Integrated Threat Defense

Cisco Solutions Summit

Timothy Snow, CCIE
Consulting Systems Engineer

The challenges come from every direction

Integrated Threat Defense…..

What we want

What we do

What we get

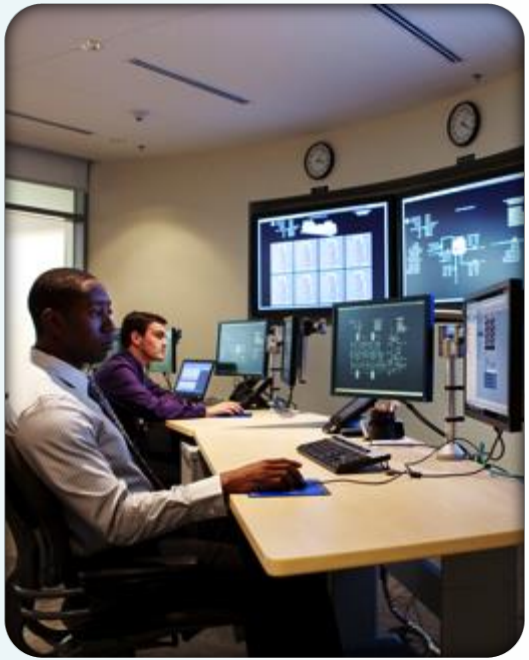
cisco

We read about what happens to everyone else…..

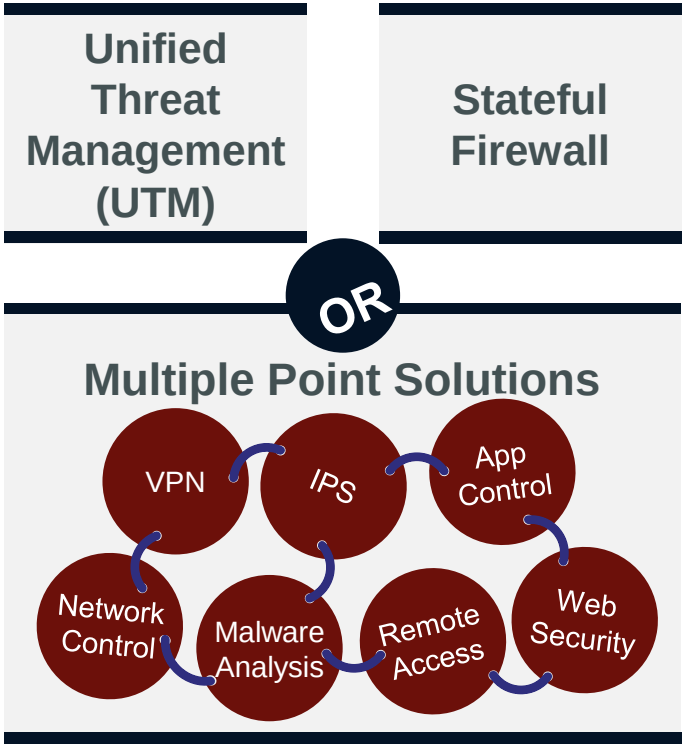
cisco

New Threats and New Security Realities

- 350% increase in countries experiencing major data breaches
- Continuing rise in data breaches in year over year
- 60% of data is stolen within hours
- 52% of breaches remain undiscovered for months
- 100% of companies connect to domains that host malicious files or services



Your security options have been limited

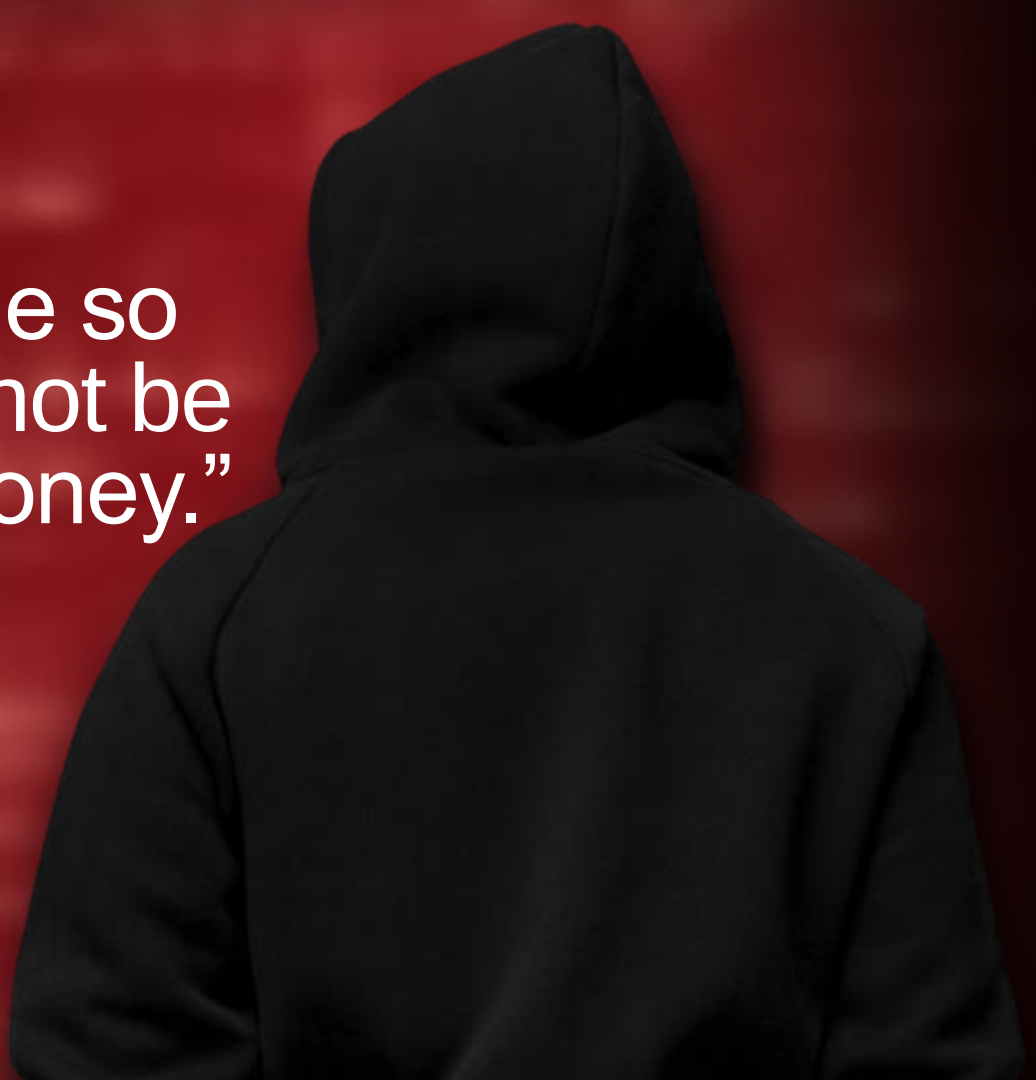


Limited threat effectiveness

Difficult integrations leave security gaps

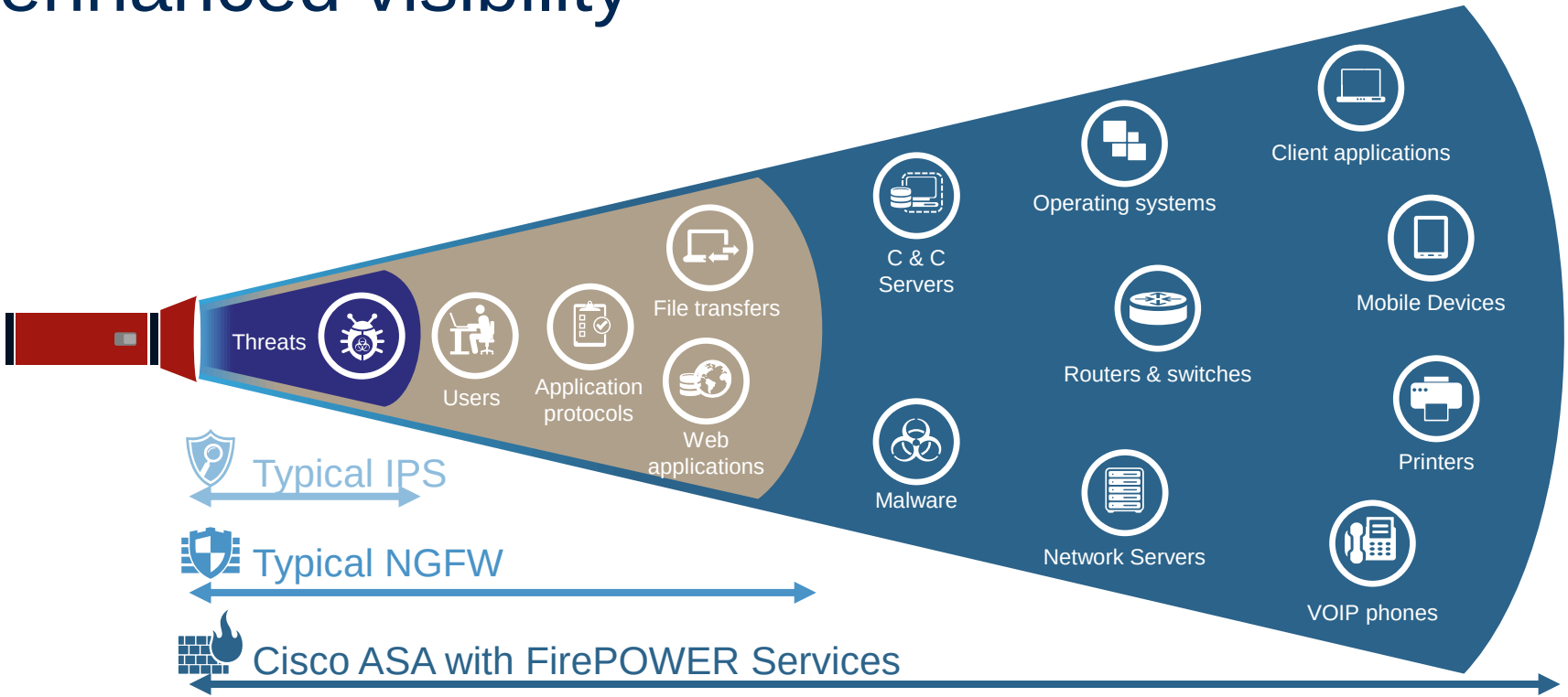
Costly & time-consuming setup and support

“There is no castle so strong that it cannot be overthrown by money.”
– Cicero

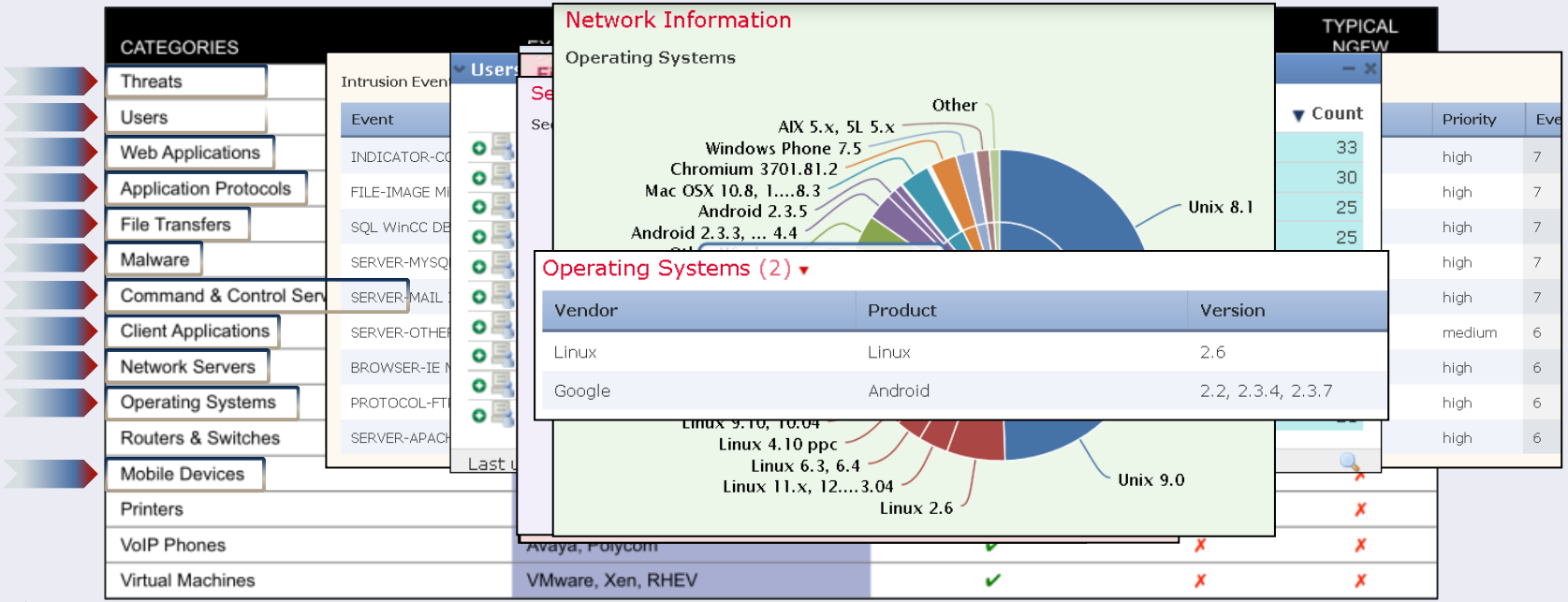


Visibility To Detect, Understand, and Stop Threats

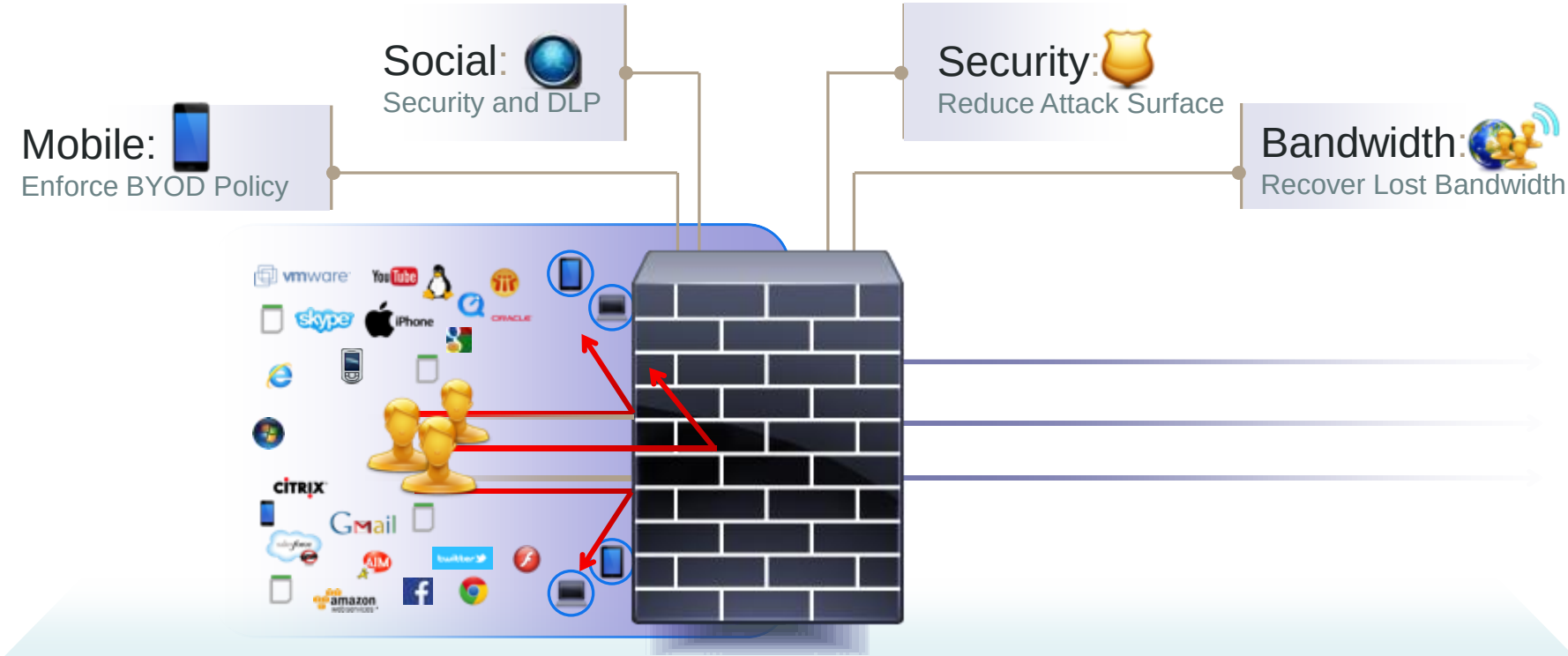
Cisco FirePOWER NGFW/NGIPS offers enhanced visibility



Cisco FireSIGHT Provides Enhanced Visibility for Accurate Threat Detection and Adaptive Defense



Visibility Enables Application Control



Automated, Integrated Threat Defense

Superior Protection for Entire Attack Continuum

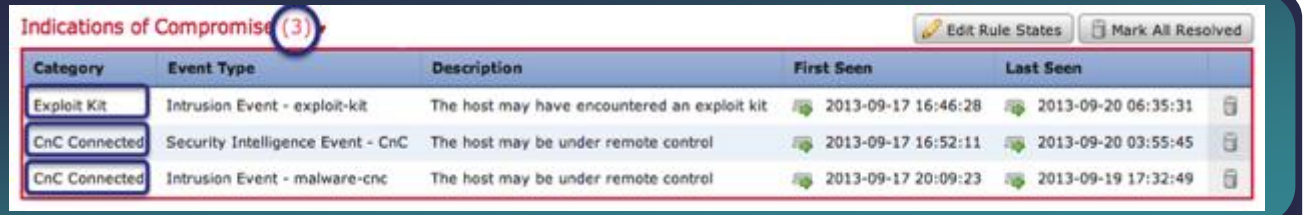
Automated, Integrated Threat Defense

Superior Protection for Entire Attack Continuum

Automated, Integrated Threat Defense

Superior Protection for Entire Attack Continuum

- Context and Threat Correlation
- Dynamic Security Control
- Multi-Vector Correlation
- Retrospective Security



Automated, Integrated Threat Defense

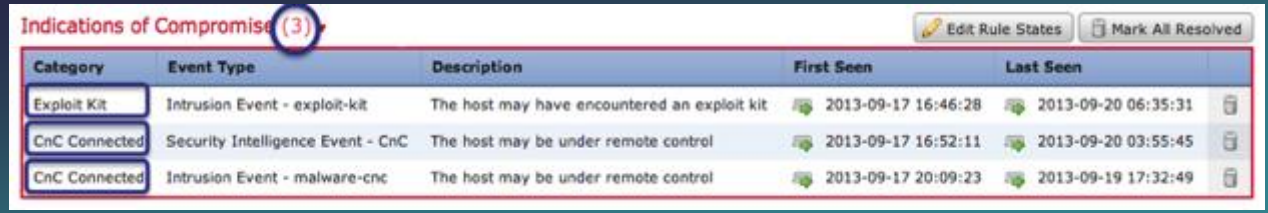
Superior Protection for Entire Attack Continuum

Context and Threat Correlation

Dynamic Security Control

Multi-Vector Correlation

Retrospective Security



Malware backdoors
Exploit kits
Web app attacks
CnC connections
Admin privilege escalations

Connections to known CnC IPs

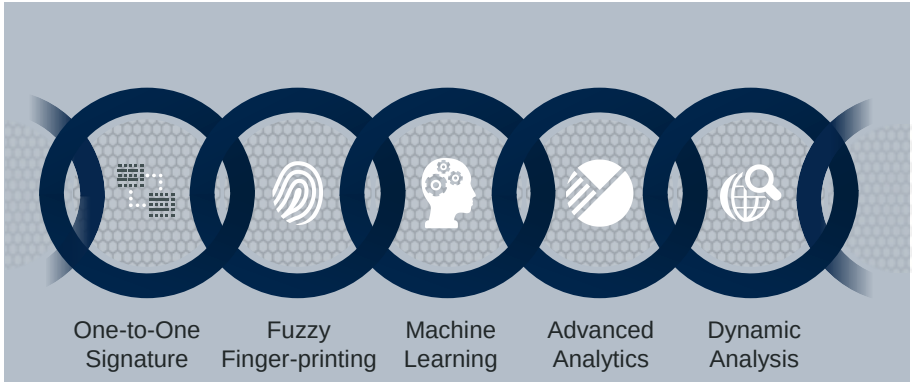
Malware detections
Office/PDF/Java compromises
Malware executions
Dropper infections

Automated, Integrated Threat Defense

Superior Protection for Entire Attack Continuum

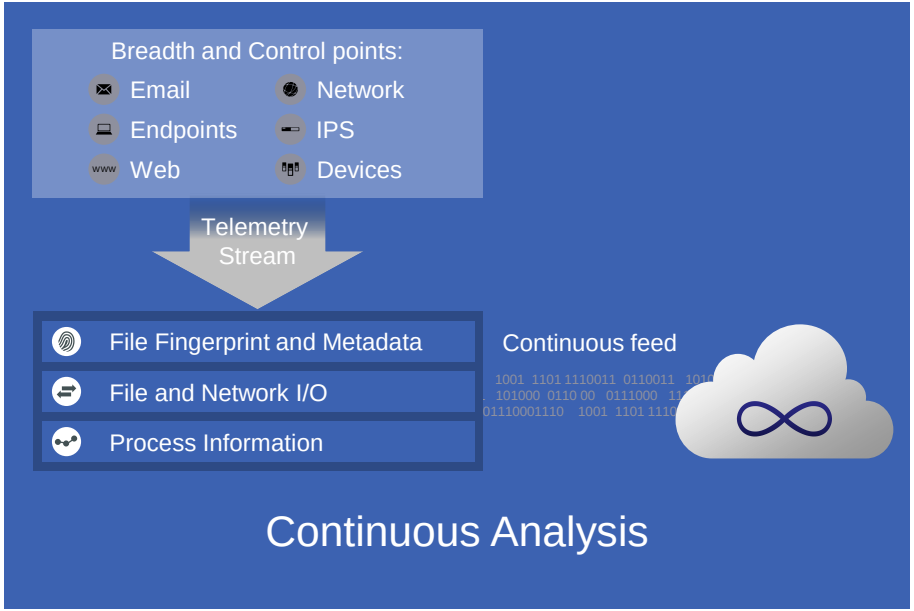
AMP Offers Point-in-Time and Continuous Protection

Point-in-Time Protection



File Reputation & Sandboxing

Retrospective Security



Continuous Analysis

Threat Scoring

300+ behavioral indicators (and growing)

- Malware families, malicious behaviors, and more
- Detailed description and actionable information

Prioritize threats with confidence

- Enhance SOC analyst and IR knowledge and effectiveness (and security product)

Behavioral Indicators — Threat Score: 100

Artifact Flagged as Known Trojan by Antivirus	Severity: 100 Confidence: 100
Process Modified an Executable File	Severity: 95 Confidence: 95
A Document File Established Network Communications	Severity: 90 Confidence: 90
PDF Contains Embedded JavaScript Stream	Severity: 80 Confidence: 80
Process Modified Shell Program Autorun Registry Key Value	Severity: 80 Confidence: 60

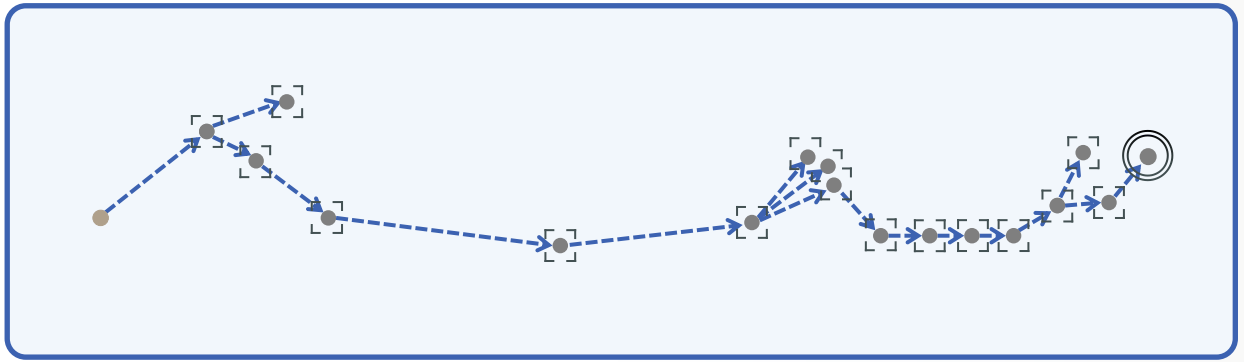
Autorun registry keys can be used to load applications when Windows is started. Malware often uses these key locations to maintain persistence on the host. The values to examine are located in subkeys Run or load. The key value will indicate where the program that will load on startup is located.

Categories persistence
Tags process, autorun, registry

Process ID	Process Name	RegKey Name	RegKey Value Name	RegKey Data Type	RegKey Data
1312 (spoolsv.exe)	spoolsv.exe	USER\S-1-5-21-1202660629-583907252-1801674531-1003\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINDOWS	load	SZ	C:\DOCUME~1\JOEMAL~1\LOCALS~1\Temp\spoolsv.exes\\0

Artifact Flagged by Antivirus has Assigned CVE Number	Severity: 70 Confidence: 50
Process Modified File in a User Directory	S

Retrospective Security Is Built Upon…



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

Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374
File Name	WindowsMediaInstaller.exe
File Type	MSEXE
File Category	Executables
Current Disposition	Malware
Threat Score	High
First Seen	2013-12-06 10:57:13 on 10.4.10.183
Last Seen	2013-12-06 18:17:27 on 10.4.10.183
Event Count	7
Seen On	4 hosts
Seen On Breakdown	2 senders → 3 receivers

Trajectory

Events Transfer | Block | Create | Move | Execute | Scan | Retrospective | Quarantine

Dispositions Unknown | Malware | Clean | Custom | Unavailable

Events

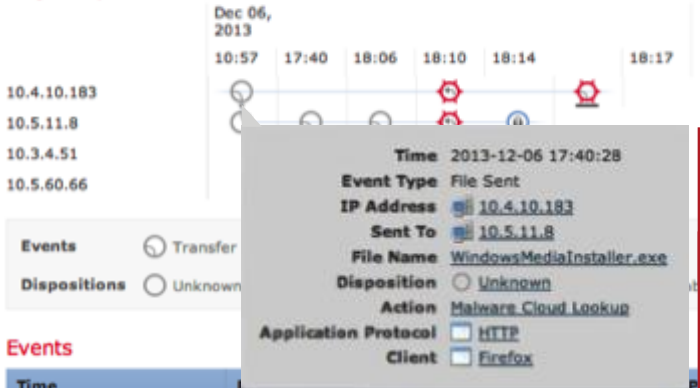
Time	Event Type	Sending IP	Receiving IP	File Name	Disp...	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		

Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374
File Name	WindowsMediaInstaller.exe
File Type	MSEXE
File Category	Executables
Current Disposition	Malware
Threat Score	High

First Seen	2013-12-06 10:57:13 on 10.4.10.183
Last Seen	2013-12-06 18:17:27 on 10.4.10.183
Event Count	7
Seen On	4 hosts
Seen On Breakdown	2 senders → 3 receivers

Trajectory



An unknown file is present on IP: 10.4.10.183, having been downloaded from Firefox

Events

Time	Event Type	Sending IP	Receiving IP	File Name	Disp...	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		

Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374
File Name	WindowsMediaInstaller.exe
File Type	MSEXE
File Category	Executables
Current Disposition	Malware
Threat Score	High

First Seen	2013-12-06 10:57:13 on 10.4.10.183
Last Seen	2013-12-06 18:17:27 on 10.4.10.183
Event Count	7
Seen On	4 hosts
Seen On Breakdown	2 senders → 3 receivers

Trajectory

Events Transfer
Dispositions Unknown

Time	2013-12-06 17:40:28
Event Type	File Received
IP Address	10.5.11.8
Received From	10.4.10.183
File Name	WindowsMediaInstaller.exe
Disposition	Unknown
Action	Malware Cloud Lookup
Application Protocol	HTTP
Client	Firefox

At 10:57, the unknown file is from IP: 10.4.10.183 to IP: 10.5.11.8

Events

Time				File Name	Disp...	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		

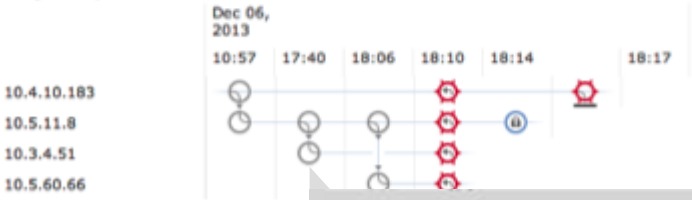
Overview | Analysis | Policies | Devices | Objects | FireAMP | Health | System | Help | admin

Context Explorer | Connections | Intrusions | Files ▸ Network File Trajectory | Hosts | Users | Vulnerabilities | Correlation | Custom | Search

Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374
File Name	WindowsMediaInstaller.exe
File Type	MSEXE
File Category	Executables
Current Disposition	Malware
Threat Score	High
First Seen	2013-12-06 10:57:13 on 10.4.10.183
Last Seen	2013-12-06 18:17:27 on 10.4.10.183
Event Count	7
Seen On	4 hosts
Seen On Breakdown	2 senders → 3 receivers

Trajectory



Events Transfer

Dispositions Unknown

Time 2013-12-06 18:06:03
Event Type File Received
IP Address 10.3.4.51
Received From 10.5.11.8
File Name WindowsMediaInstaller.exe
Disposition Unknown
Action
Application Protocol NetBIOS-ssn (SMB)

Seven hours later the file is then transferred to a third device (10.3.4.51) using an SMB application

Events

Time	Event Ty...			File Na...					Web Ap...	Description
2013-12-06 10:57:13	Retrospec...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		

Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374
File Name	WindowsMediaInstaller.exe
File Type	MSEXE
File Category	Executables
Current Disposition	Malware
Threat Score	High
First Seen	2013-12-06 10:57:13 on 10.4.10.183
Last Seen	2013-12-06 18:17:27 on 10.4.10.183
Event Count	7
Seen On	4 hosts
Seen On Breakdown	2 senders → 3 receivers

Trajectory

Events Transfer Block
Dispositions Unknown Malware

Time 2013-12-06 18:10:03
Event Type File Received
IP Address 10.5.60.66
Received From 10.5.11.8
File Name WindowsMediaInstaller.exe
Disposition Unknown
Action
Application Protocol NetBIOS-ssn (SMB)

The file is copied yet again onto a fourth device (10.5.60.66) through the same SMB application a half hour later

Events

Time	Event Type	Se							Description
2013-12-06 10:57:13	Retrospectiv...								
2013-12-06 17:40:28	Transfer	10		MediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox	Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...				
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...				
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox	

Overview | Analysis | Policies | Devices | Objects | FireAMP | Health | System | Help | admin

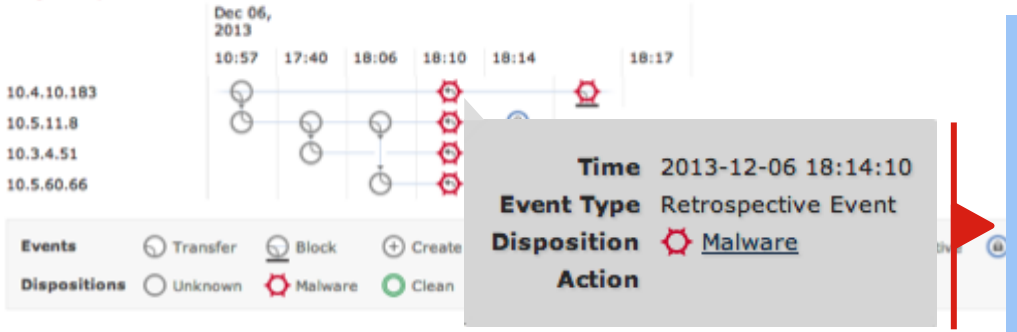
Context Explorer | Connections | Intrusions | Files ▸ Network File Trajectory | Hosts | Users | Vulnerabilities | Correlation | Custom | Search

Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374
File Name	WindowsMediaInstaller.exe
File Type	MSEXE
File Category	Executables
Current Disposition	Malware
Threat Score	High

First Seen	2013-12-06 10:57:13 on 10.4.10.183
Last Seen	2013-12-06 18:17:27 on 10.4.10.183
Event Count	7
Seen On	4 hosts
Seen On Breakdown	2 senders → 3 receivers

Trajectory



The Cisco TALOS Intelligence Cloud has learned this file is malicious and a retrospective event is raised for all four devices immediately.

Events

Time	Event Type	Sending IP	Receiving IP	File Name	Disp...	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		

Overview | Analysis | Policies | Devices | Objects | FireAMP — Health | System | Help | admin

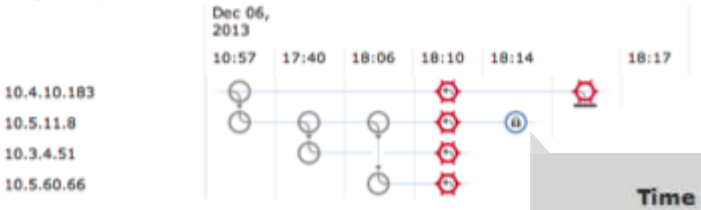
Context Explorer | Connections | Intrusions | Files ▸ Network File Trajectory | Hosts | Users | Vulnerabilities | Correlation | Custom | Search

Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374
File Name	WindowsMediaInstaller.exe
File Type	MSEXE
File Category	Executables
Current Disposition	Malware
Threat Score	High

First Seen	2013-12-06 10:57:13 on 10.4.10.183
Last Seen	2013-12-06 18:17:27 on 10.4.10.183
Event Count	7
Seen On	4 hosts
Seen On Breakdown	2 senders → 3 receivers

Trajectory



Events: Transfer | Block | Create | Mo...

Dispositions: Unknown | Malware | Clean | Cu...

Time 2013-12-06 18:14:23
Event Type File Quarantined
IP Address 10.5.11.8
File Name WindowsMediaInstaller.exe
Disposition Malware
Action

At the same time, a device with the FireAMP endpoint connector reacts to the retrospective event and immediately stops and quarantines the newly detected malware

Events

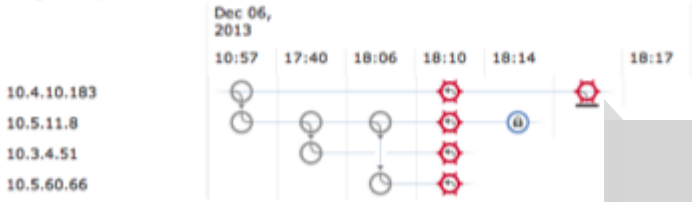
Time	Event Type	Sending IP			Disp...	A...			
2013-12-06 10:57:13	Retrospectiv...				Malwa...				
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox	Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...				
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...				
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox	

Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374
File Name	WindowsMediaInstaller.exe
File Type	MSEXE
File Category	Executables
Current Disposition	Malware
Threat Score	High

First Seen	2013-12-06 10:57:13 on 10.4.10.183
Last Seen	2013-12-06 18:17:27 on 10.4.10.183
Event Count	7
Seen On	4 hosts
Seen On Breakdown	2 senders → 3 receivers

Trajectory



Events: Transfer | Block | Create | Move
Dispositions: Unknown | Malware | Clean | Custom

Time	2013-12-06 18:17:27
Event Type	File Sent
IP Address	10.4.10.183
Blocked Recipient	10.5.11.8
File Name	WindowsMediaInstaller.exe
Disposition	Malware
Action	Malware Block
Application Protocol	HTTP
Client	Firefox

8 hours after the first attack, the Malware tries to re-enter the system through the original point of entry but is recognized and blocked.

Events

Time	Event Type	Sending IP	Receiving IP	File Name	Disp...	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		

Remediate quickly after a breach

Advanced Malware Protection (AMP)

Continuous analysis + retrospective security

- Reduce clean-up time from weeks to hours with AMP everywhere
- Identify malware and suspicious files through behavioral indicators
- Eliminate infections by turning back the clock

Cisco Security Intelligence to Battle Advanced Threats

Built on unmatched collective security analytics

Threat Intelligence

- 1.6 million global sensors
- 100 TB of data received per day
- 150 million+ deployed endpoints
- 600 engineers, technicians, and researchers
- 35% worldwide email traffic
- 13 billion web requests
- 24x7x365 operations
- 4.3 billion web blocks per day
- 40+ languages

Cisco Talos Collective Security Intelligence

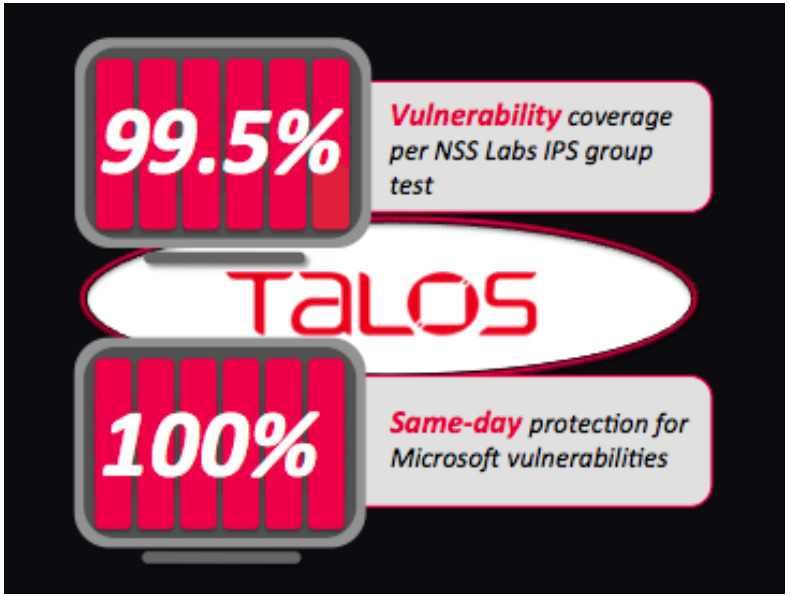
Pervasive Across the Portfolio

Research Response

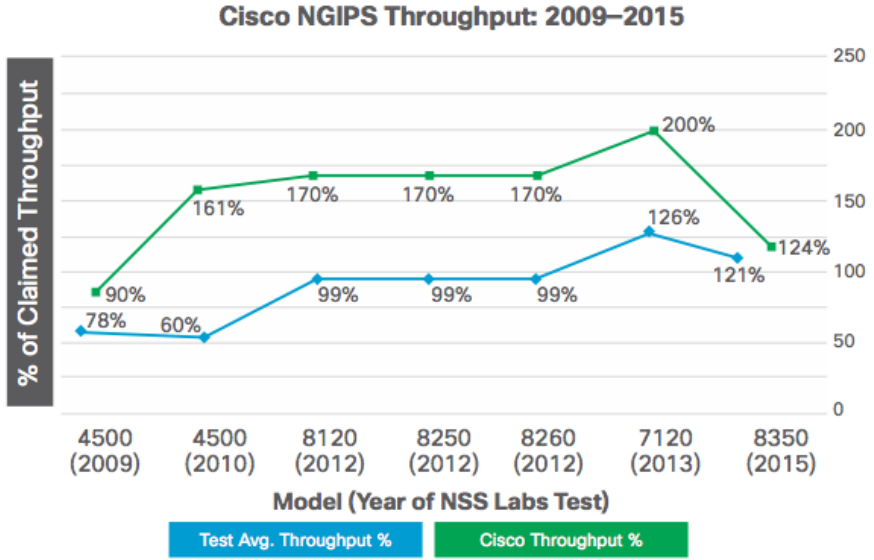
- 1.1 million incoming malware samples per day
- Cisco AMP community
- Advanced Microsoft and industry disclosures
- Snort and ClamAV open source communities
- AEGIS™ program
- Private and public threat feeds
- Talos Security Intelligence
- AMP Threat Grid Intelligence
- Cisco AMP Threat Grid Dynamic Analysis 10 million files/month

Defend Your Network – Cisco NG FW/IPS/AMP System

#1 in Detection, #1 in Performance, #1 in Vulnerability Coverage, 100% Evasion Free



Attacks evolve. You need defenses you can trust



"For the past six years, Cisco (Sourcefire) has consistently achieved excellent results in security effectiveness based on our real-world evaluations of exploit evasions, threat block rate and protection capabilities."

Vikram Phatak, CTO NSS Labs, Inc.

Cisco NGFW / NGIPS Offerings

FirePOWER NGIPS

- **Best-of-Breed NGIPS for Advanced Threat Protection**
- **Scalability up to 60Gbps+**
- **Application and Identity Aware**
- **Lower TCO Through Automation**

Embedded Advanced Malware Prevention (AMP)

- **Class-leading advanced malware solution**
- **File reputation and sandboxing**
- **Malware Forensics reports**
- **Malware and file Retrospection**
- **Cisco AMP Everywhere ensures pervasive coverage**

Cisco NGFW
ASA w/ FirePOWER Services

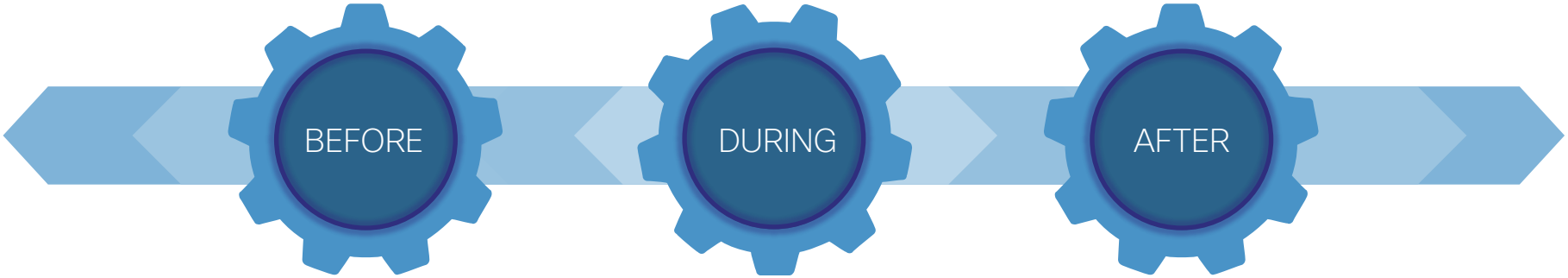
- **Only threat-focused NGFW to cover full attack continuum**
- **Available on existing ASA-x platforms**
- **Integrated NGIPS + AMP**
- **Ultra-Granular Policies: App, Identity, Risk, Business Relevance**

Common NGIPS and AMP code base
Common Threat Management– FireSIGHT
Common Collective Security Intelligence




Flexible Deployment — Appliance — Virtual — Cloud

Why Choose FirePOWER For Integrated Threat Defense?



Supported by Talos, Cisco's threat intelligence organization

(NGFW/NGIPS)

- Discover threats and enforce security policies
- Detect, block, and defend against attacks
- Remediate breaches and prevent future attacks

cisco


CISCO
TM