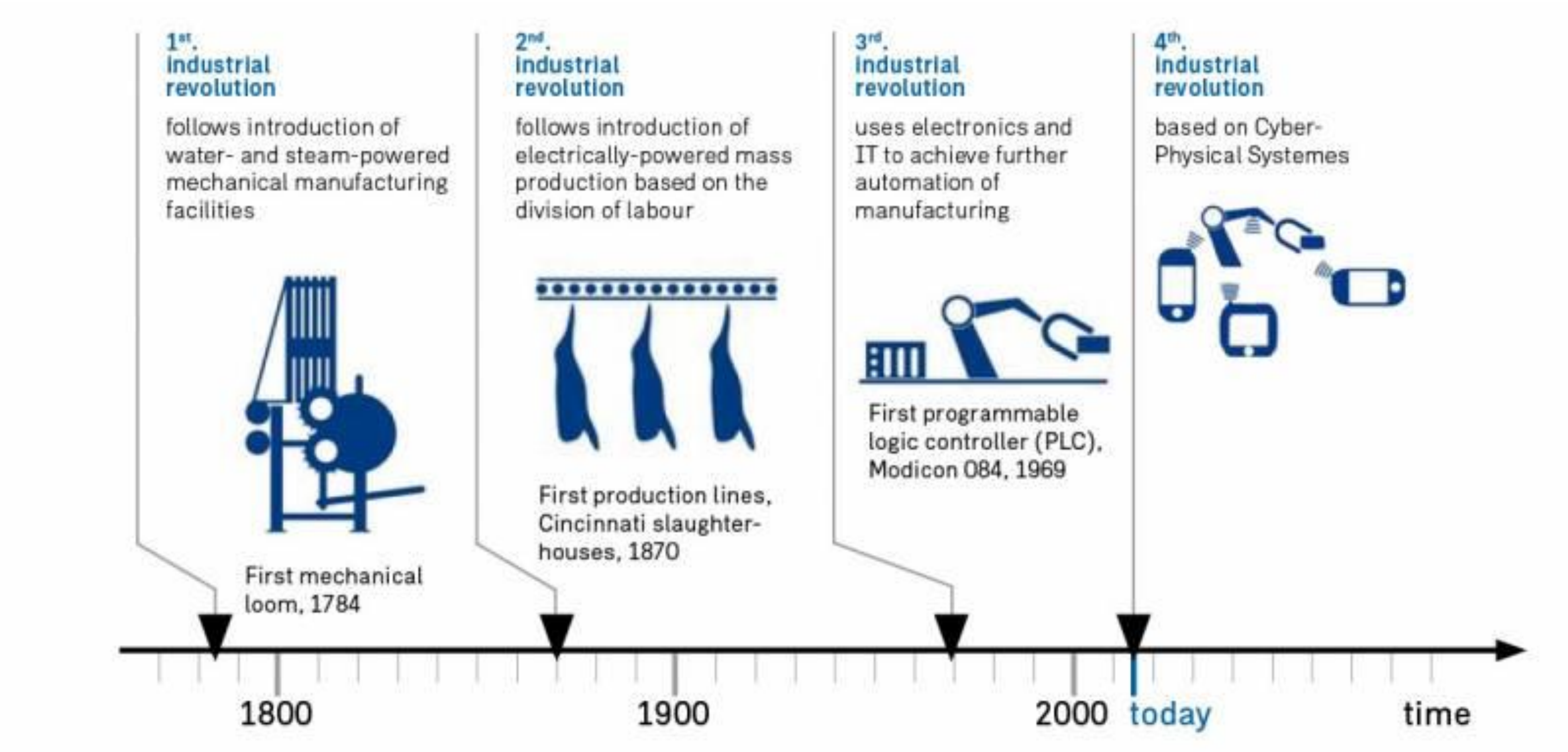
Ascending the Path to Better Security

Respond to Insider Threats and External Cyber Attacks

Nikos Mourtzinos, CCIE #9763
nmourtzi@cisco.com

April 2016

Industry Revolution 4.0 – Digital Transformation - IoT



1st. industrial revolution

follows introduction of water- and steam-powered mechanical manufacturing facilities

First mechanical loom, 1784

2nd. industrial revolution

follows introduction of electrically-powered mass production based on the division of labour

First production lines, Cincinnati slaughter-houses, 1870

3rd. industrial revolution

uses electronics and IT to achieve further automation of manufacturing

First programmable logic controller (PLC), Modicon 084, 1969

4th. industrial revolution

based on Cyber-Physical Systemes

Security as a Business Enabler

The Security Problem

Changing
Business Models

Dynamic
Threat Landscape

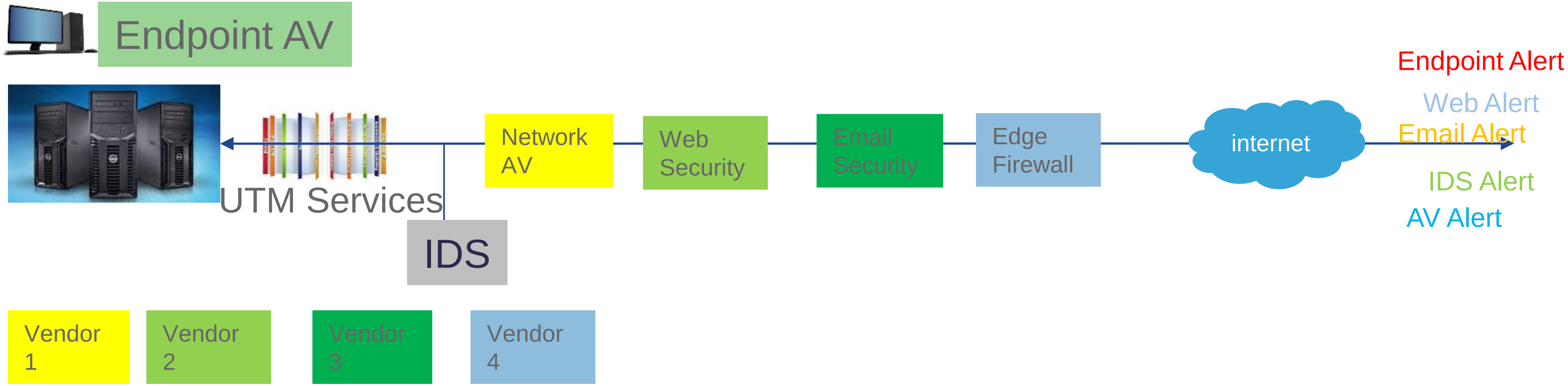
Complexity
and Fragmentation

Complexity and Fragmentation

Limited Visibility

Lacks Correlation

Manual Response



Endpoint AV

UTM Services

IDS

Network AV

Web Security

Email Security

Edge Firewall

internet

Endpoint Alert

Web Alert

Email Alert

IDS Alert

AV Alert

Vendor 1

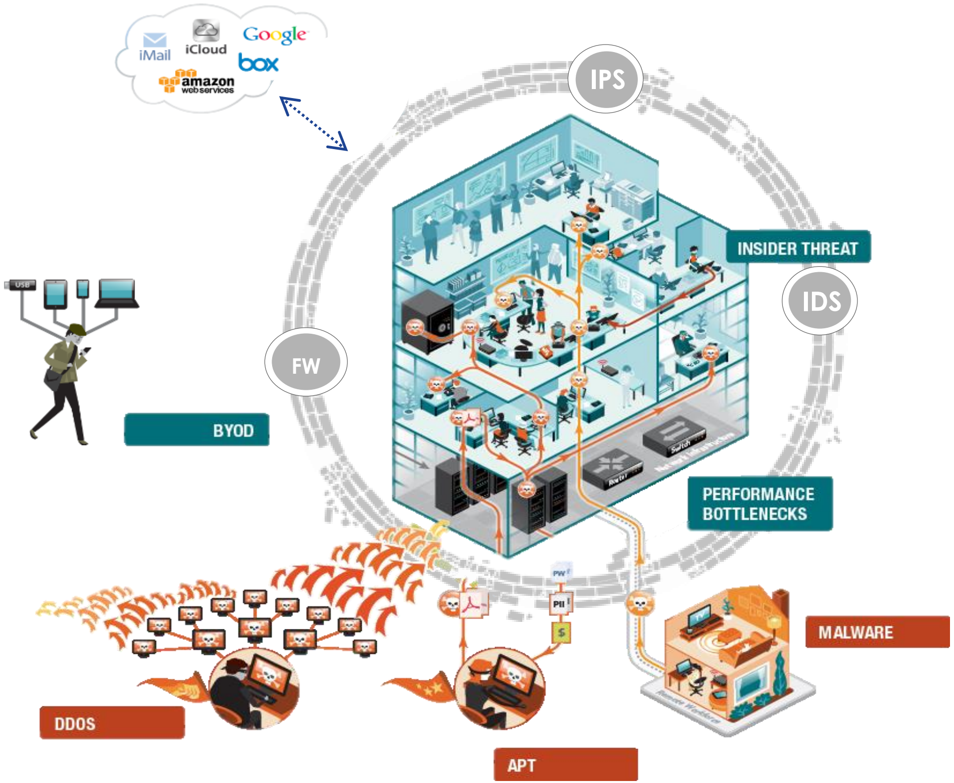
Vendor 2

Vendor 3

Vendor 4

Failure of Legacy Security Architectures

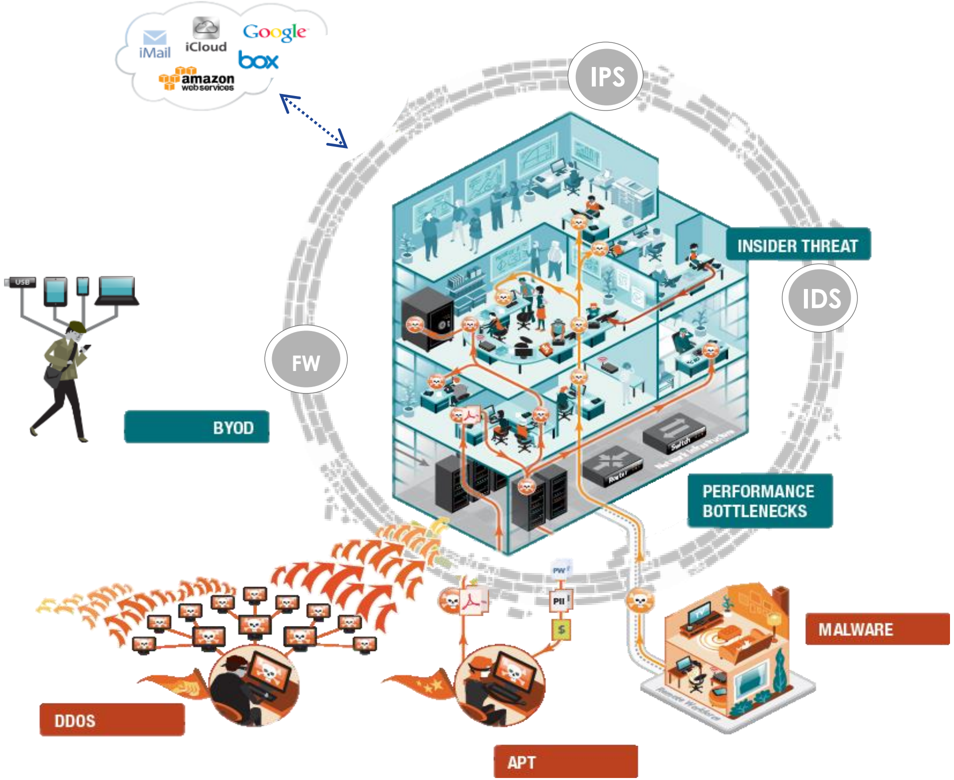
Today top threats still get through



Despite massive security investments

Traditional defenses are no longer enough

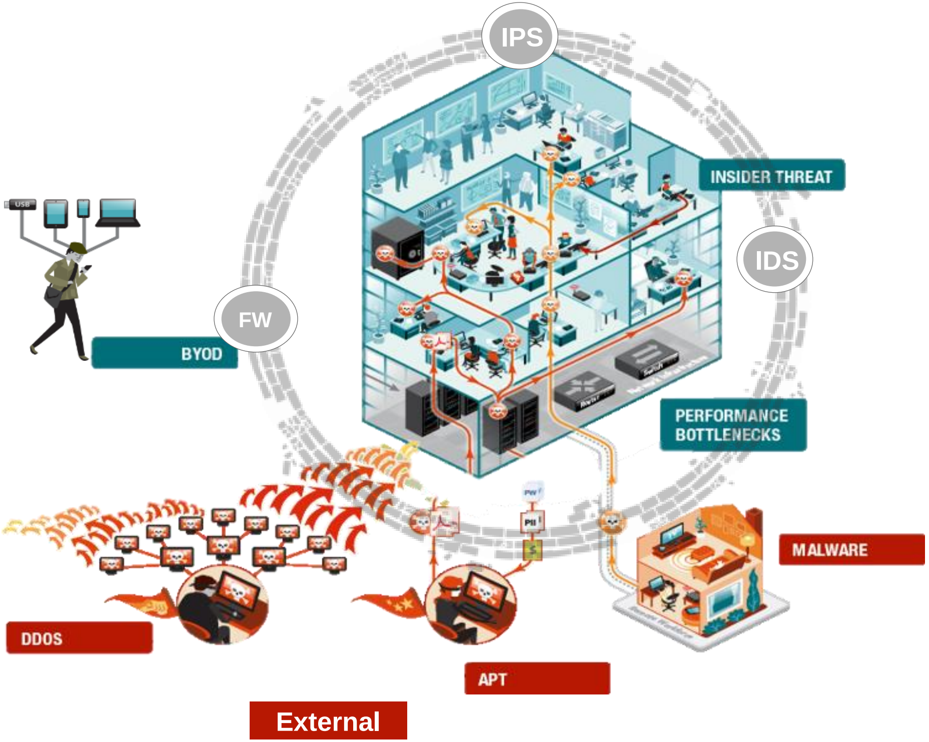
Let’s take a deeper look into today’s TOP Threats



External THREATs

Insider THREATs

External Threats



Next Gen Firewall
Next Gen IPS
Email Security
Web Security
Network Antivirus
Endpoint Antivirus

Enhanced Security & Simplifies Operations & Cost Savings

Superior Network Visibility

Servers, hosts, Mobiles
Applications, OS, Vulnerabilities,

Automated Tuning

Adjust IPS policies automatically based on network changes

Impact Assessment & Correlation

Threat correlation reduces actionable events by up to 99%

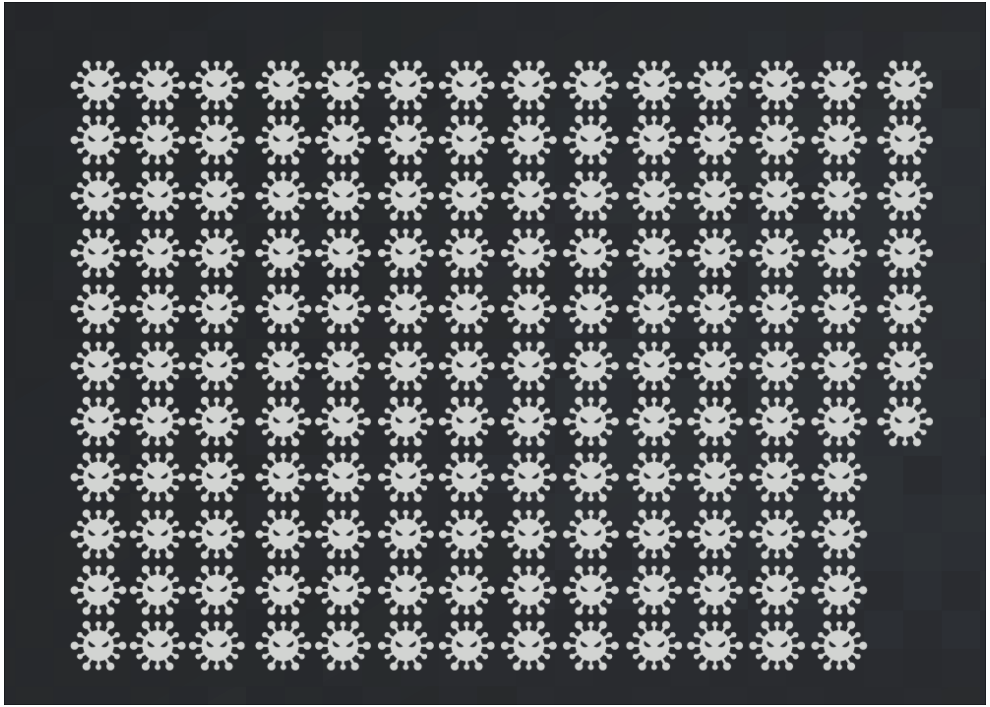
Advanced Malware Protection

Analyses files to block malware

Remediation

Continuous Analysis, Trajectory

Cisco Talos Threat Intelligence



TALOS

1.5 Million

Malware Samples

DAILY

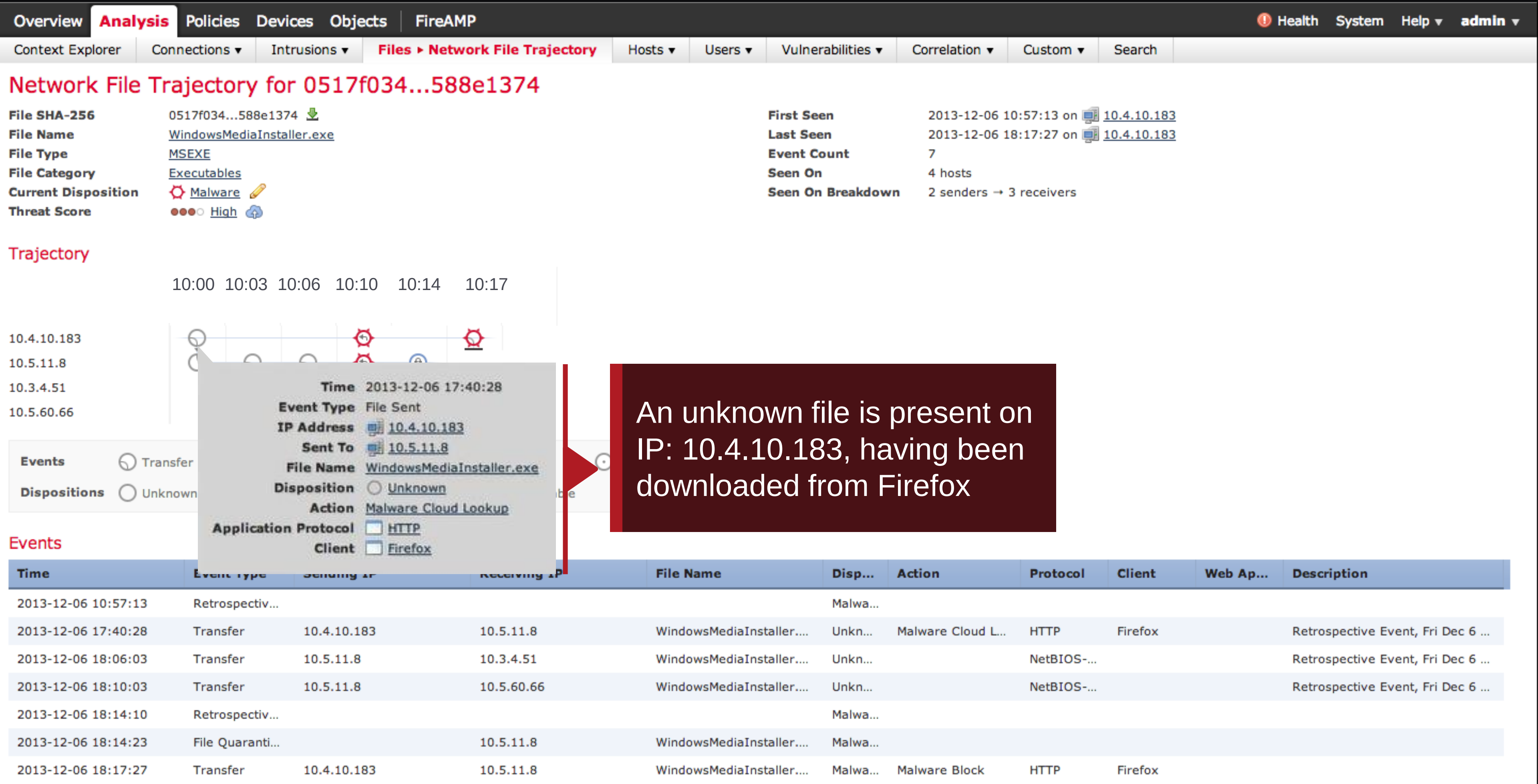
Advanced Malware Protection

Advanced Malware Protection

Analyses files to block malware

Analyses files to detect and block malware

- File Reputation
- Big data analytics
- Continuous analysis
- Dynamic Analysis with Sandboxing (outside-looking-in)



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

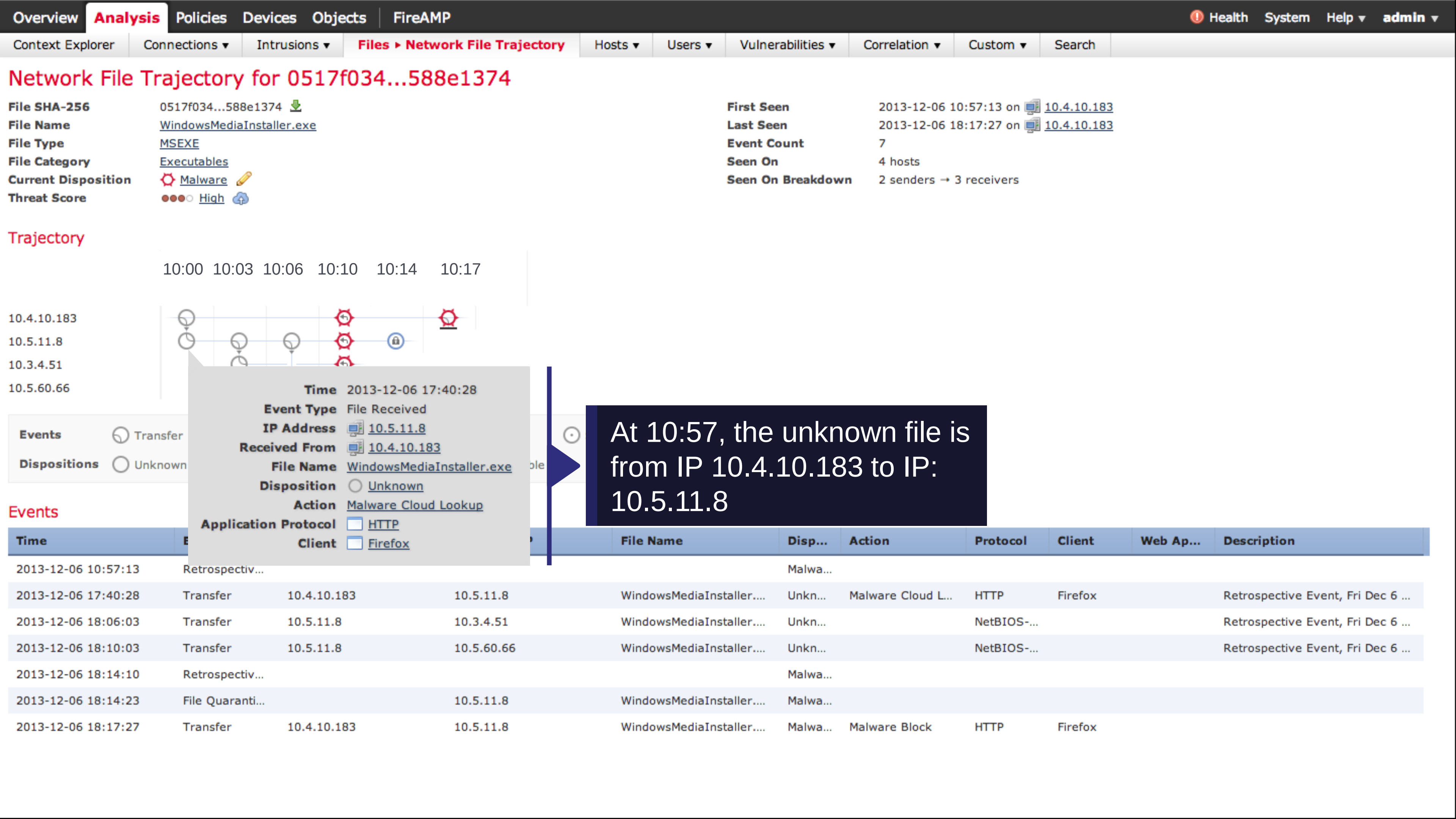
Trajectory

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

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



Network File Trajectory for 0517f034...588e1374

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

Trajectory

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

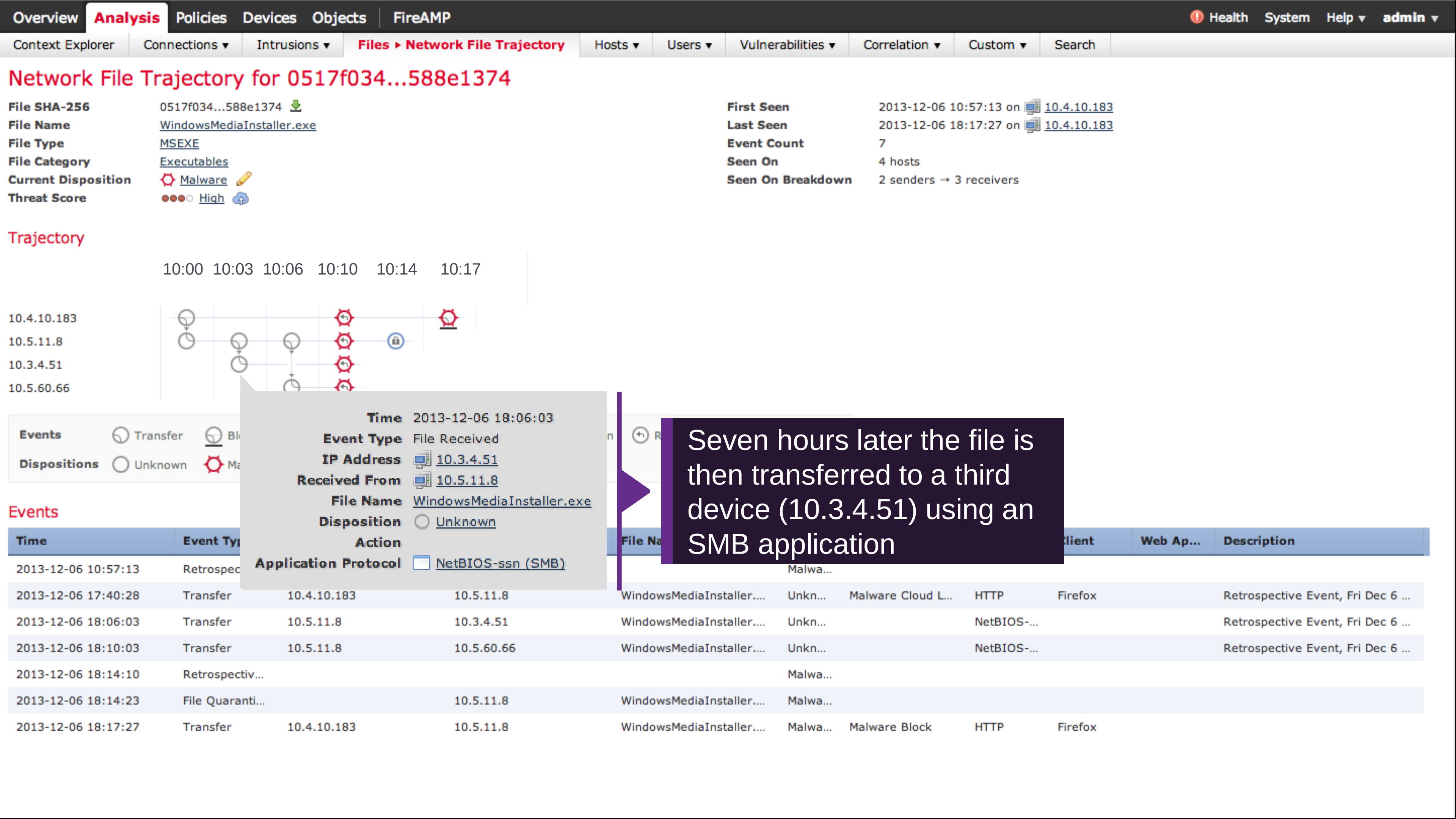
Events ○ Transfer

Dispositions ○ Unknown ble

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

Events

Time	E		P	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

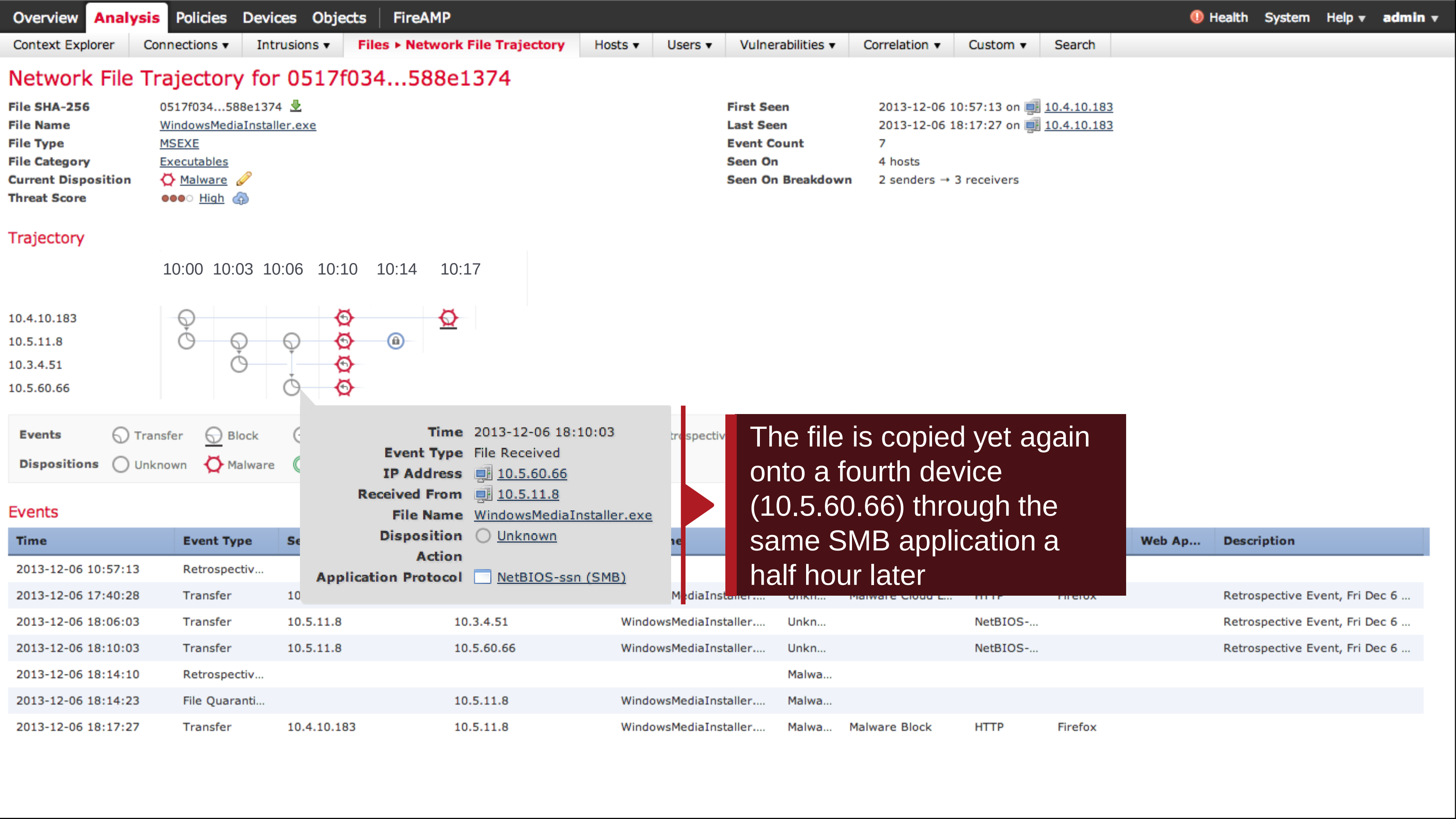
Trajectory

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)

Events

Time	Event Typ			File Na				lient	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		

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



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

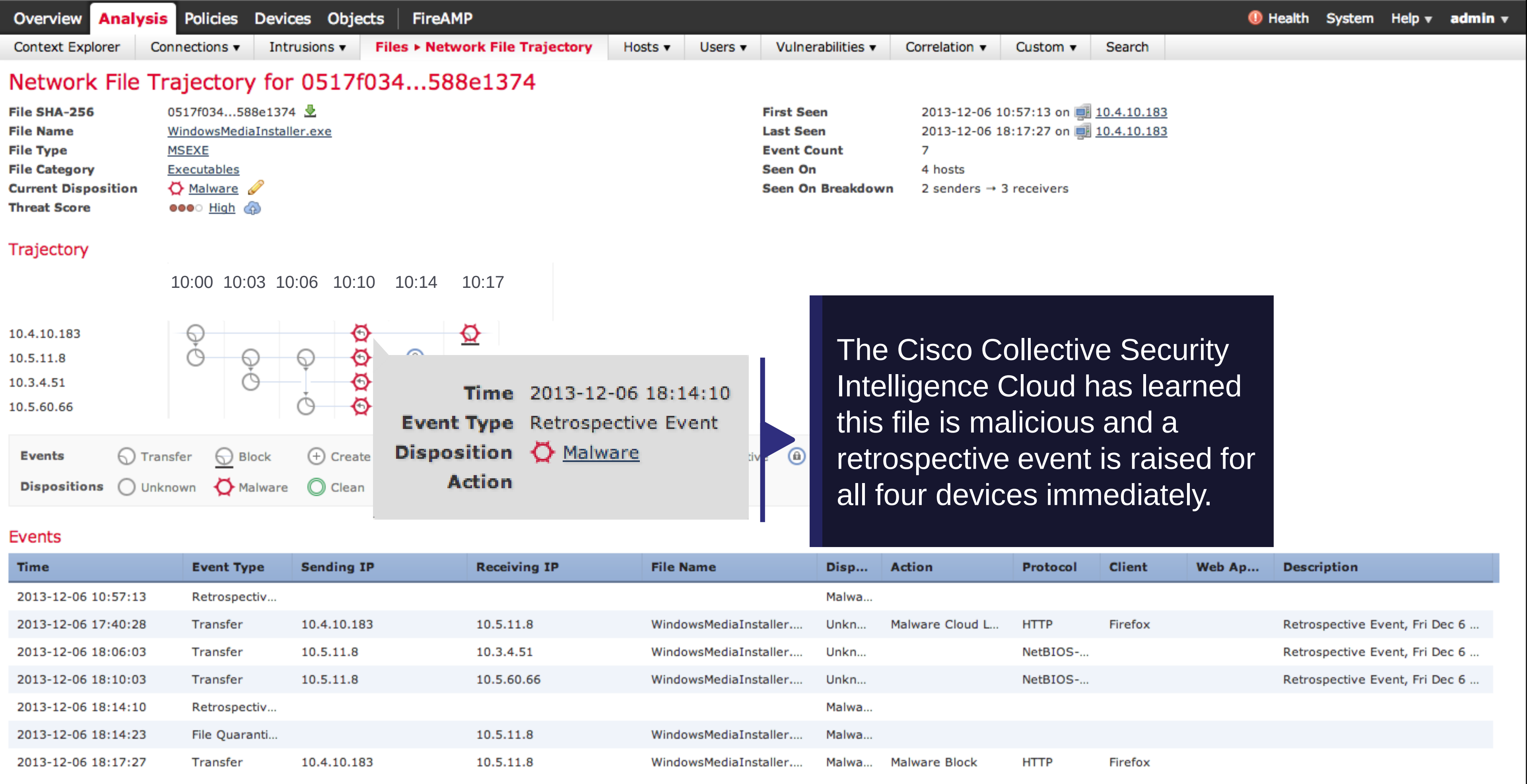
Trajectory

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)

Events

Time	Event Type	Se		ne					Web Ap...	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		

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



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

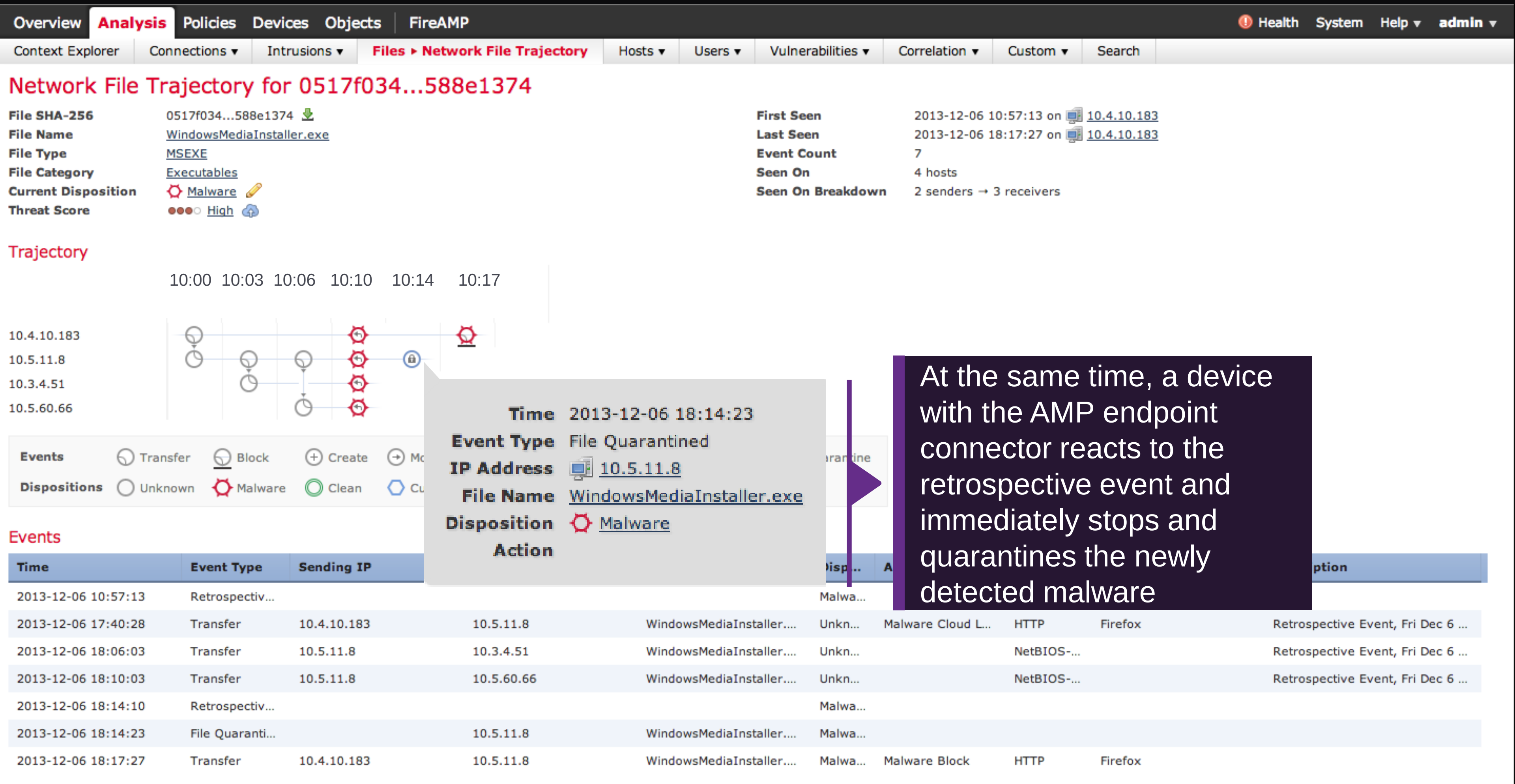
Trajectory

Time	2013-12-06 18:14:10
Event Type	Retrospective Event
Disposition	Malware
Action	

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		

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



Network File Trajectory for 0517f034...588e1374

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

Trajectory

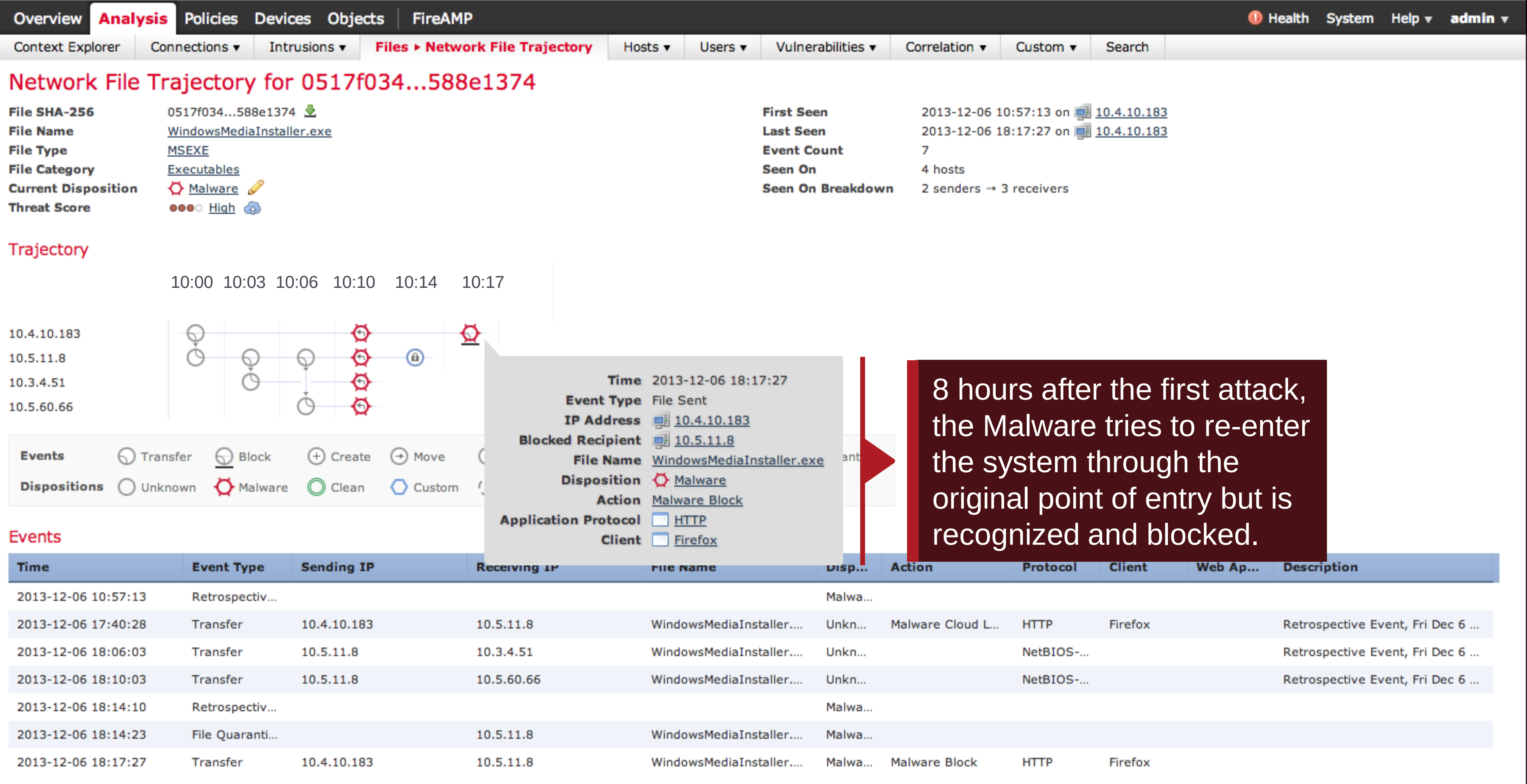
Events	Transfer	Block	Create	Mo	...ara tine
Dispositions	Unknown	Malware	Clean	Cu	

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

Events

Time	Event Type	Sending IP			Disp...	A			...ption
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	

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



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

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

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		

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.

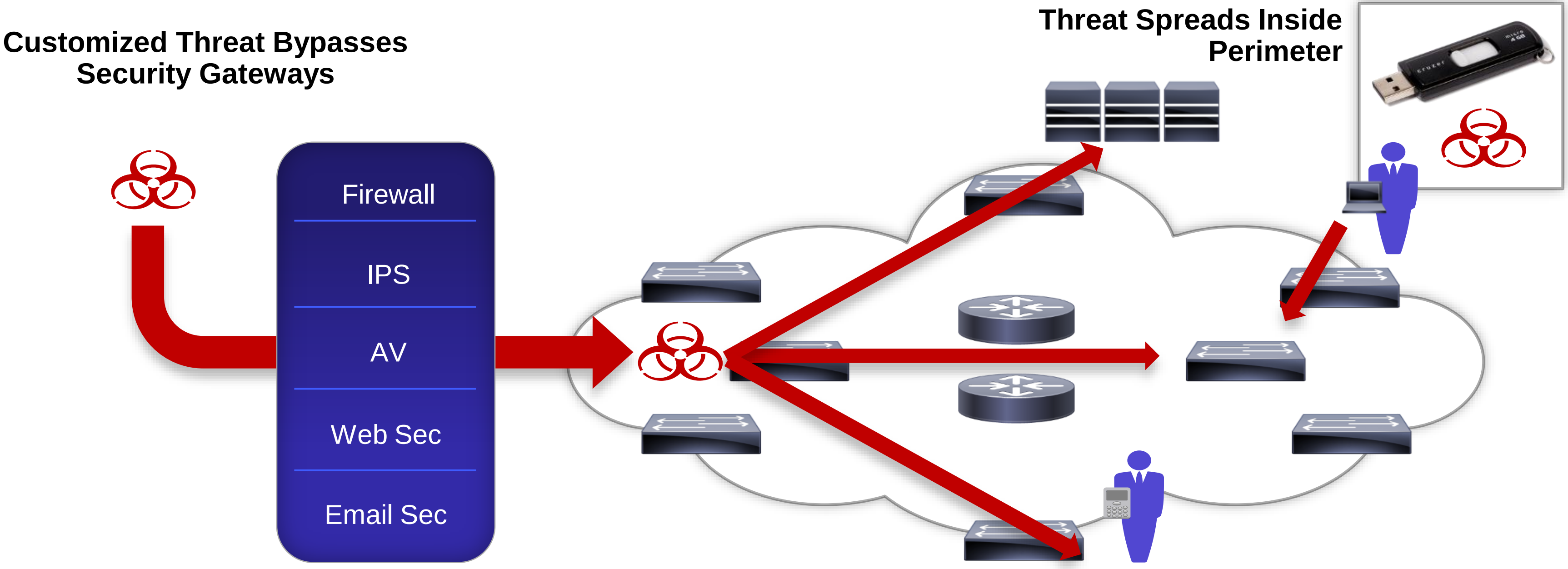
Insider THREATs

One out of four breaches are caused by malicious insiders

INSIDER THREAT
!
Perimeter defenses useless

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

Cisco Cyber Threat Defense


Customized Threat Bypasses Security Gateways
Firewall
IPS
AV
Web Sec
Email Sec
Threat Spreads Inside Perimeter
cruzer
micro 4 GB

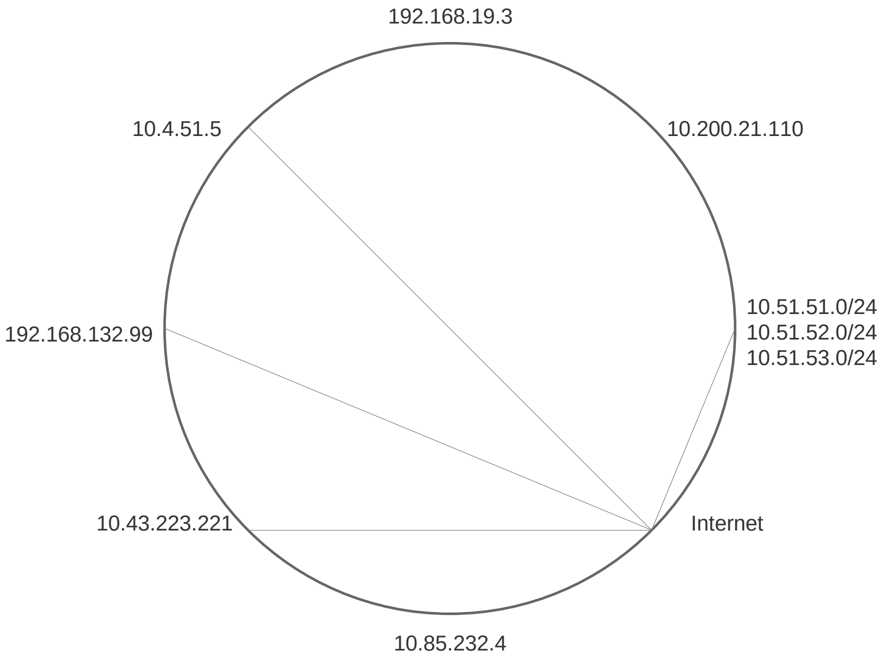
Customized Cyber Threats Evade Existing Security Constructs

Fingerprints of Threat are Found Only in Network Fabric

Network with Only Perimeter Visibility

Visibility available for traffic transiting through perimeter

Many devices in your network without visibility

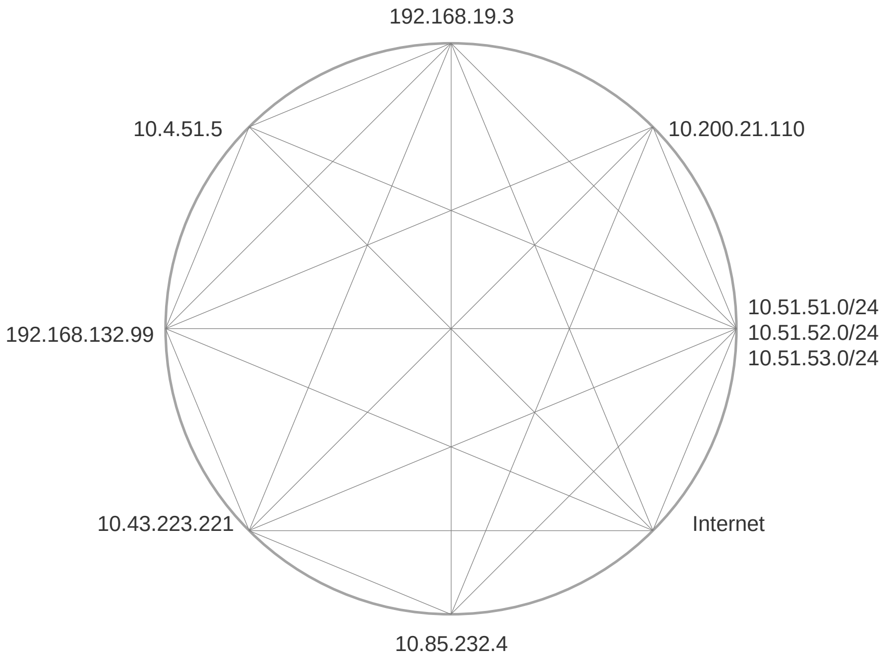


Enabling Visibility Inside Your Network

KNOW
every host

RECORD
every conversation

EVERYTHING
on the network

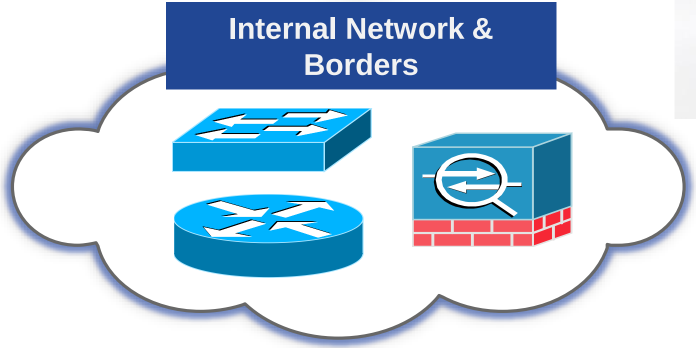


Key Concept - NetFlow

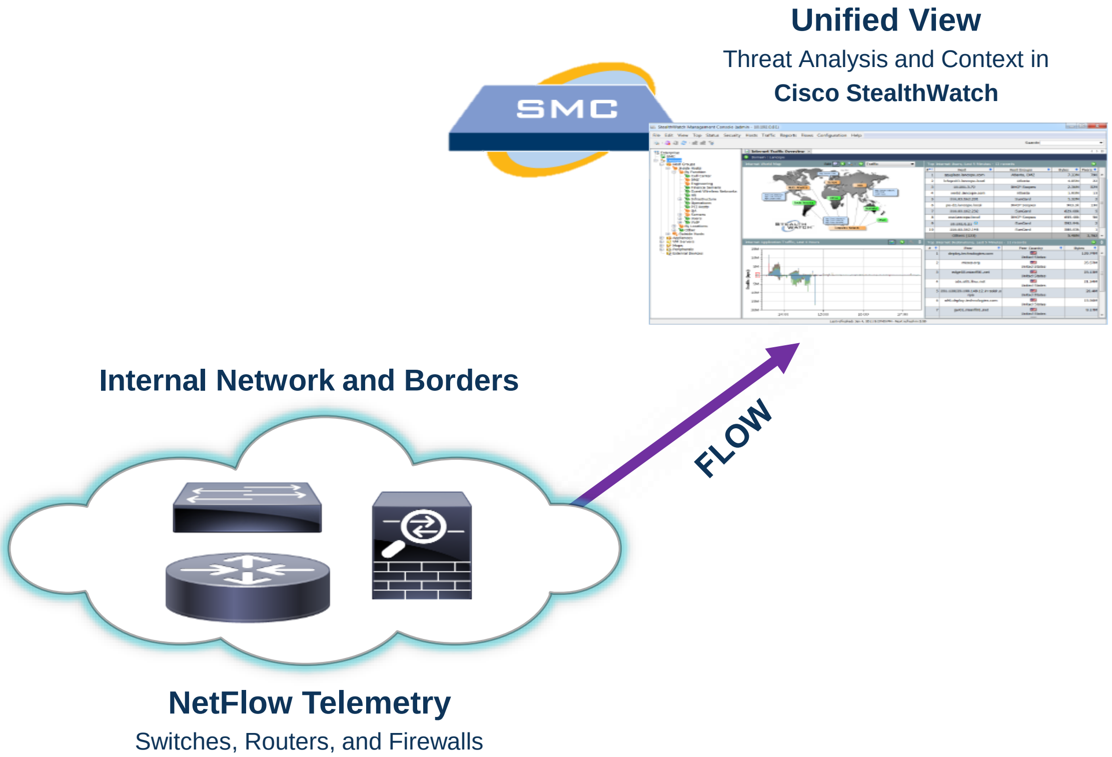
- NetFlow is like a phone bill

NetFlow provides detailed data such as:

- What is talking to what
- Direction of traffic
- over what protocols and ports
- for how long, at what speed
- for what duration
- Volume of traffic
- What nations traffic is going to



Next Generation Cyber Threat Defense



Unified View

Threat Analysis and Context in

Cisco StealthWatch

Internal Network and Borders

NetFlow Telemetry

Switches, Routers, and Firewalls

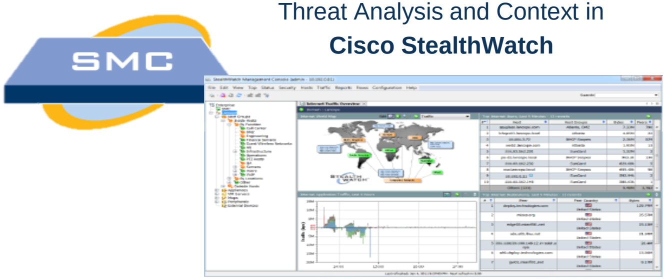
- Aggregating, analyzing NetFlow
- Network Behavior - Baseline
- Anomaly Detection

Next Generation Cyber Threat Defense

Unified View

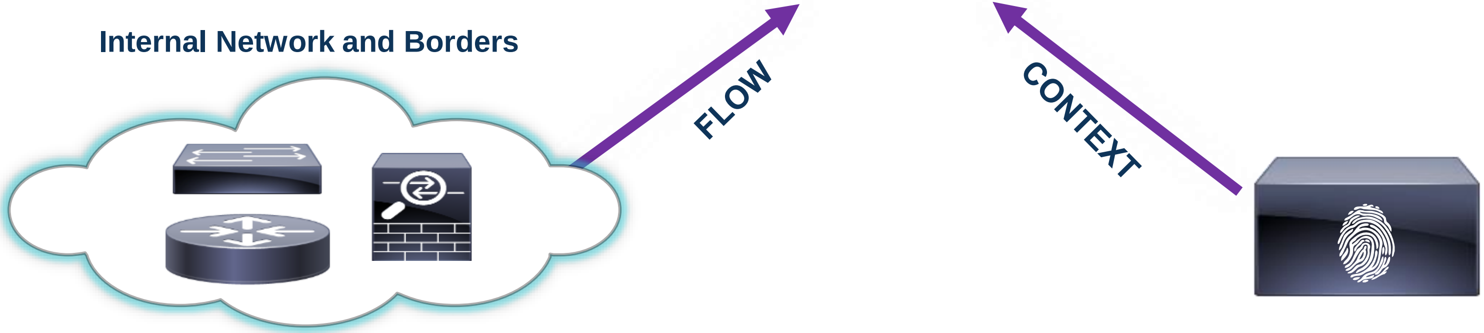
Threat Analysis and Context in

Cisco StealthWatch



- Aggregating, analyzing NetFlow
- Network Behavior - Baseline
- Anomaly Detection

Internal Network and Borders



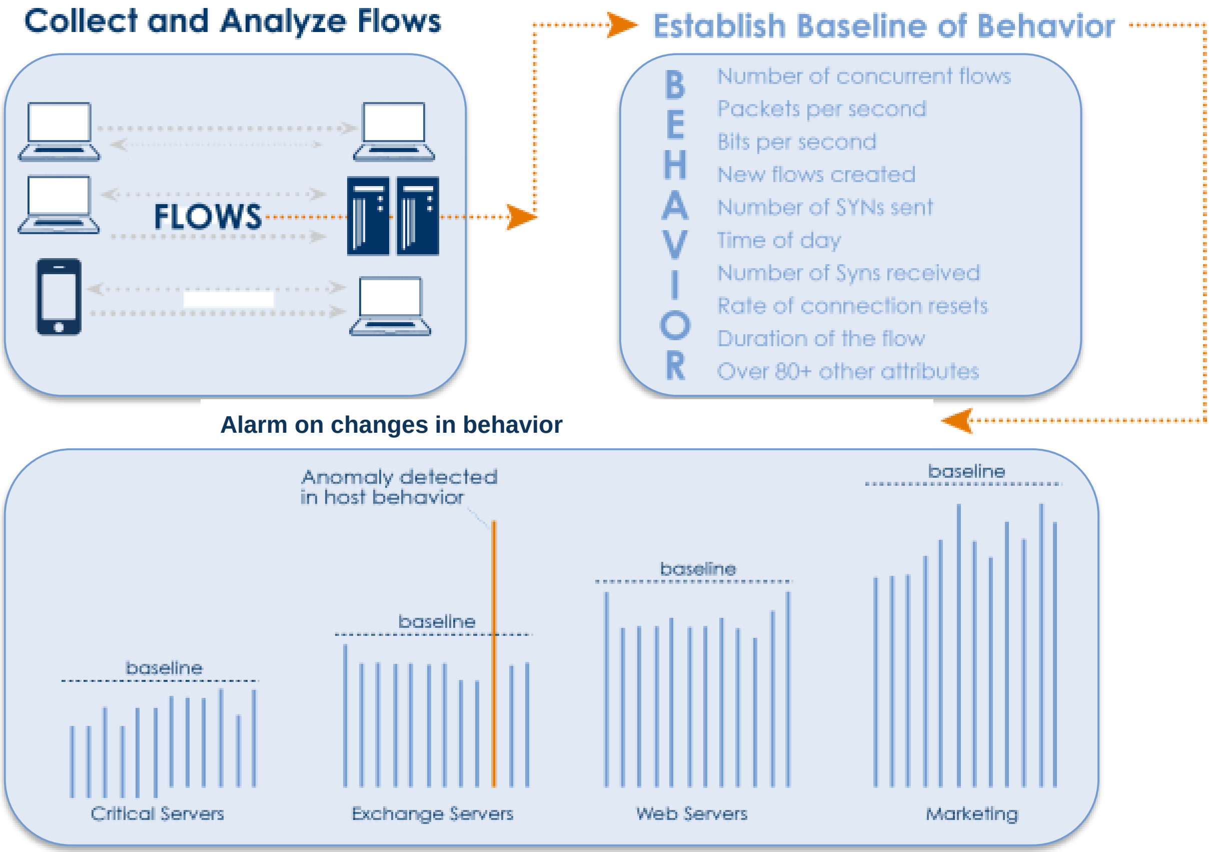
NetFlow Telemetry

Switches, Routers, and Firewalls

Cisco Identity Services Engine

Identity, Device, Posture

Network Behavior– Baseline (Normal)



Collect and Analyze Flows

Establish Baseline of Behavior

BEHAVIOR

- Number of concurrent flows
- Packets per second
- Bits per second
- New flows created
- Number of SYNs sent
- Time of day
- Number of Syns received
- Rate of connection resets
- Duration of the flow
- Over 80+ other attributes

Alarm on changes in behavior

Anomaly Detection

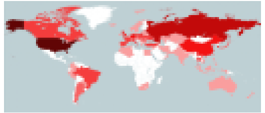
Modern Detection Algorithms

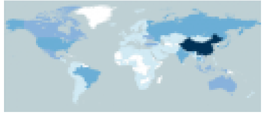
Behavioral Anomaly Research

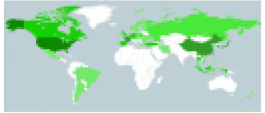
Malware Analysis

Incident Investigations

Research Partnerships





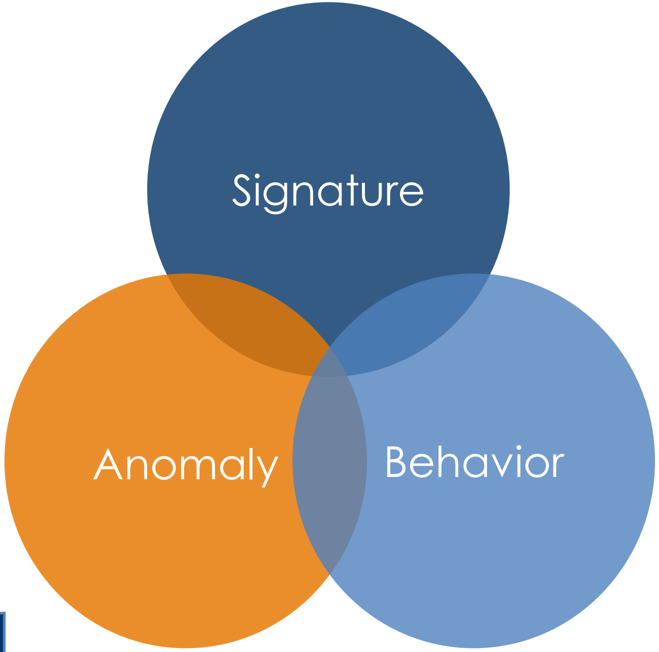


Advanced Detection Methods

Signature IPS, Antivirus, Content Filter

Behavior

Anomaly

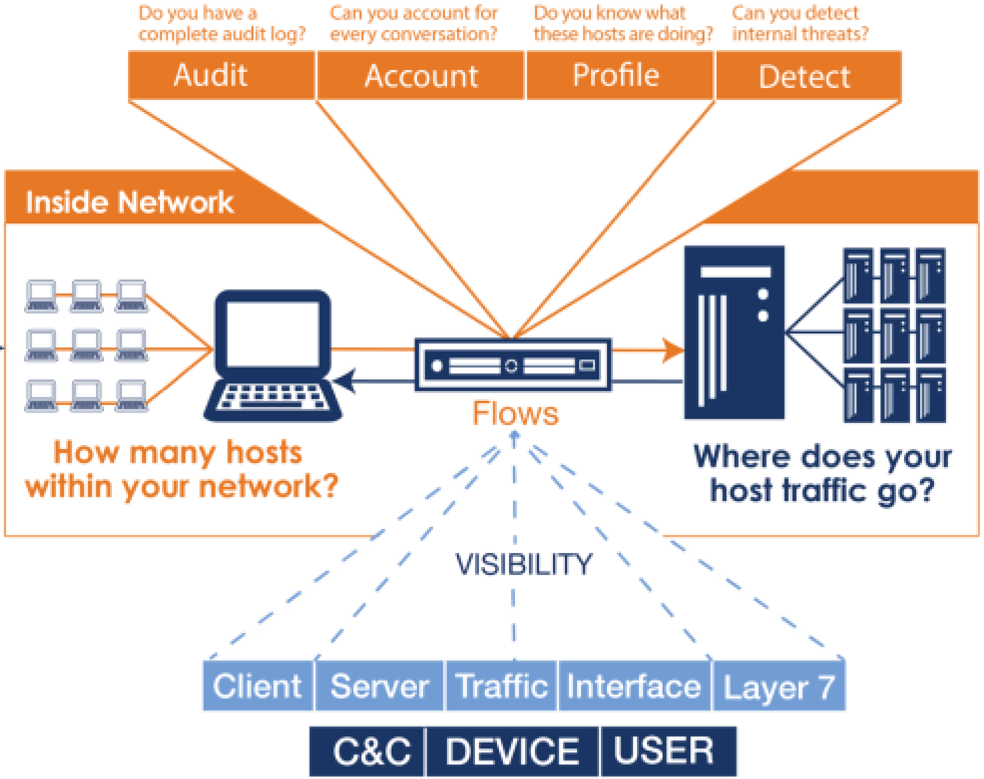


	Signature	Behavior	Anomaly
Known Exploits	**BEST**	Good	Limited
0-day Exploits	Limlted	**BEST**	Good
Credential Abuse	Limited	Limited	**BEST**

Breaking down the Boundaries

Perimeter Defense

Visibility
NGIPS
AMP - Sandboxing
IoC - Correlation


Do you have a complete audit log?
Can you account for every conversation?
Do you know what these hosts are doing?
Can you detect internal threats?
Audit
Account
Profile
Detect
Inside Network
How many hosts within your network?
Flows
Where does your host traffic go?
VISIBILITY
Client
Server
Traffic
Interface
Layer 7
C&C
DEVICE
USER

Consolidation,
Integration,
Automation

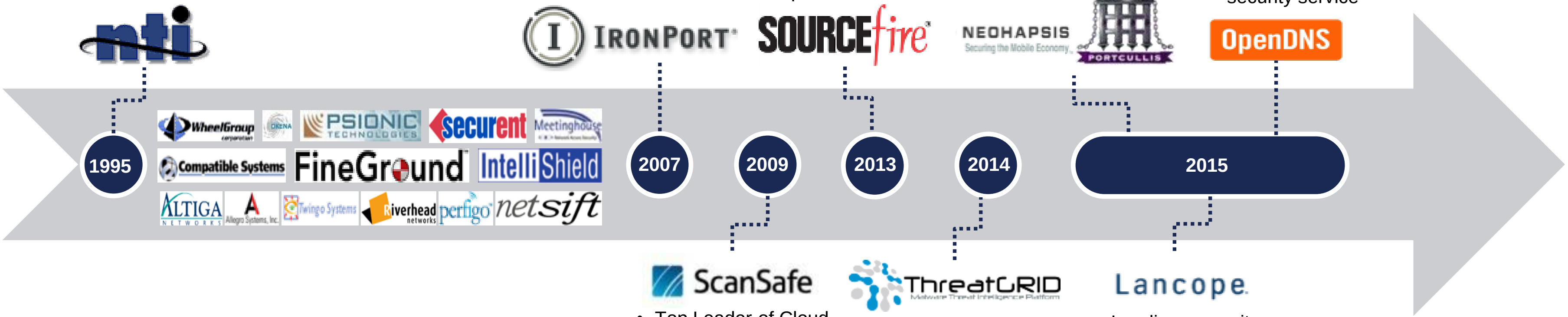
Next Generation Cyber Threat Defense

Increases visibility

Enhances protection

Simplifies operations

Cisco is Investing in Security



- PIX Firewall which was foundation of current ASA-X

- Top Leader of contents security

- Top Leader of Cloud-based Web Security

- Snort®, ClamAV®, Open source projects Founder
- VRT World-class research
- Top Leader of IPS

- Leading Dynamic Malware Analysis (Sandbox)
- Currently Integrated to AMP

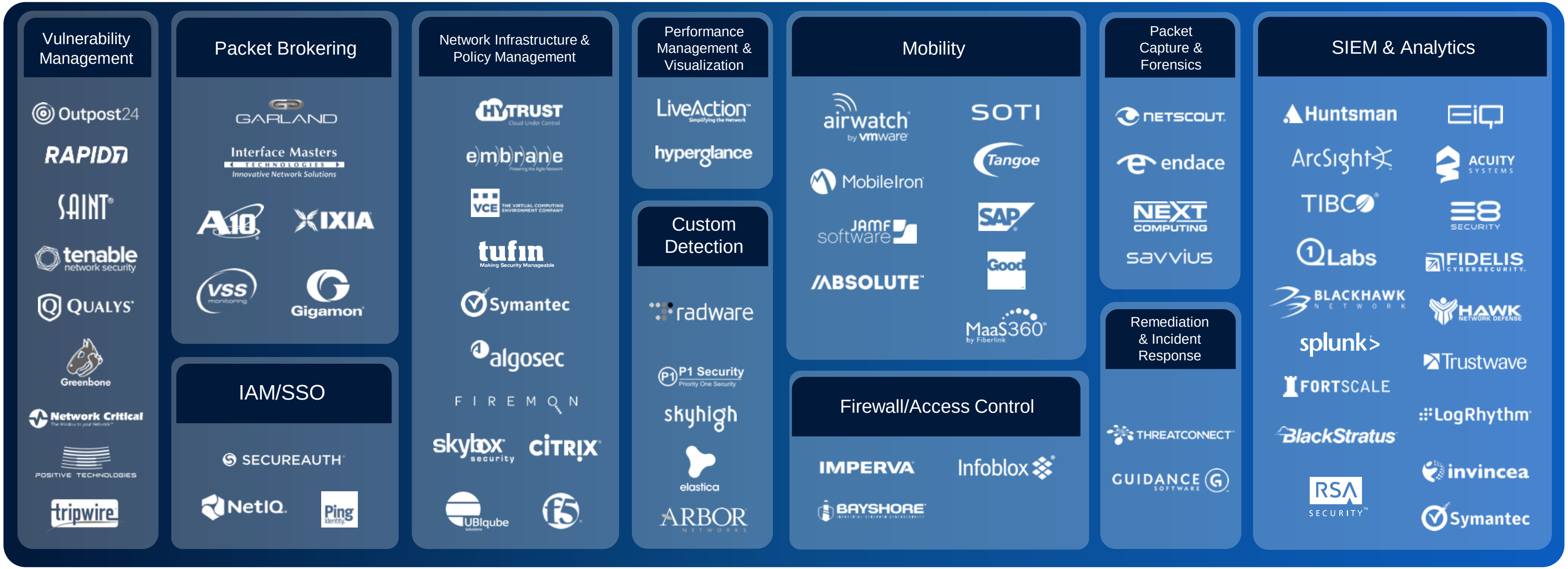
- Top Leaders of security advisory services
- Provides risk management and compliance to Fortune 500 customers

- Cloud based DNS security service

- Leading security analytics platform to defend against advanced cyber threats

Ecosystem and Integration

Combined API Framework



Vulnerability Management

- Outpost24
- RAPID7
- SAINT
- tenable network security
- QUALYS
- Greenbone
- Network Critical
- POSITIVE TECHNOLOGIES
- tripwire

Packet Brokering

- GARLAND
- Interface Masters Technologies Innovative Network Solutions
- A10
- IXIA
- VSS monitoring
- Gigamon

IAM/SSO

- SECUREAUTH
- NetIQ
- Ping Identity

Network Infrastructure & Policy Management

- HYTRUST Cloud Under Control
- embrane Powering the Agile Network
- VCE The Virtual Computing Environment Company
- tufin Making Security Manageable
- Symantec
- algosec
- FIREMON
- skybox security
- CITRIX
- UBIqube
- f5

Performance Management & Visualization

- LiveAction Simplifying the Network
- hyperglance

Custom Detection

- radware
- P1 Security Priority One Security
- skyhigh
- elastica
- ARBOR NETWORKS

Mobility

- airwatch by vmware
- SOTI
- MobileIron
- Tangoe
- JAMF software
- SAP
- ABSOLUTE
- Good
- MaaS360 by Fiberlink

Firewall/Access Control

- IMPERVA
- Infoblox
- BAYSHORE

Packet Capture & Forensics

- NETSCOUT
- endace
- NEXT COMPUTING
- savvius

Remediation & Incident Response

- THREATCONNECT
- GUIDANCE SOFTWARE

SIEM & Analytics

- Huntsman
- EIQ
- ArcSight
- ACUITY SYSTEMS
- TIBCO
- E8 SECURITY
- 1Labs
- FIDELIS CYBERSECURITY
- BLACKHAWK NETWORK
- HAWK NETWORK DEFENSE
- splunk>
- Trustwave
- FORTSCALE
- LogRhythm
- BlackStratus
- invincea
- RSA SECURITY
- Symantec

cisco

Market Recognition

"Cisco Is Going on a Security Push" FORTUNE

SC MAGAZINE AWARDS 2016 Honored in the U.S.

BEST SECURITY COMPANY

IDC

Cisco's Security Everywhere... "that's pretty brilliant"

Goldman Sachs

Cisco…best traction among security vendors

BT

Opportunity for Cisco and BT together to be a $100 million account within 18 months

– CEO
BT Security Group

NSS LABS

Security Value Map Leader: NGFW, NGIPS and Breach Detection Systems (AMP)

FORRESTER®

Cisco's Network Security Portfolio finally stands on its own merit

Cisco is building the foundation for the Security industry for the upcoming 20-50 years, and making smart bets…

– Marcos Ortiz
Senior Product Manager, Big Data Apps and Cybersecurity