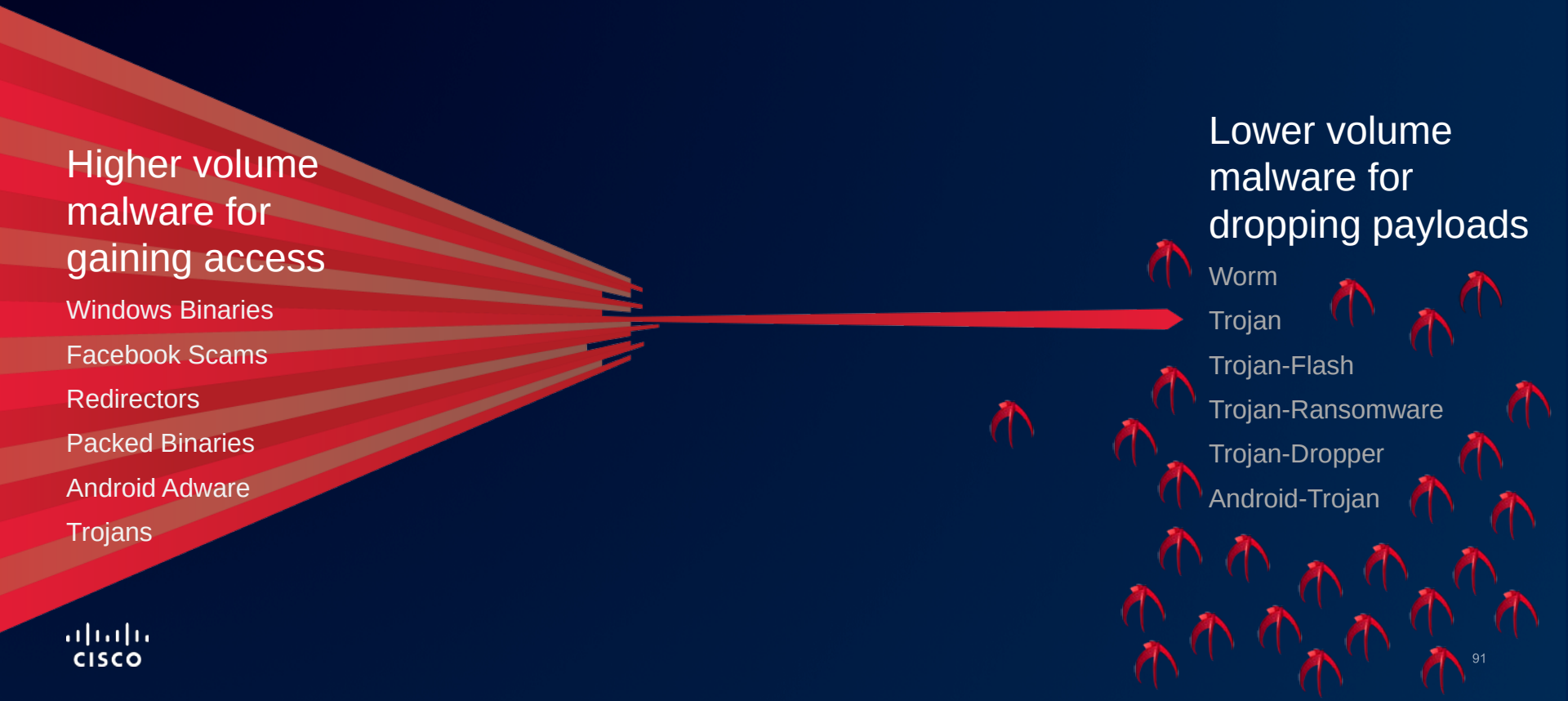
Adversaries expand focus from client-side attacks to server-side attack

Adobe Flash vulnerabilities continue to be leveraged by exploit kits.



In April, Cisco estimated that 10% of all Jboss servers worldwide were compromised.

Attack Methods: A Spectrum of Opportunity



Exploit Kit Activity: Adobe Flash and Malvertising

Adobe Flash and Microsoft Silverlight vulnerabilities are leveraged by most exploit kits

Malware Use of HTTPS:

HTTPS increased 300% for ad-injectors in the last 4 months.

Increased

300%

in 4 months

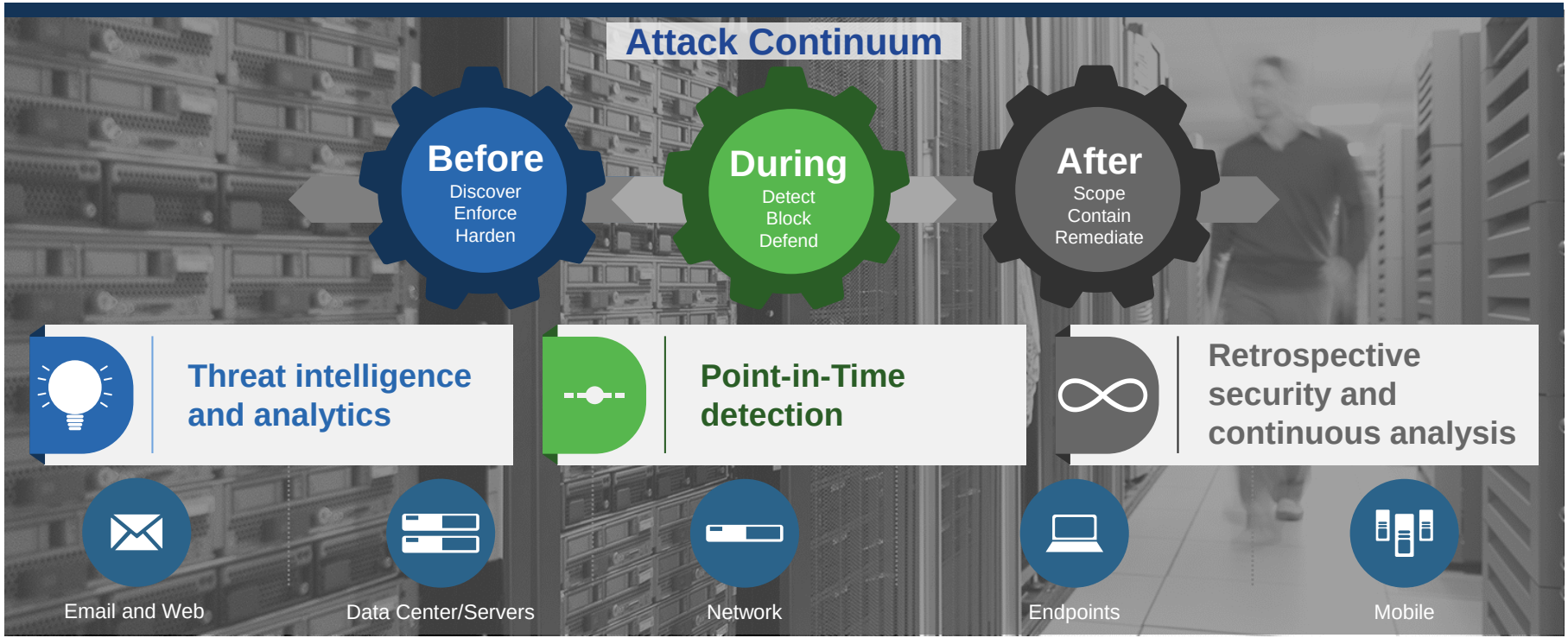
Ad injection is the biggest contributor. Adversaries are using HTTPS traffic to expand time to operate.

2016 Midyear Cybersecurity Report

www.cisco.com/go/mcr2016

Conclusion

Cisco Provides Threat Intelligence, Point-in-Time Detection, and Continuous Analysis of Files to Defeat Advanced Threats



Thank You and Next Steps

Contact Your Cisco Partner
https://tools.cisco.com/WWChannels/LOCATR/performBasicSearch.do

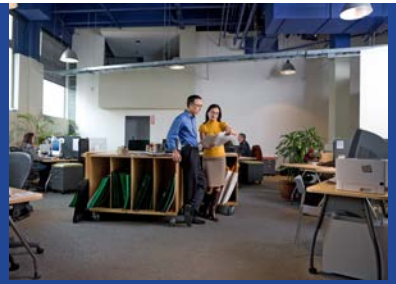
Brian Avery
bravery@cisco.com

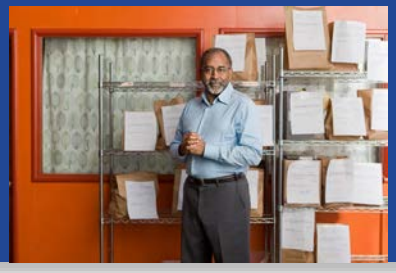
Learn more about Cisco Security:
www.cisco.com/go/security/

Join us again for a future Cisco Customer Education Event

- CCE sessions are held weekly on a variety of topics
- CCE sessions can help you understand the capabilities and business benefits of Cisco technologies
- Watch replays of past events and register for upcoming events!

Visit http://cs.co/cisco101 for details





Thank you.