Das Bild kann zurzeit nicht angezeigt werden.

Cisco ASA with FirePOWER Services

TDM

Thomas Jankowsky

Consulting Systems Engineer

May 2015

Introduction

Industry’s First Threat-Focused Next-Generation Firewall (NGFW)

#1 Cisco® security announcement of the year

Proven Cisco ASA firewalling

+

Industry-leading NGIPS and AMP

=

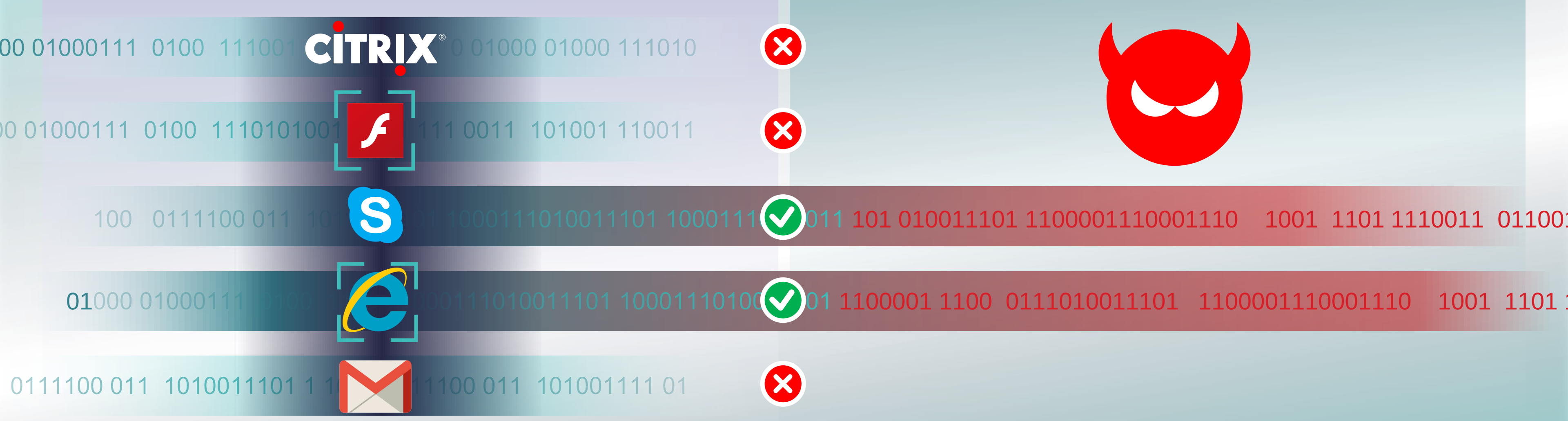
Cisco ASA with FirePOWER™ Services

- Integrate defense layers so that organizations get the best visibility
- Help enable dynamic controls to automatically adapt
- Protect against advanced threats across the entire attack continuum

The Problem with Legacy Next-Generation Firewalls

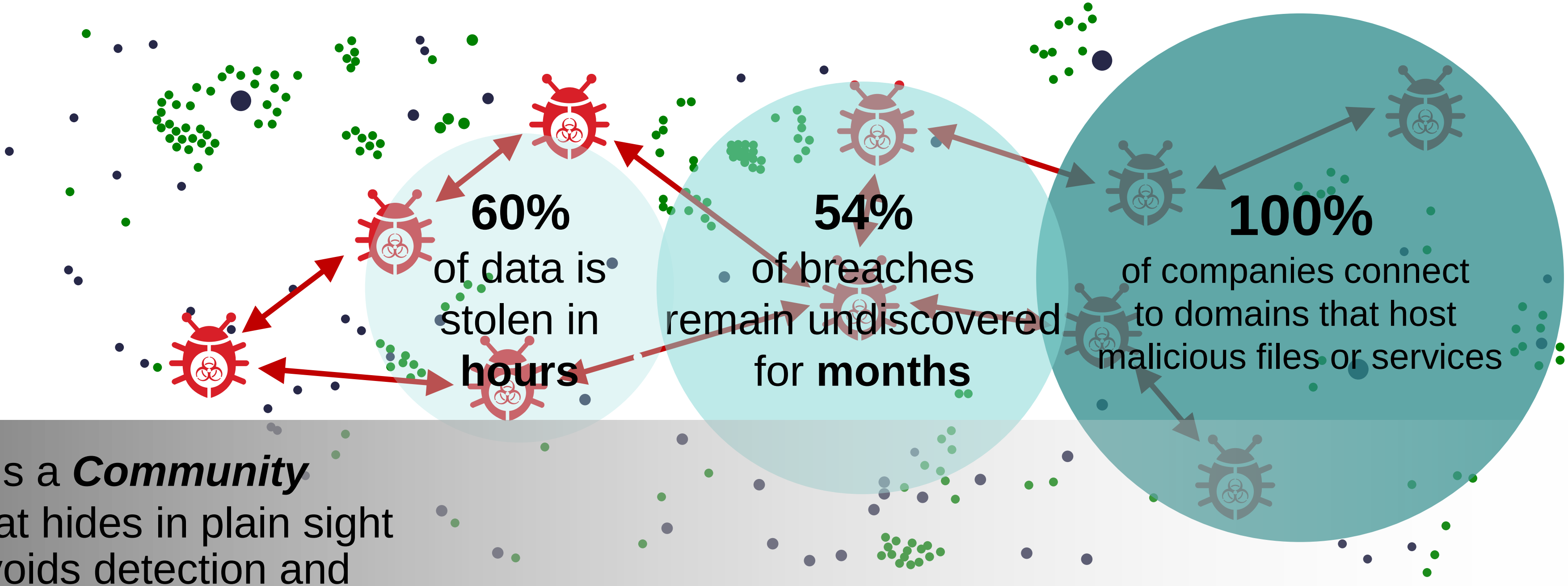
Focus on the Apps…

…But Miss the Threat



Legacy NGFWs can reduce attack surface area but advanced malware often evades security controls.

Threat Landscape Demands more than Application Control



60%
of data is stolen in **hours**

54%
of breaches remain undiscovered for **months**

100%
of companies connect to domains that host malicious files or services

It is a ***Community***
that hides in plain sight
avoids detection and
attacks swiftly

Defensive, In-Depth Security Alone Is Not Enough

Siloed Approach

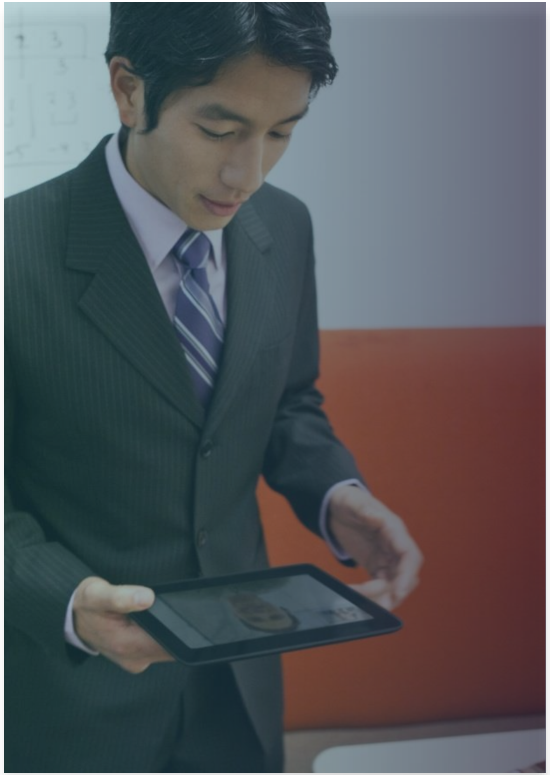
Increased complexity and reduced effectiveness

Poor Visibility

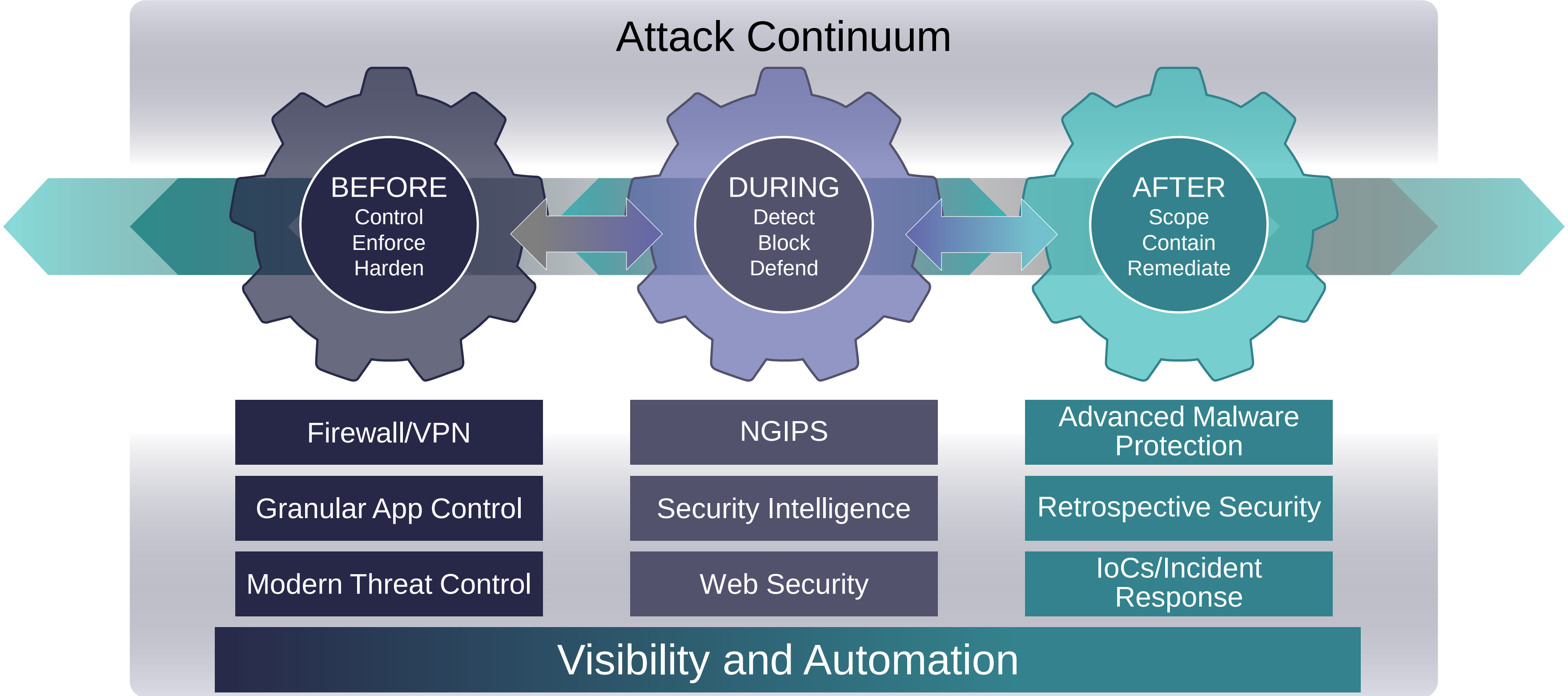
Undetected multivector and advanced threats

Manual and Static

Slow, manual, and inefficient response



Integrated Threat Defense Across the Attack Continuum



Attack Continuum

BEFORE
Control
Enforce
Harden

DURING
Detect
Block
Defend

AFTER
Scope
Contain
Remediate

Firewall/VPN

Granular App Control

Modern Threat Control

NGIPS

Security Intelligence

Web Security

Advanced Malware Protection

Retrospective Security

IoCs/Incident Response

Visibility and Automation

Cisco ASA with FirePOWER Services

Industry's First Adaptive, Threat-Focused NGFW

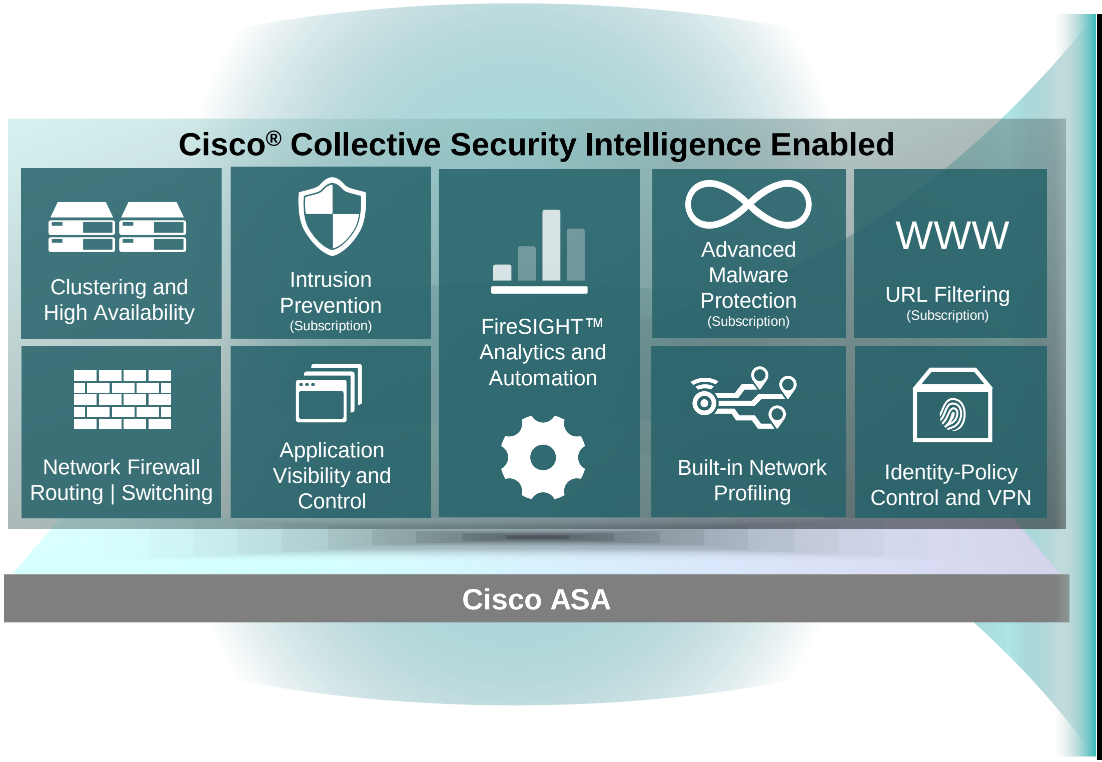
→ Features

- Cisco® ASA firewalling combined with Sourcefire® next-generation IPS
- Integrated threat defense over the entire attack continuum
- Best-in-class security intelligence, application visibility and control (AVC), and URL filtering

→ Benefits

- Superior, multilayered threat protection
- Superior network visibility
- Advanced malware protection
- Reduced cost and complexity

Superior Integrated and Multilayered Protection



Cisco® Collective Security Intelligence Enabled
Clustering and High Availability
Intrusion Prevention (Subscription)
FireSIGHT™ Analytics and Automation
Advanced Malware Protection (Subscription)
WWW
URL Filtering (Subscription)
Network Firewall Routing | Switching
Application Visibility and Control
Built-in Network Profiling
Identity-Policy Control and VPN
Cisco ASA

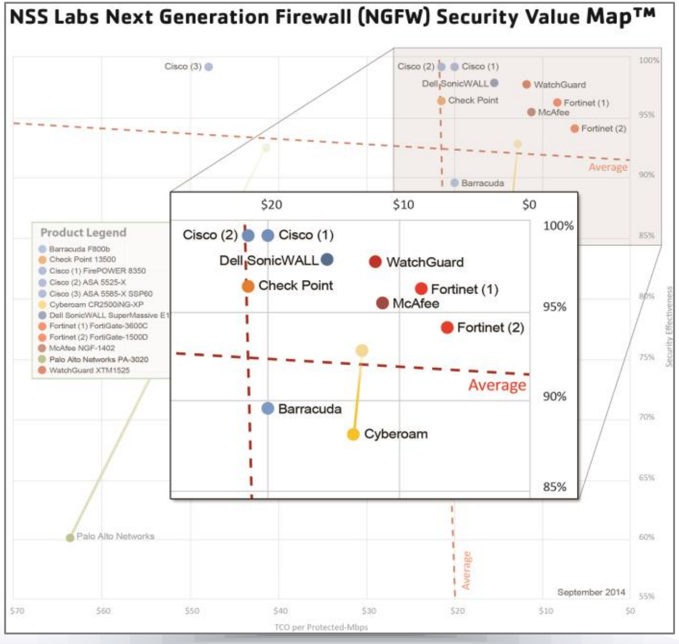
- World's most widely deployed, enterprise-class, ASA stateful firewall
- Granular Cisco Application Visibility and Control (AVC)
- Industry-leading FirePOWER™ next-generation IPS (NGIPS)
- Reputation- and category-based URL filtering
- Advanced malware protection

Cisco FirePOWER Brings Superior Network Visibility

	Threats	Users	Web Applications	Application Protocols	File Transfers	Malware	Command and Control Servers	Client Applications	Network Servers	Operating Systems	Routers and Switches	Mobile Devices	Printers	VoIP Phones	Virtual Machines
Cisco® FirePOWER Services	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Typical IPS	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Typical NGFW	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗

NSS Labs: Next-Generation Firewall Security Value Map

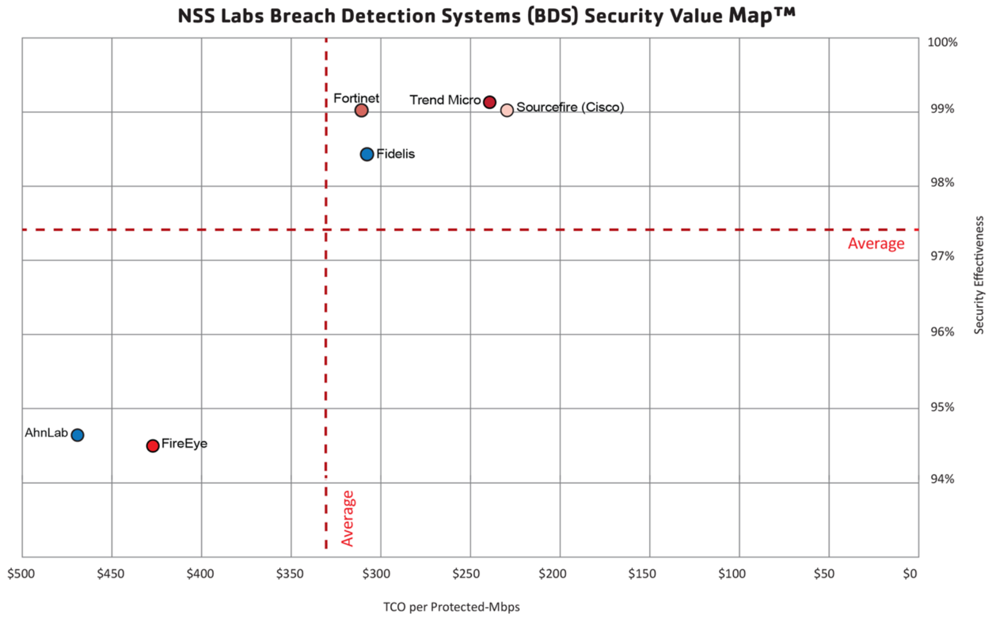
The NGFW Security Value Map shows the placement of Cisco® ASA with FirePOWER Services and the FirePOWER™ 8350 as compared to other vendors. All products achieved 99.2 percent in security effectiveness. Now customers can be confident they'll get the best protections possible, regardless of deployment.


NSS Labs Next Generation Firewall (NGFW) Security Value Map™

Source: NSS Labs 2014

NSS Labs: Breach Detection Systems Security Value Map

Cisco® Advanced Malware Protection (AMP) has the lowest TCO of any product tested. It is also a a leader in security effectiveness, achieving detection of 99 percent of all tested attacks. AMP excelled in time to detection, catching threats faster than competing breach detection systems.

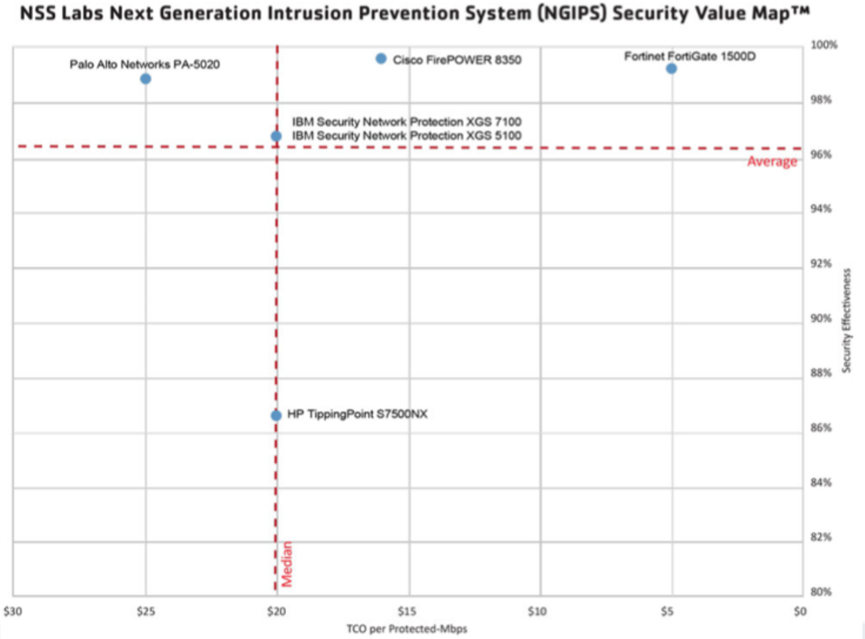


Source: NSS Labs 2014

NSS Labs: Next-Generation IPS Security Value Map

Based on individual and comparative testing of vendors in the IPS market Cisco FirePOWER™ NGIPS* provides the best threat protection possible (99.5%) while also being 100% effective in identifying and defeating evasion techniques.

* Formerly Sourcefire FirePOWER


NSS Labs Next Generation Intrusion Prevention System (NGIPS) Security Value Map™

Source: NSS Labs 2012

Cisco ASA with FirePOWER Services

Base Hardware and Software

- New ASA 5585-X Bundle SKUs with FirePOWER Services Module
- New ASA 5500-X SKUs running FirePOWER Services Software
- FirePOWER Services Spare Module/Blade for ASA 5585-X Series
- FirePOWER Services Software
- Hardware includes Application Visibility and Control (AVC)

Security Subscription Services

- IPS, URL, Advanced Malware Protection (AMP) Subscription Services
- One- and Three-Year Term Options

Management

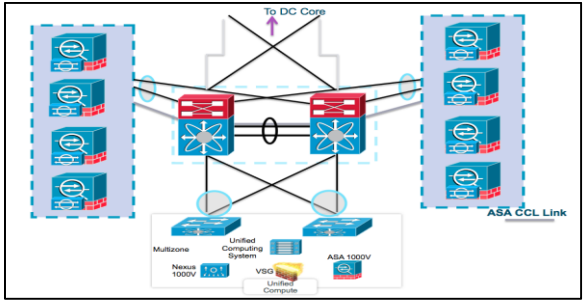
- FireSIGHT Management Center (HW Appliance or Virtual)
- Cisco Security Manager (CSM) or ASDM

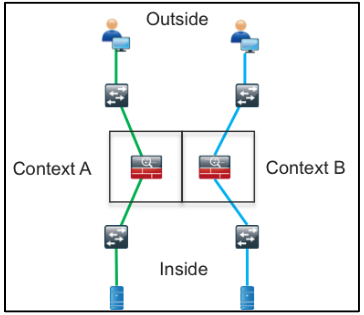
Support

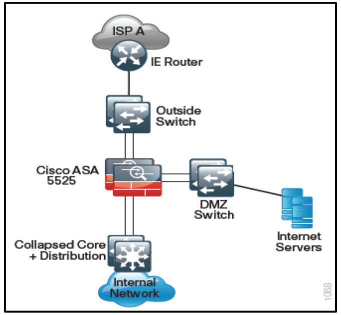
- SmartNET
- Software Application Support plus Upgrades

Performance and Deployment

FirePOWER Services Support All Current ASA Deployment Models







Clustering for linear scalability

Up to 16x ASA in cluster

Eliminates Asymmetrical traffic issues

Each FirePOWER Services module inspects traffic independently

Multi-context mode for policy flexibility

Each ASA Interface appears as a separate interface to FirePOWER Services module

Allows for granular policy enforcement on both ASA and FirePOWER services

HA for increased redundancy

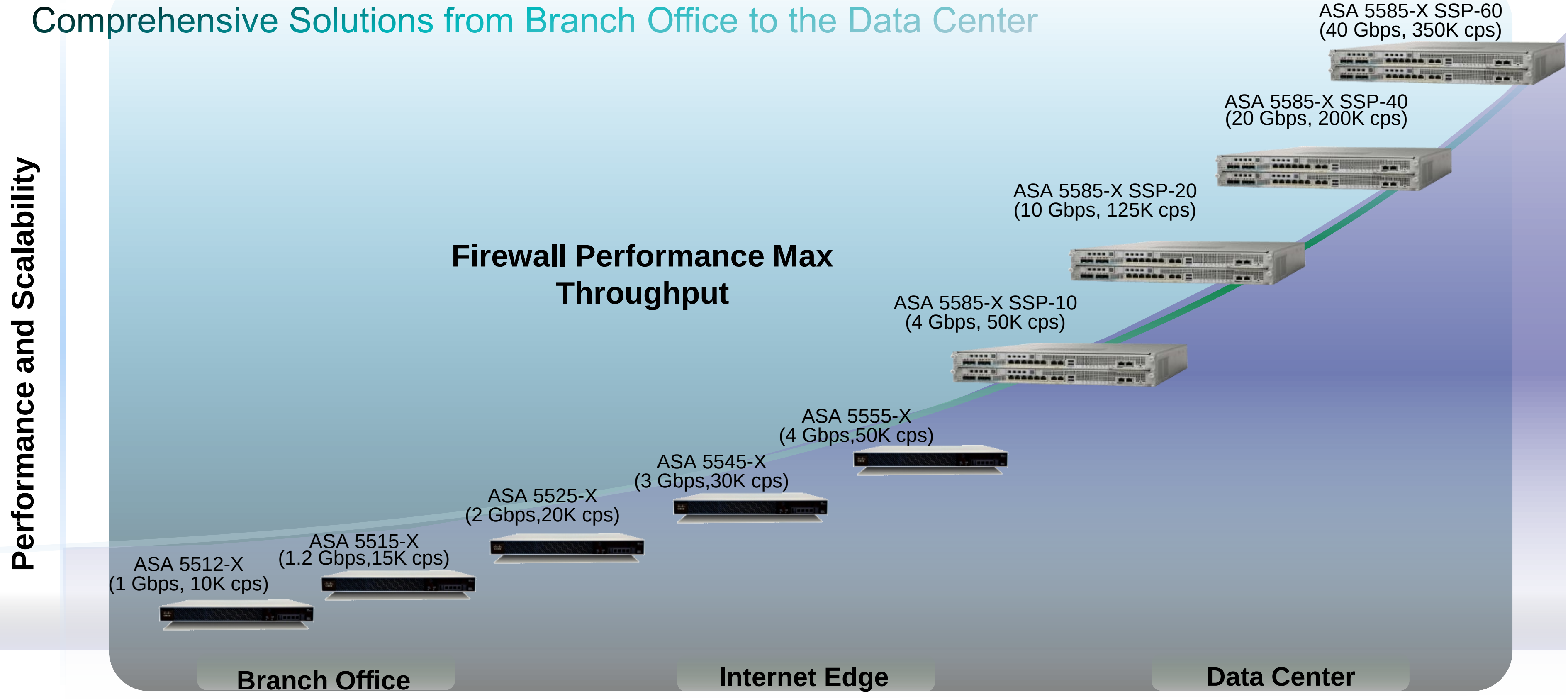
Redundancy and state sharing (A/S & A/A pair)

L2 and L3 designs

*State sharing does not occur between FirePOWER Services Modules

Cisco ASA 5500-X Series Portfolio

Comprehensive Solutions from Branch Office to the Data Center



ASA 5585-X SSP-60
(40 Gbps, 350K cps)

ASA 5585-X SSP-40
(20 Gbps, 200K cps)

ASA 5585-X SSP-20
(10 Gbps, 125K cps)

Firewall Performance Max Throughput

ASA 5585-X SSP-10
(4 Gbps, 50K cps)

ASA 5555-X
(4 Gbps,50K cps)

ASA 5545-X
(3 Gbps,30K cps)

ASA 5525-X
(2 Gbps,20K cps)

ASA 5515-X
(1.2 Gbps,15K cps)

ASA 5512-X
(1 Gbps, 10K cps)

FirePOWER Services for ASA: Data Sheet Performance

- Maximum Throughput numbers are used to compare Data Sheets, they should NEVER be used for sizing guidance.
- Maximum Throughput numbers can be achieved using different traffic profiles or different configurations. Typically neither reflects how the device will be used in a customers environment.

Model	5512-X	5515-X	5525-X	5545-X	5555-X	5585-10	5585-20	5585-40	5585-60
Maximum Application Control Throughput in Mbps	300	500	1100	1500	1750	4500	7000	10000	15000
Maximum Application Control and IPS Throughput in Mbps	150	250	650	1000	1250	2000	3500	6000	10000

FirePOWER Services for ASA: Sizing Guidance

440 byte HTTP Transactional test in Mbps

IPS uses Balanced Profile, AVC uses Network Discovery: Applications

Model	5512-X	5515-X	5525-X	5545-X	5555-X	5585-10	5585-20	5585-40	5585-60
FirePOWER IPS or AVC (1 Service)	100	150	375	575	725	1200	2000	3500	6000
FirePOWER IPS + AVC (2 Services)	75	100	255	360	450	800	1200	2100	3500
FirePOWER IPS+AVC+AMP (3 Services)	60	85	205	310	340	550	850	1500	2300

As with all performance discussions, YOUR MILEAGE MAY VARY!!

FireSIGHT Management Center Models

	750	1500	2000	3500	4000	Virtual
Max. Devices Managed	10	35	70	150	300	Virtual FireSIGHT Management Center Up to 25 Managed Devices
Event Storage	100 GB	125 GB	1.8 TB	400 GB	4.8/6.3 TB	
Max. Network Map (hosts / users)	2K/2K	50K/50K	150K/150K	300K/300K	600K/600K	Virtual FireSIGHT Management Center offerings limited to 2 or 10 Managed Devices **FS-VMW-2-SW-K9** **FS-VMW-10-SW-K9** **Only for FirePOWER Services for ASA devices.**
Events per Sec (EPS)	2000	6000	12000	10000	20000	

ASA Services Packet Flow

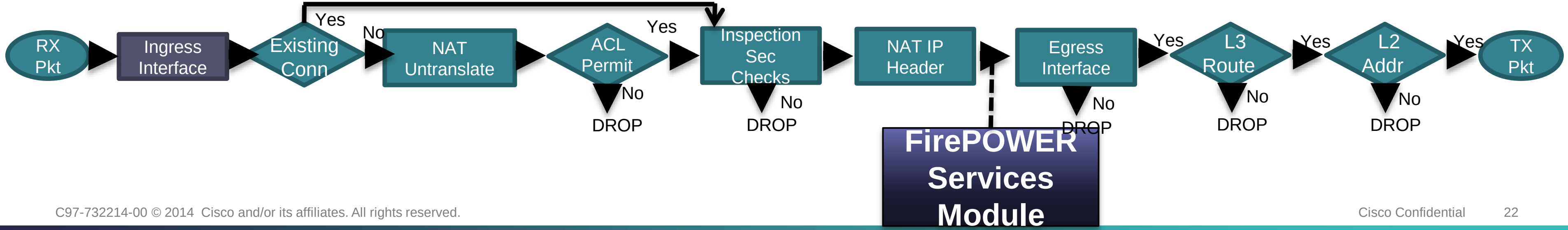
Packet Flow Overview

- ➢ Packet flow between the solution components
  1. Ingress processing – inbound ACLs, IP defragmentation, TCP normalization, TCP intercept, protocol inspection, clustering/HA traffic control, VPN decryption, etc.
  2. Sourcefire Services processing – URL filtering, AVC, NGIPS, AMP, etc.
  3. Egress processing – outbound ACLs, NAT, routing, VPN encryption, etc.
- ➢ Packets are redirected to the FirePOWER Services module using the Cisco ASA Modular Policy Framework (MPF)
  - MPF is a well known component of ASA architecture.
  - MPF supports fail-open, fail-closed and monitor only options
  - MPF class map, policy map and service policy determine which traffic is send to the FirePOWER Services module
- ➢ Example of MPF configuration to send all traffic to the FirePOWER Services module:

```
policy-map global_policy
        class class-default
         sfr fail-open
         service-policy global_policy global
```

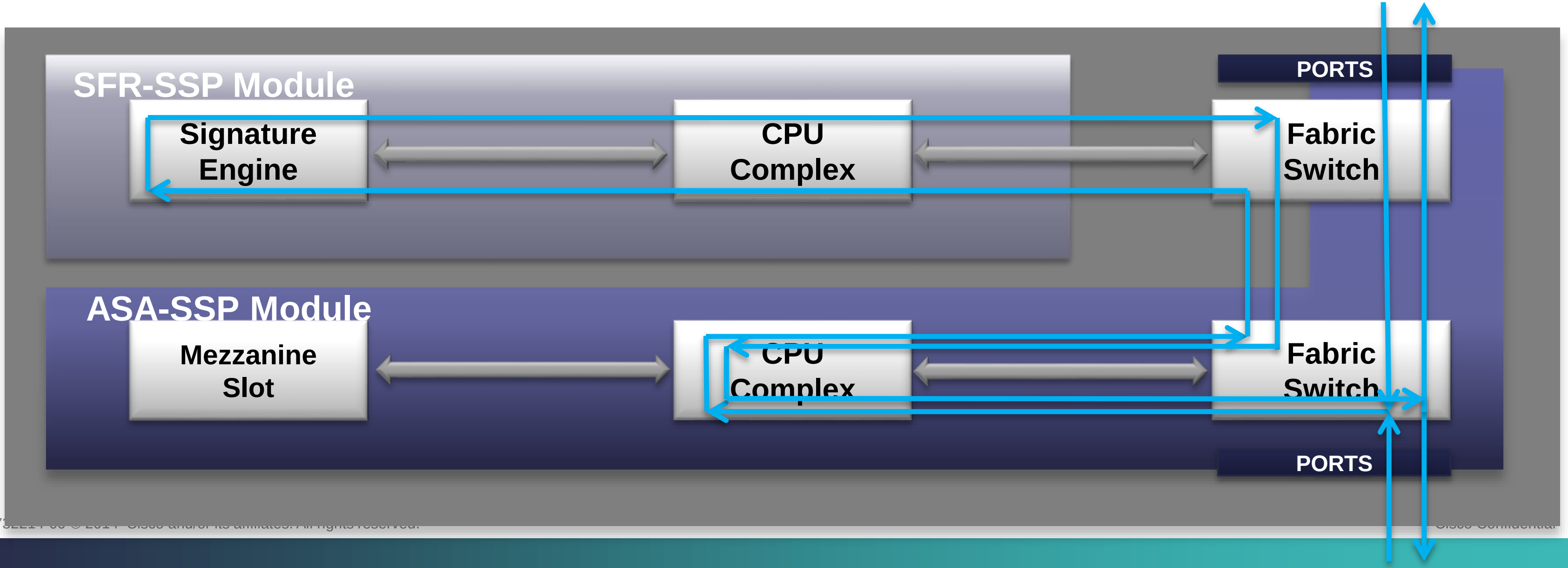
Packet Processing Order of Operations

- ASA Module processes all ingress packets against ACL, Connection tables, Normalization and CBAC before traffic is forwarded to the FirePOWER Services module
- ASA provides flow normalization and context-aware selection/filtering to the FirePOWER Services
- Clustered ASA provides flow symmetry and HA to the FirePOWER Services
- Packets and flows are not dropped by FirePOWER Services
  - Packets are marked for Drop or Drop with Reset and sent back to ASA
  - This allow the ASA to clear the connection from the state tables and send resets if needed



ASA 5585-X Data Port Utilization

- ASA SSP processes all ingress and egress packets
  - No packets are directly processed by FirePOWER SSP except for the FirePOWER SSP management port.
  - ASA configures and controls the FirePOWER SSP data ports



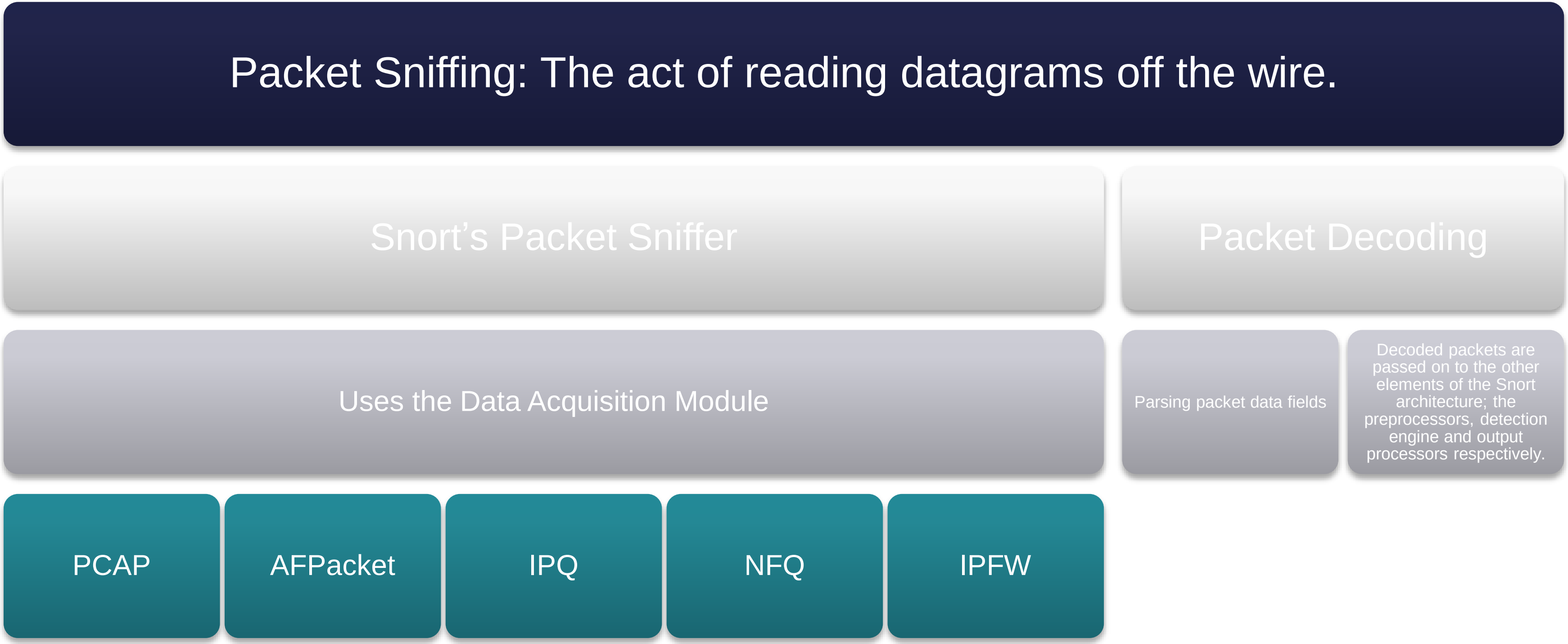
ASA FirePOWER Services Features

IPS

IPS Technology

- The Snort Engine's Basic Architecture
  - The sniffer
  - Preprocessors
  - The detection engine
  - The output and alerting module

IPS Technology



Packet Sniffing: The act of reading datagrams off the wire.

Snort’s Packet Sniffer

Packet Decoding

Uses the Data Acquisition Module

Parsing packet data fields

Decoded packets are passed on to the other elements of the Snort architecture; the preprocessors, detection engine and output processors respectively.

PCAP

AFPacket

IPQ

NFQ

IPFW

IPS Technology

Preprocessors

Handle the task of presenting packets and packet data in a contextually relevant way to the detection engine.

For example

- Packet fragment reassembly
- Maintaining TCP state
- TCP Stream reassemble
- Protocol normalization

IPS Technology

Detection Engine:

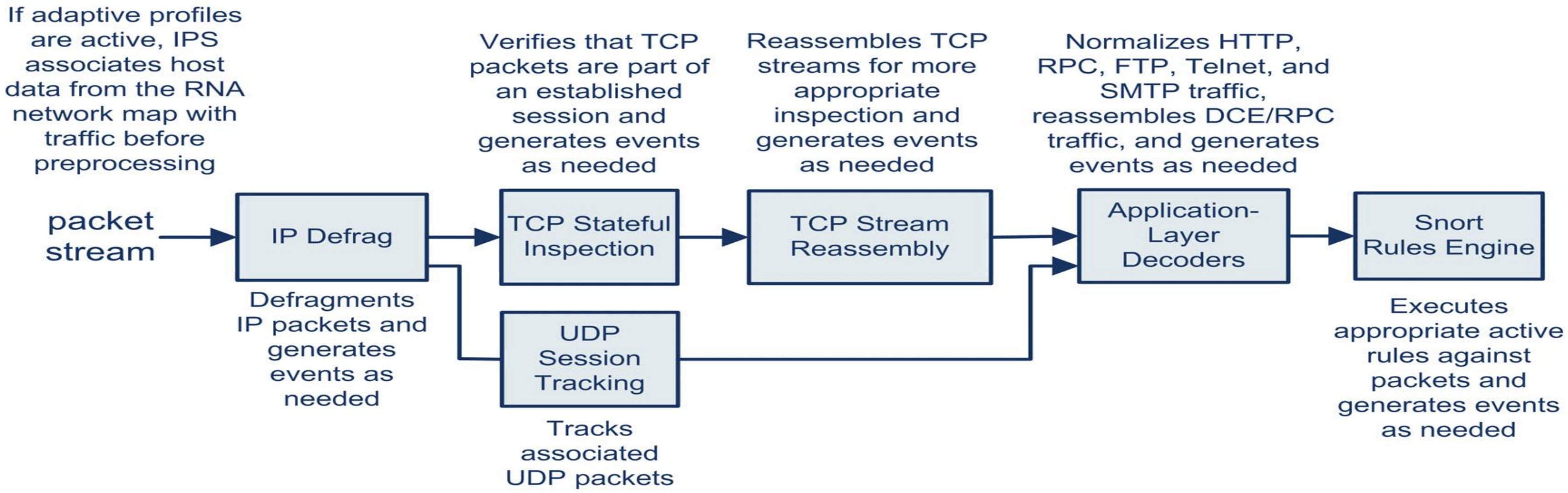
The detection engine accepts the parsed, normalized and stream-reassembled network traffic for inspection against the rule base. This component of the Snort architecture actually has two components to perform the action of inspection:

Rules builder - the Snort rules builder goes through all the rules to assemble them in such a way that inspection is optimized by eliminating redundancies

Inspection against the built rules – Inspection takes place against the rule chains built by the rule builder

IPS Technology

Preprocessor Execution Order



If adaptive profiles are active, IPS associates host data from the RNA network map with traffic before preprocessing

packet stream

IP Defrag

Defragments IP packets and generates events as needed

TCP Stateful Inspection

Verifies that TCP packets are part of an established session and generates events as needed

UDP Session Tracking

Tracks associated UDP packets

TCP Stream Reassembly

Reassembles TCP streams for more appropriate inspection and generates events as needed

Application-Layer Decoders

Normalizes HTTP, RPC, FTP, Telnet, and SMTP traffic, reassembles DCE/RPC traffic, and generates events as needed

Snort Rules Engine

Executes appropriate active rules against packets and generates events as needed

Application Identification

Application Identification and Control

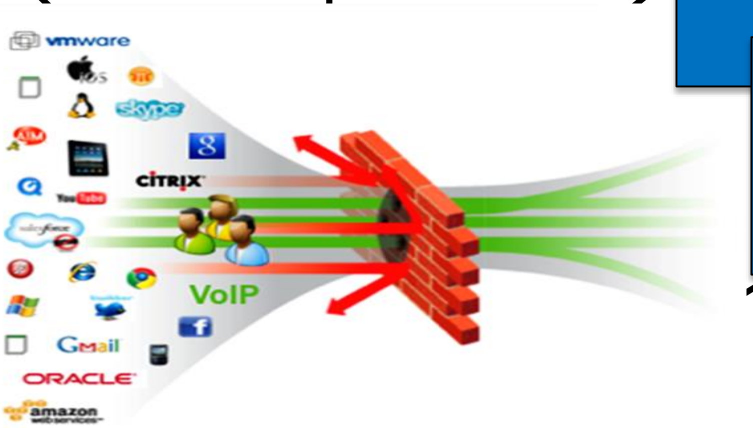
Restrict mobile apps in BYOD environments

Limit social media to control malware and data leakage

Reduce attack surface and inspection requirements

Deep visibility into app usage, regardless of port/protocol

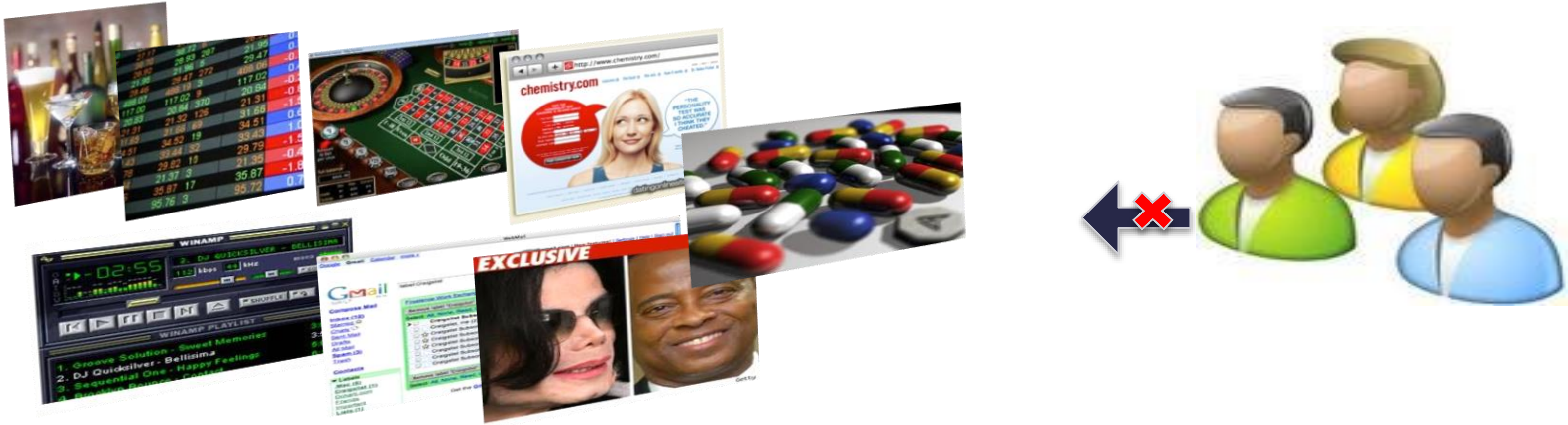
Reclaim bandwidth from streaming / sharing apps



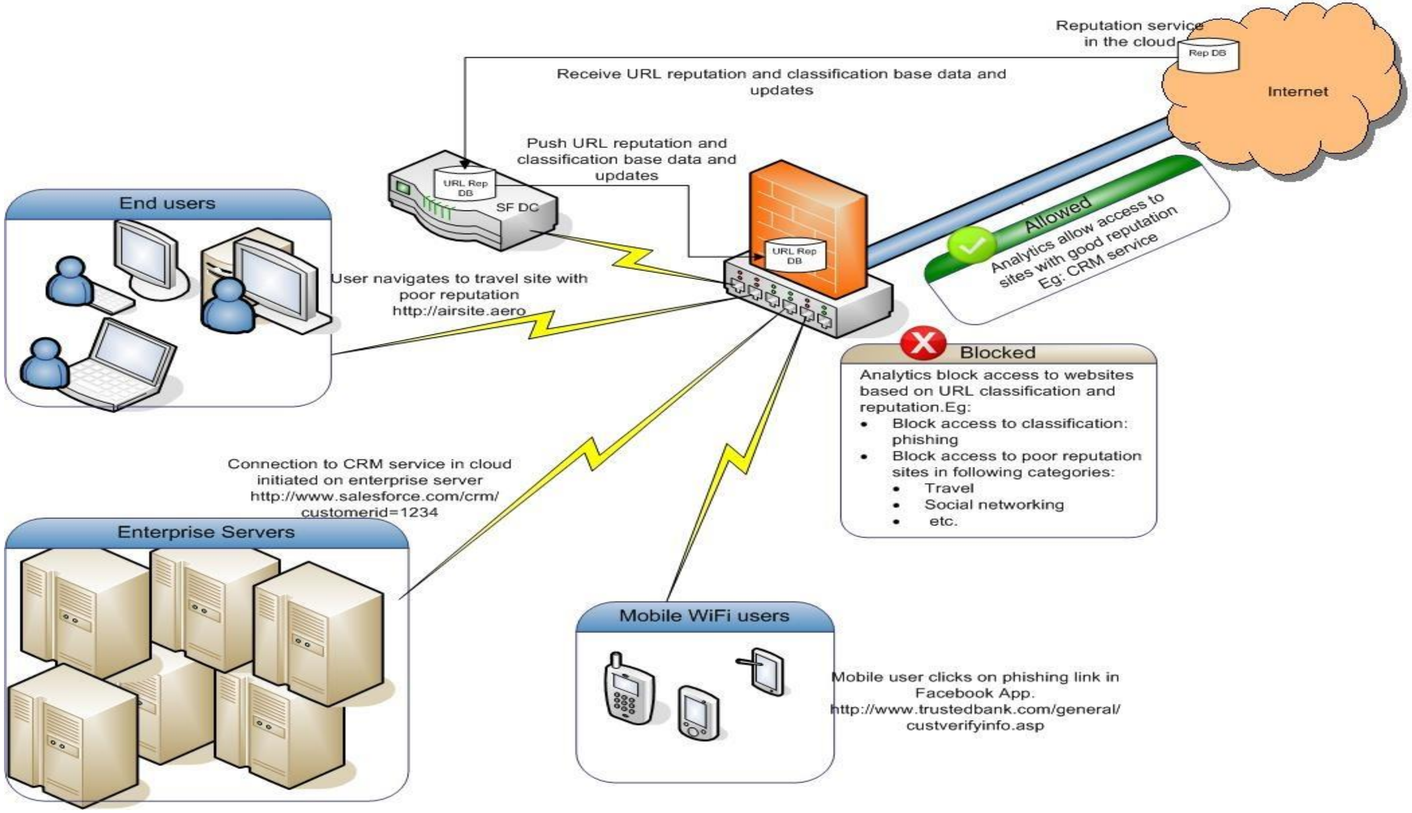
URL Filtering

URL Filtering

- Block non-business-related sites by category
- Based on user and user group



URL Filtering



Receive URL reputation and classification base data and updates

Push URL reputation and classification base data and updates

User navigates to travel site with poor reputation http://airsite.aero

Connection to CRM service in cloud initiated on enterprise server http://www.salesforce.com/crm/customerid=1234

Mobile user clicks on phishing link in Facebook App. http://www.trustedbank.com/general/custverifyinfo.asp

Allowed

Analytics allow access to sites with good reputation Eg: CRM service

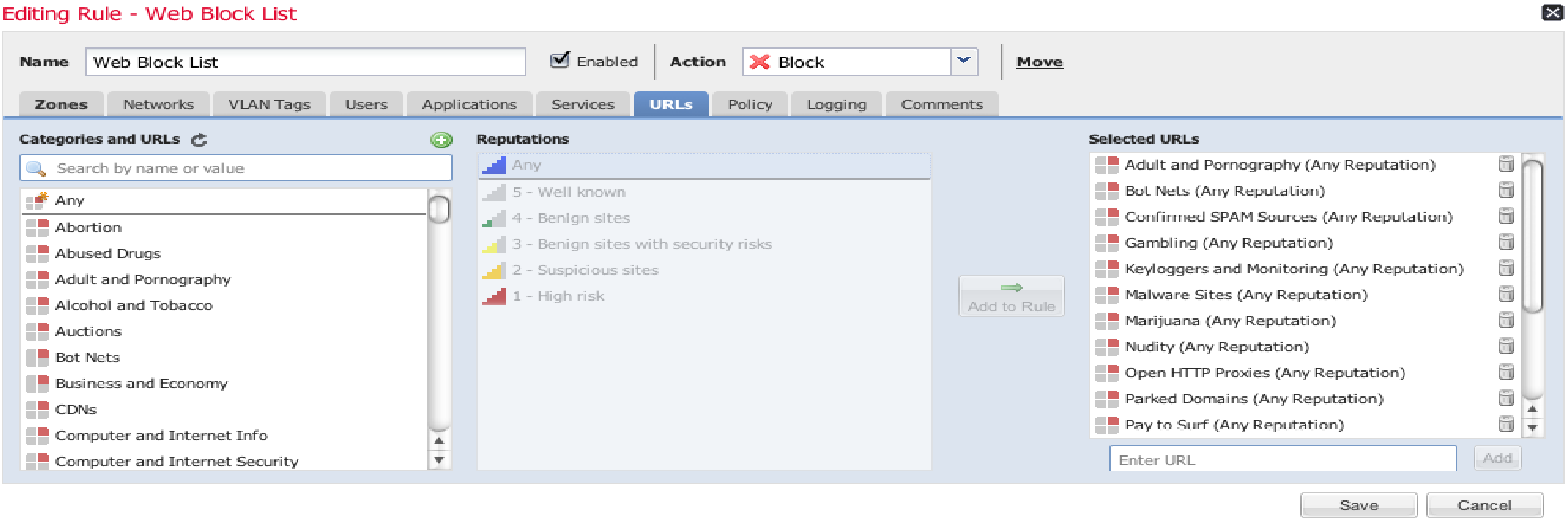
Blocked

Analytics block access to websites based on URL classification and reputation.Eg:

- Block access to classification: phishing
- Block access to poor reputation sites in following categories:
  - Travel
  - Social networking
  - etc.

URL Filtering

- Dozens of Content Categories
- URLs Categorized by Risk



Editing Rule - Web Block List

Name: Web Block List

☑ Enabled

Action: Block

Categories and URLs

Search by name or value

- Any
- Abortion
- Abused Drugs
- Adult and Pornography
- Alcohol and Tobacco
- Auctions
- Bot Nets
- Business and Economy
- CDNs
- Computer and Internet Info
- Computer and Internet Security

Reputations

- Any
- 5 - Well known
- 4 - Benign sites
- 3 - Benign sites with security risks
- 2 - Suspicious sites
- 1 - High risk

Selected URLs

- Adult and Pornography (Any Reputation)
- Bot Nets (Any Reputation)
- Confirmed SPAM Sources (Any Reputation)
- Gambling (Any Reputation)
- Keyloggers and Monitoring (Any Reputation)
- Malware Sites (Any Reputation)
- Marijuana (Any Reputation)
- Nudity (Any Reputation)
- Open HTTP Proxies (Any Reputation)
- Parked Domains (Any Reputation)
- Pay to Surf (Any Reputation)

Enter URL

URL Reputation

Each URL is assigned one Reputations score

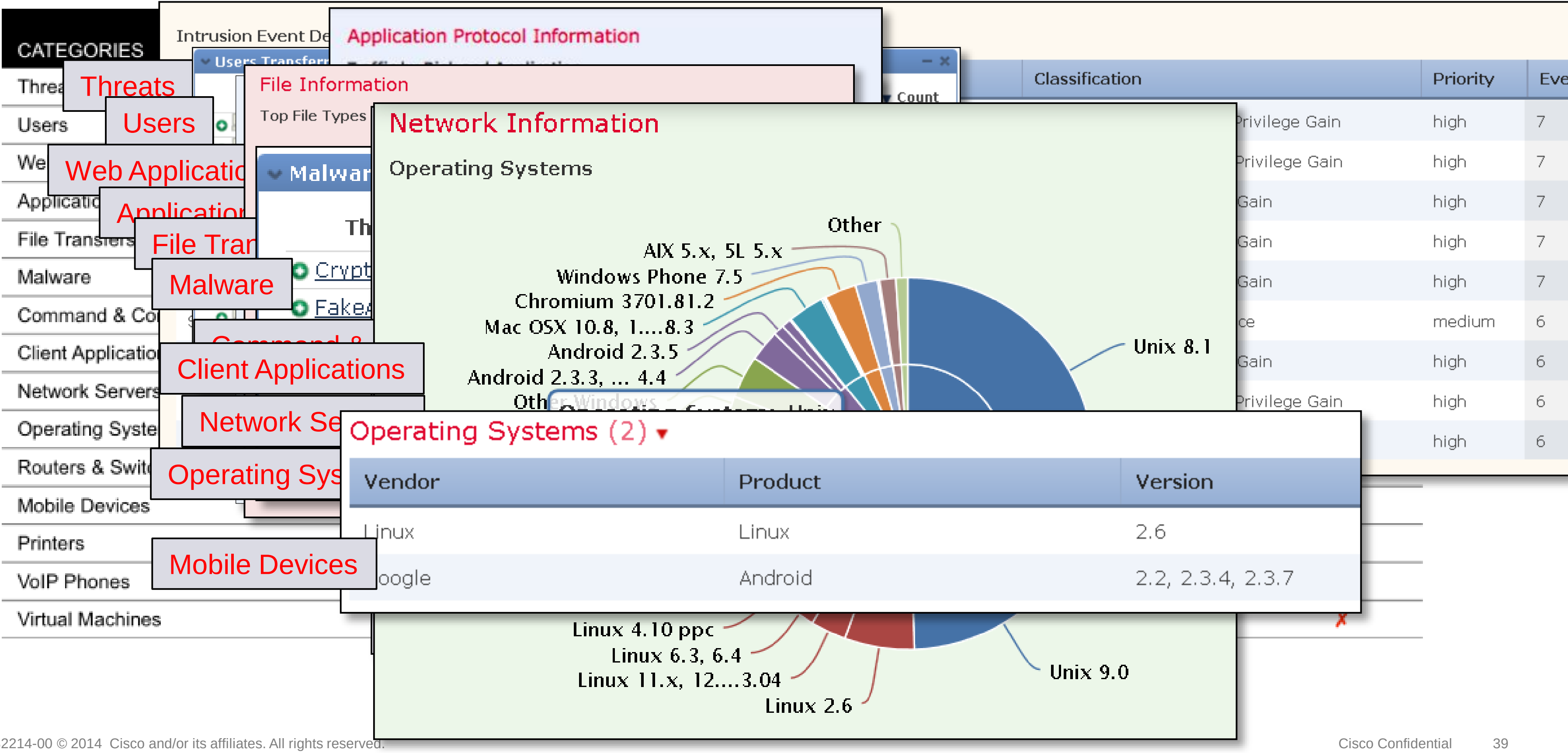
URL reputations indicate a “safety rating”

Available Reputation values are:

- Well known
- Benign sites
- Benign sites with security risks
- Suspicious sites
- High Risk

FireSIGHT

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

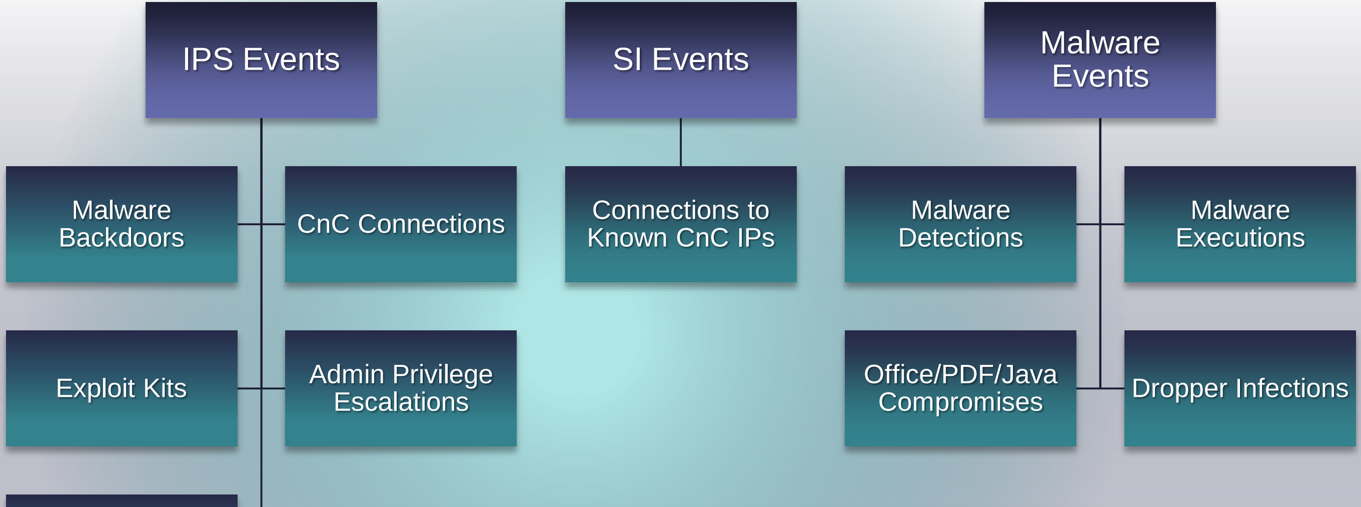


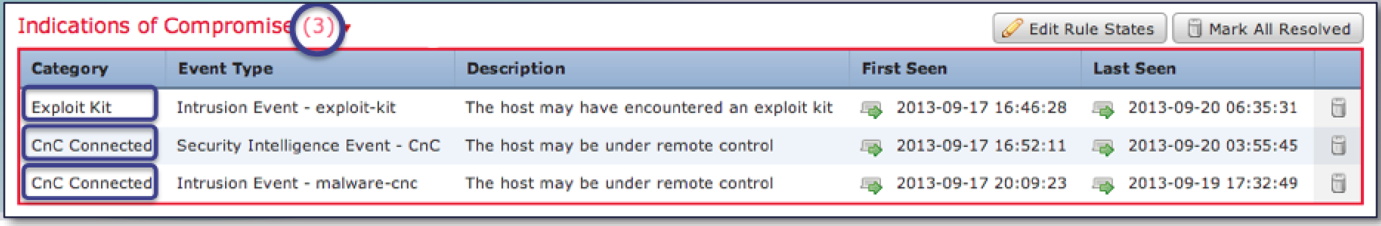
Classification	Priority	Eve
Privilege Gain	high	7
Privilege Gain	high	7
Gain	high	7
Gain	high	7
Gain	high	7
ce	medium	6
Gain	high	6
Privilege Gain	high	6
	high	6

Operating Systems (2) ▾

Vendor	Product	Version
Linux	Linux	2.6
oogle	Android	2.2, 2.3.4, 2.3.7

Indications of Compromise (IoCs)

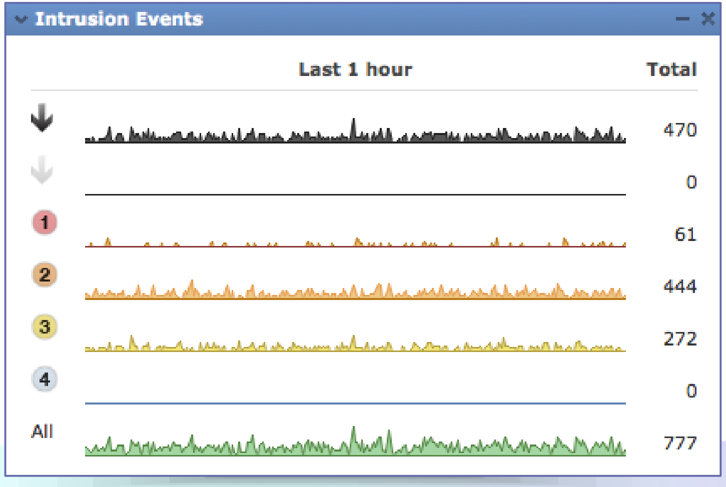




Indications of Compromise (3)

Category	Event Type	Description	First Seen	Last Seen
Exploit Kit	Intrusion Event - exploit-kit	The host may have encountered an exploit kit	2013-09-17 16:46:28	2013-09-20 06:35:31
CnC Connected	Security Intelligence Event - CnC	The host may be under remote control	2013-09-17 16:52:11	2013-09-20 03:55:45
CnC Connected	Intrusion Event - malware-cnc	The host may be under remote control	2013-09-17 20:09:23	2013-09-19 17:32:49

Impact Assessment



Intrusion Events

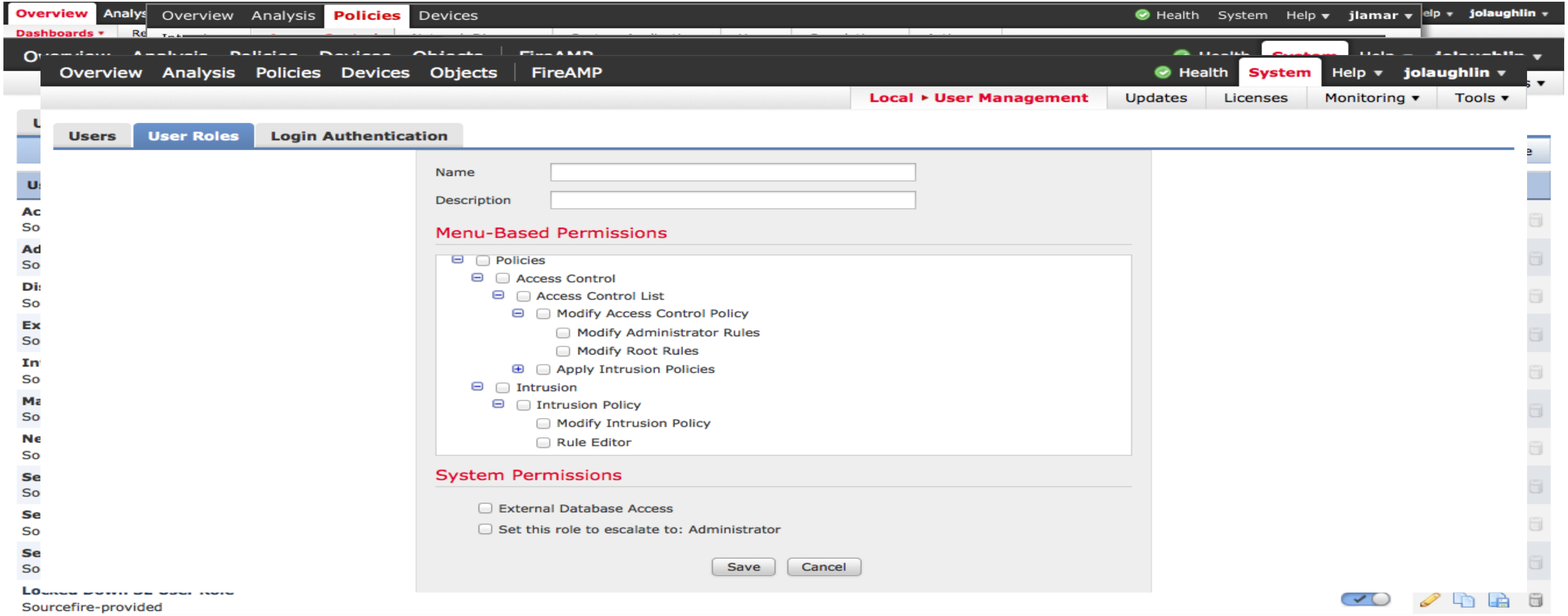
	Last 1 hour	Total
⬇		470
⬇		0
1		61
2		444
3		272
4		0
All		777

Correlates all intrusion events to an impact of the attack against the target

IMPACT FLAG	ADMINISTRATOR ACTION	WHY
1	Act Immediately, Vulnerable	Event corresponds to vulnerability mapped to host
2	Investigate, Potentially Vulnerable	Relevant port open or protocol in use, but no vuln mapped
3	Good to Know, Currently Not Vulnerable	Relevant port not open or protocol not in use
4	Good to Know, Unknown Target	Monitored network, but unknown host
0	Good to Know, Unknown Network	Unmonitored network

FireSIGHT Management Center

Single console for event, policy, and configuration management



Name

Description

Menu-Based Permissions

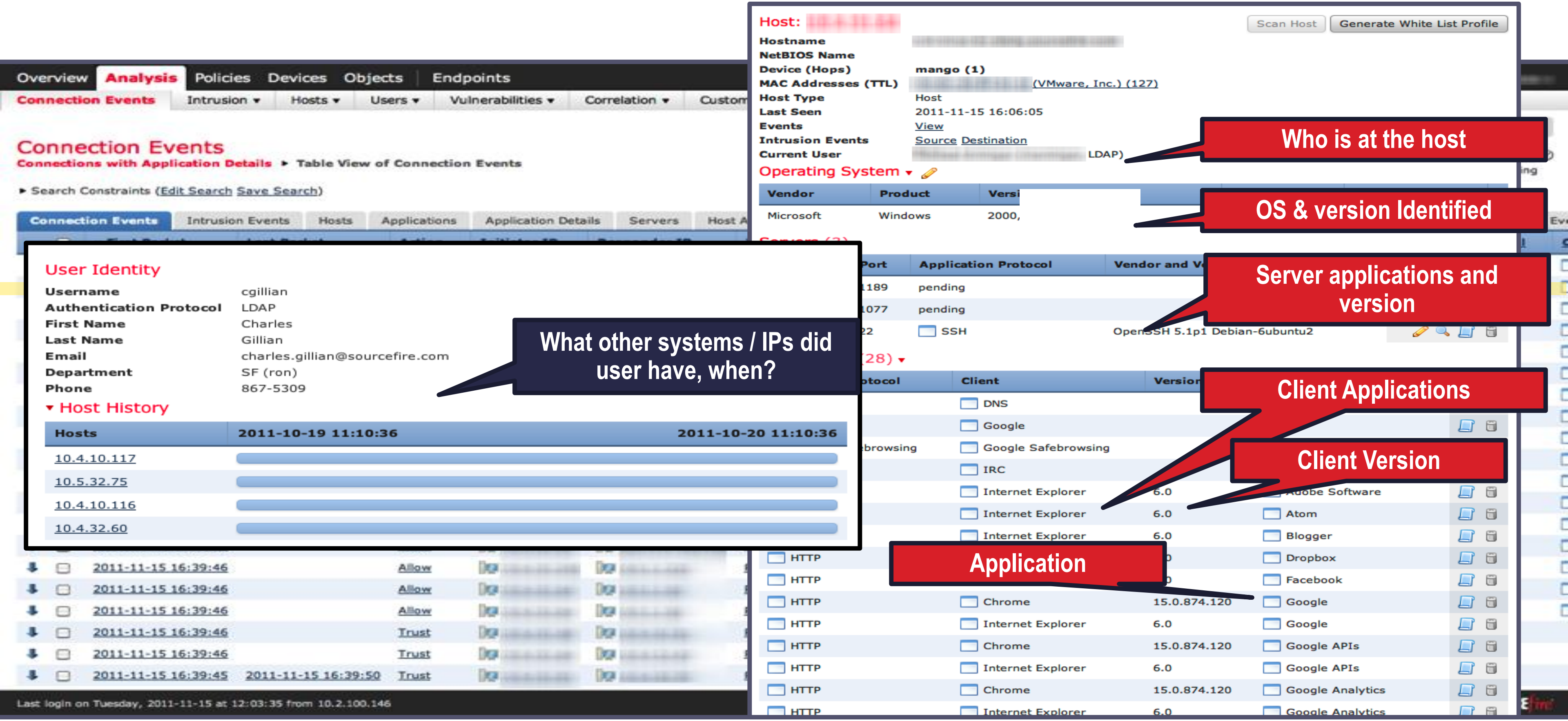
- ⊟ □ Policies
  - ⊟ □ Access Control
    - ⊟ □ Access Control List
      - ⊟ □ Modify Access Control Policy
        - □ Modify Administrator Rules
        - □ Modify Root Rules
      - ⊞ □ Apply Intrusion Policies
  - ⊟ □ Intrusion
    - ⊟ □ Intrusion Policy
      - □ Modify Intrusion Policy
      - □ Rule Editor

System Permissions

□ External Database Access

□ Set this role to escalate to: Administrator

Awareness Delivers Insight



Connection Events

Connections with Application Details ▸ Table View of Connection Events

▸ Search Constraints (Edit Search Save Search)

User Identity

Username	cgillian
Authentication Protocol	LDAP
First Name	Charles
Last Name	Gillian
Email	charles.gillian@sourcefire.com
Department	SF (ron)
Phone	867-5309

▾ Host History

Hosts	2011-10-19 11:10:36	2011-10-20 11:10:36
10.4.10.117		
10.5.32.75		
10.4.10.116		
10.4.32.60		

What other systems / IPs did user have, when?

2011-11-15 16:39:46		Allow	[redacted]
2011-11-15 16:39:46		Allow	[redacted]
2011-11-15 16:39:46		Allow	[redacted]
2011-11-15 16:39:46		Trust	[redacted]
2011-11-15 16:39:46		Trust	[redacted]
2011-11-15 16:39:45	2011-11-15 16:39:50	Trust	[redacted]

Last login on Tuesday, 2011-11-15 at 12:03:35 from 10.2.100.146

Host: [redacted]

Hostname	[redacted]
NetBIOS Name	
Device (Hops)	mango (1)
MAC Addresses (TTL)	[redacted] (VMware, Inc.) (127)
Host Type	Host
Last Seen	2011-11-15 16:06:05
Events	View
Intrusion Events	Source Destination
Current User	[redacted] LDAP)

Who is at the host

Operating System ▾

Vendor	Product	Versi
Microsoft	Windows	2000,

OS & version Identified

Port	Application Protocol	Vendor and Ve
1189	pending	
1077	pending	
22	SSH	OpenSSH 5.1p1 Debian-6ubuntu2

Server applications and version

(28) ▾

otocol	Client	Version	
	DNS		
	Google		
browsing	Google Safebrowsing		
	IRC		
	Internet Explorer	6.0	Adobe Software
	Internet Explorer	6.0	Atom
	Internet Explorer	6.0	Blogger
HTTP		0	Dropbox
HTTP		0	Facebook
HTTP	Chrome	15.0.874.120	Google
HTTP	Internet Explorer	6.0	Google
HTTP	Chrome	15.0.874.120	Google APIs
HTTP	Internet Explorer	6.0	Google APIs
HTTP	Chrome	15.0.874.120	Google Analytics
HTTP	Internet Explorer	6.0	Google Analytics

Client Applications

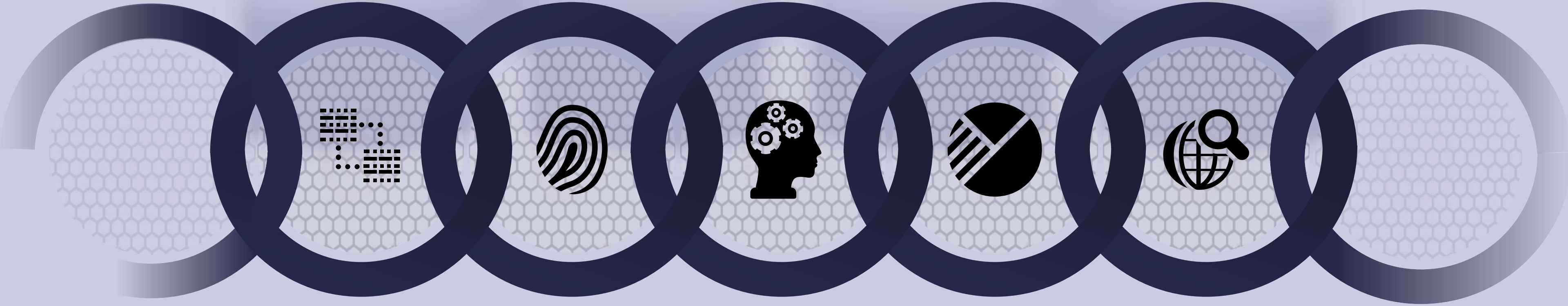
Client Version

Application

Cisco Advanced Malware Protection

Advanced Malware Protection

All detection is less than 100%



One-to-One Signature

Fuzzy Finger-Printing

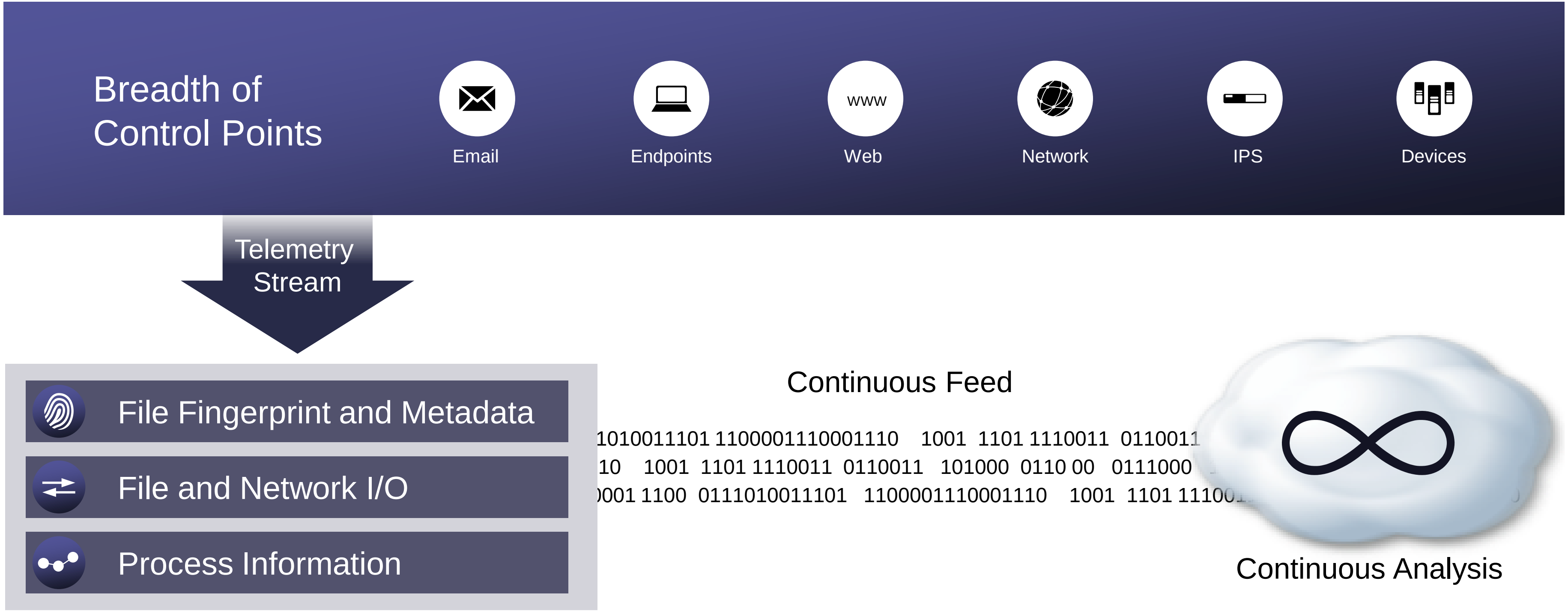
Machine Learning

Advanced Analytics

Dynamic Analysis

Reputation Filtering and File Sandboxing

AMP Provides Continuous Retrospective Security



Breadth of Control Points

- File Fingerprint and Metadata
- File and Network I/O
- Process Information

Continuous Feed

Continuous Analysis

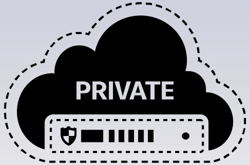
Expanding Advanced Malware Protection Everywhere

ASA

Dedicated FirePOWER Appliance

Web & Email Security Appliances

Cloud Based Web Security & Hosted Email



Private Cloud

PC / MAC

Mobile

Virtual

NGIPS /NGFW on FirePOWER

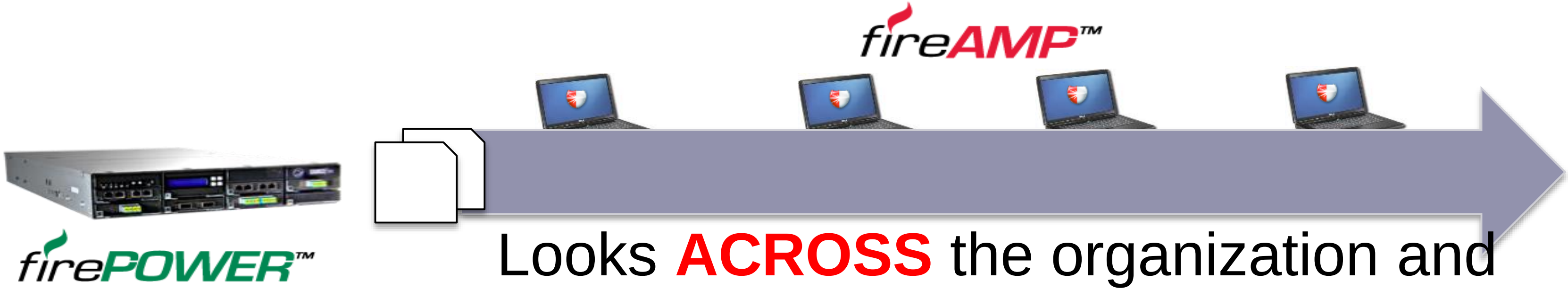
Continuous & Zero-Day Detection

Advanced Analytics And Correlation

Enterprise Capabilities

File Trajectory

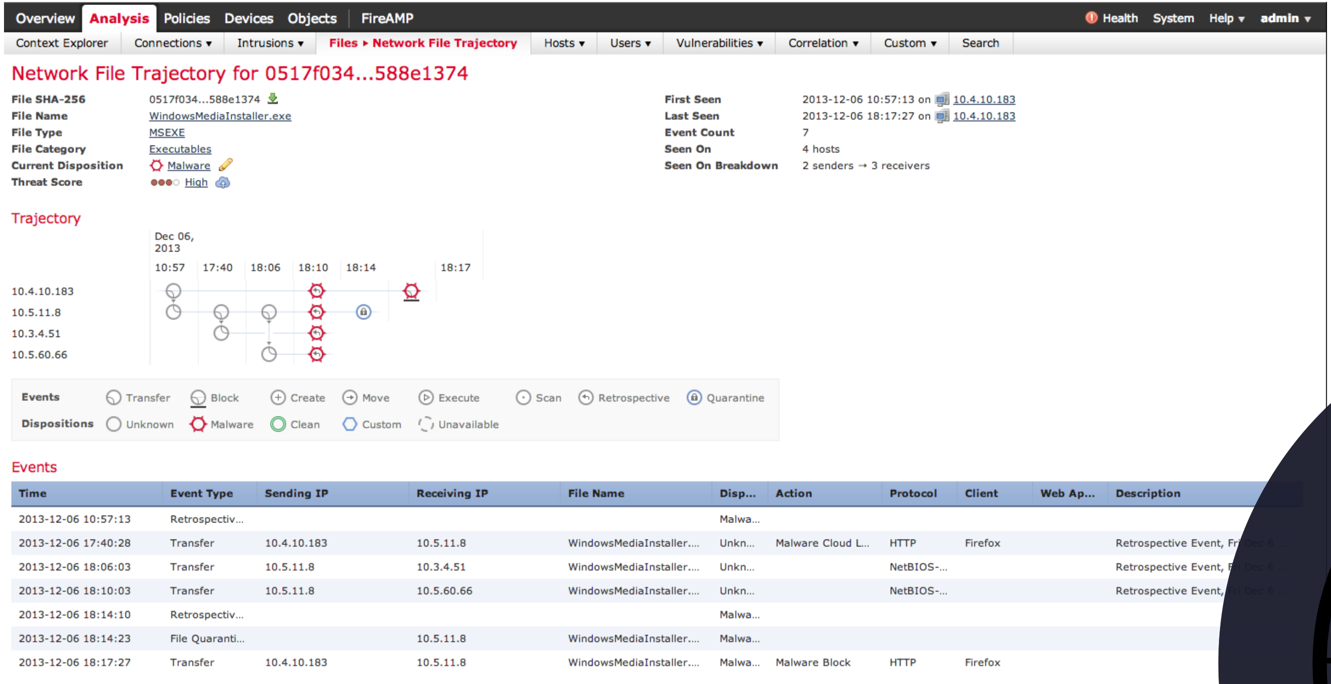
Quickly understand the scope of malware problem



Looks **ACROSS** the organization and answers:

- What systems were infected?
- Who was infected first (“patient 0”) and when did it happen?
- What was the entry point?
- When did it happen?
- What else did it bring in?

How Cisco AMP Works: Network File Trajectory Use Case



Network File Trajectory for 0517f034...588e1374

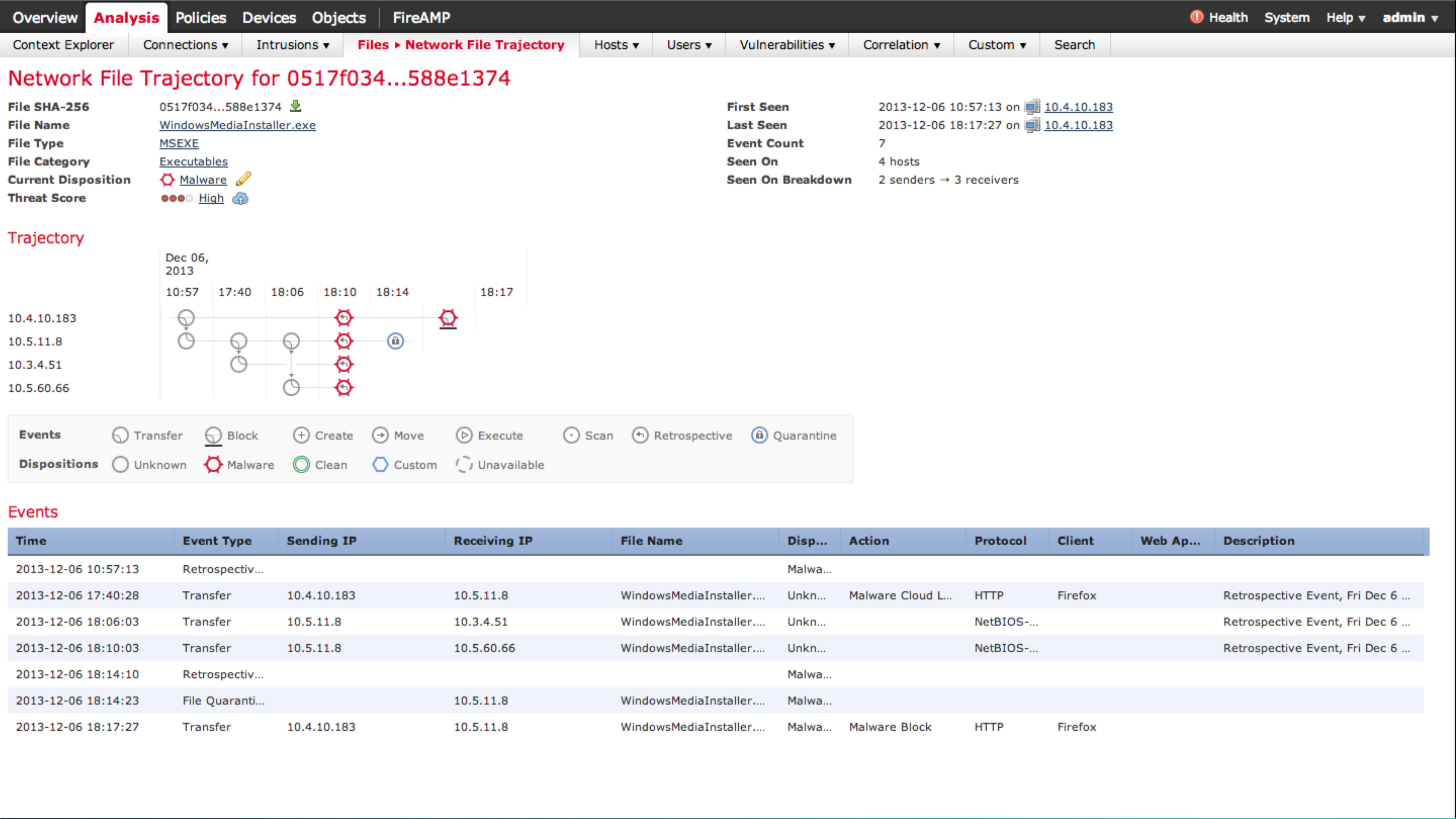
File SHA-256	0517f034...588e1374	**First Seen**	2013-12-06 10:57:13 on 10.4.10.183
File Name	WindowsMediaInstaller.exe	**Last Seen**	2013-12-06 18:17:27 on 10.4.10.183
File Type	MSEXE	**Event Count**	7
File Category	Executables	**Seen On**	4 hosts
Current Disposition	Malware	**Seen On Breakdown**	2 senders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

Trajectory

Events	Transfer	Block	Create	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		



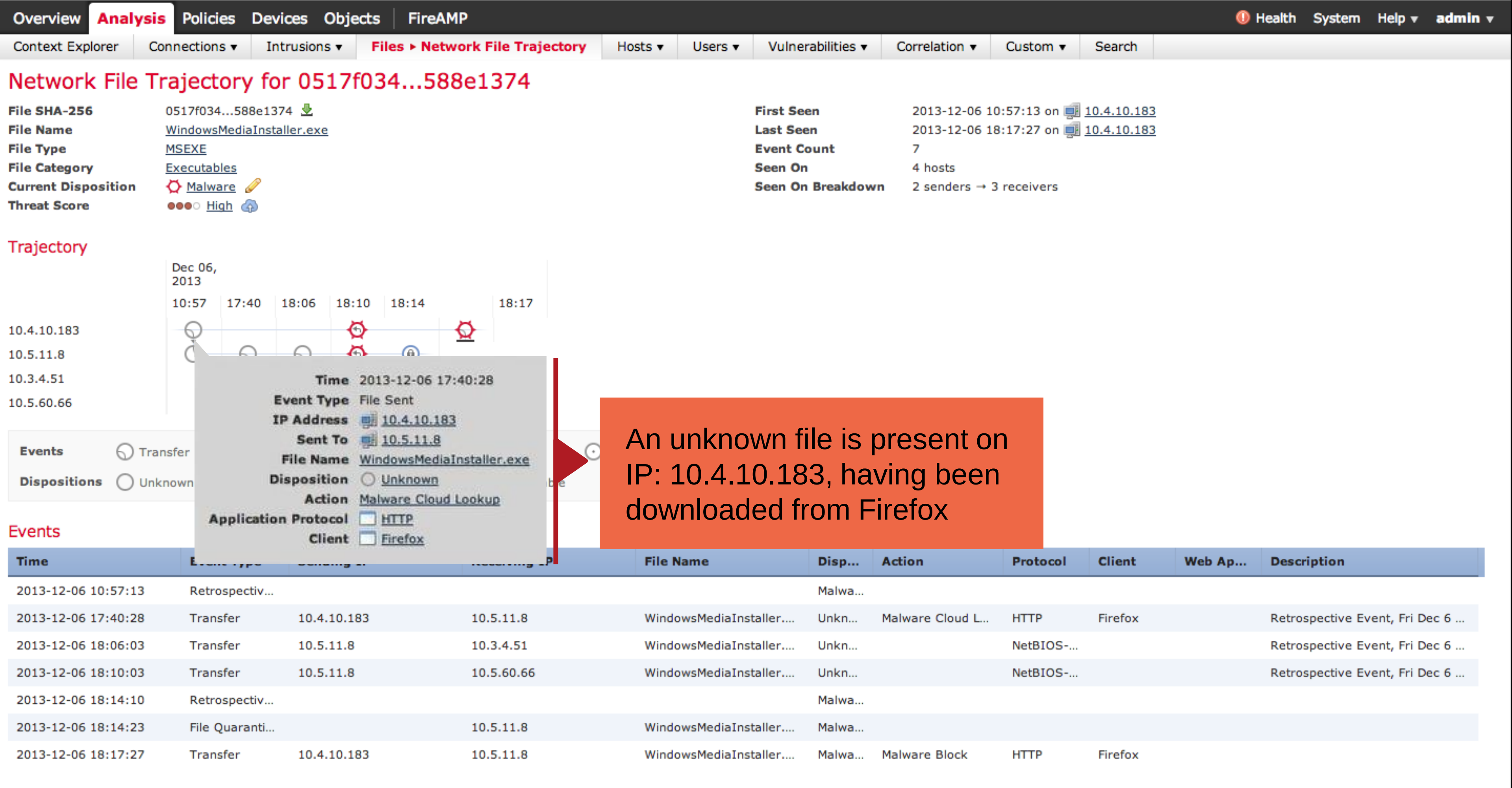
Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374	**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

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

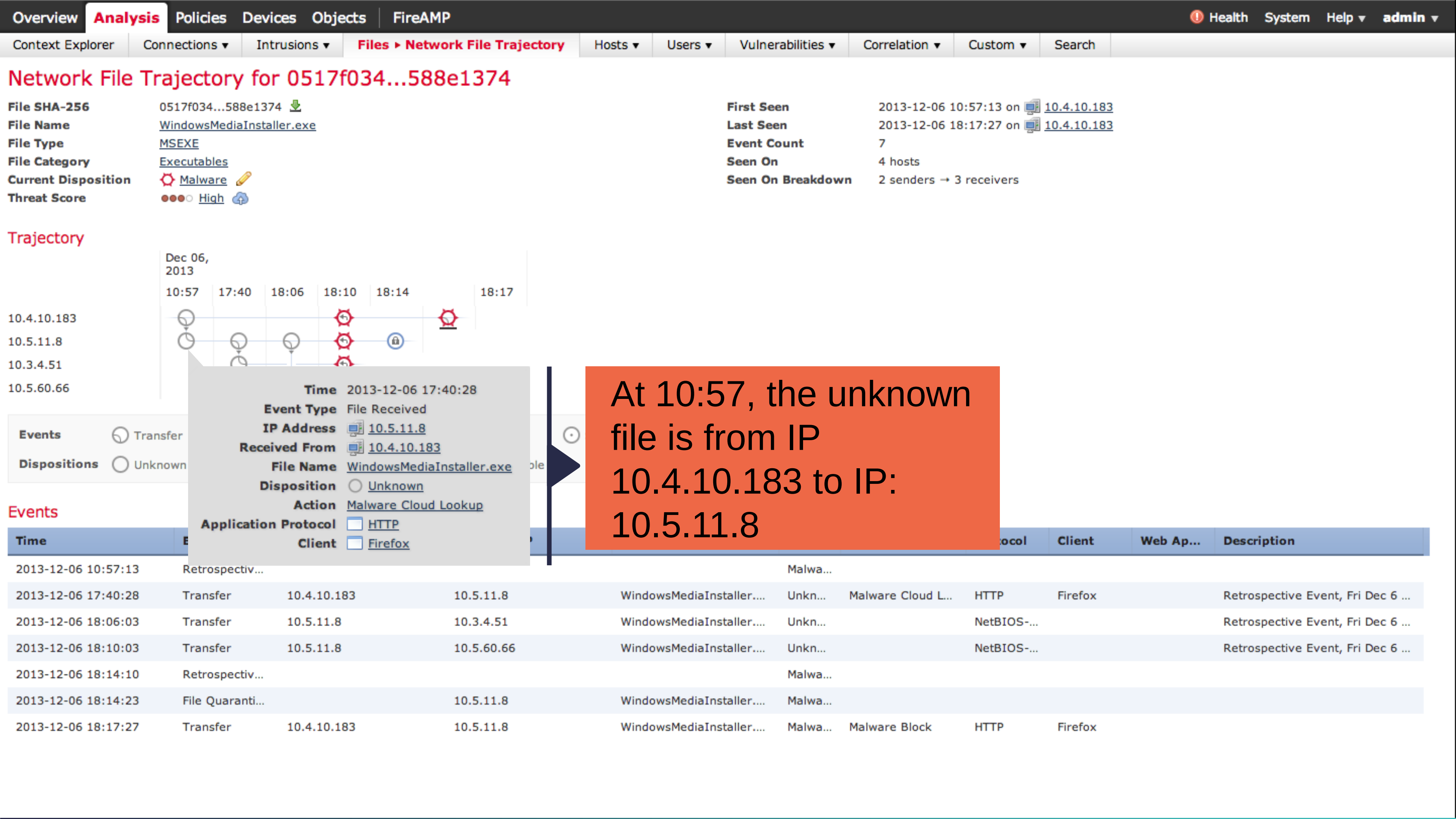
Trajectory

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
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

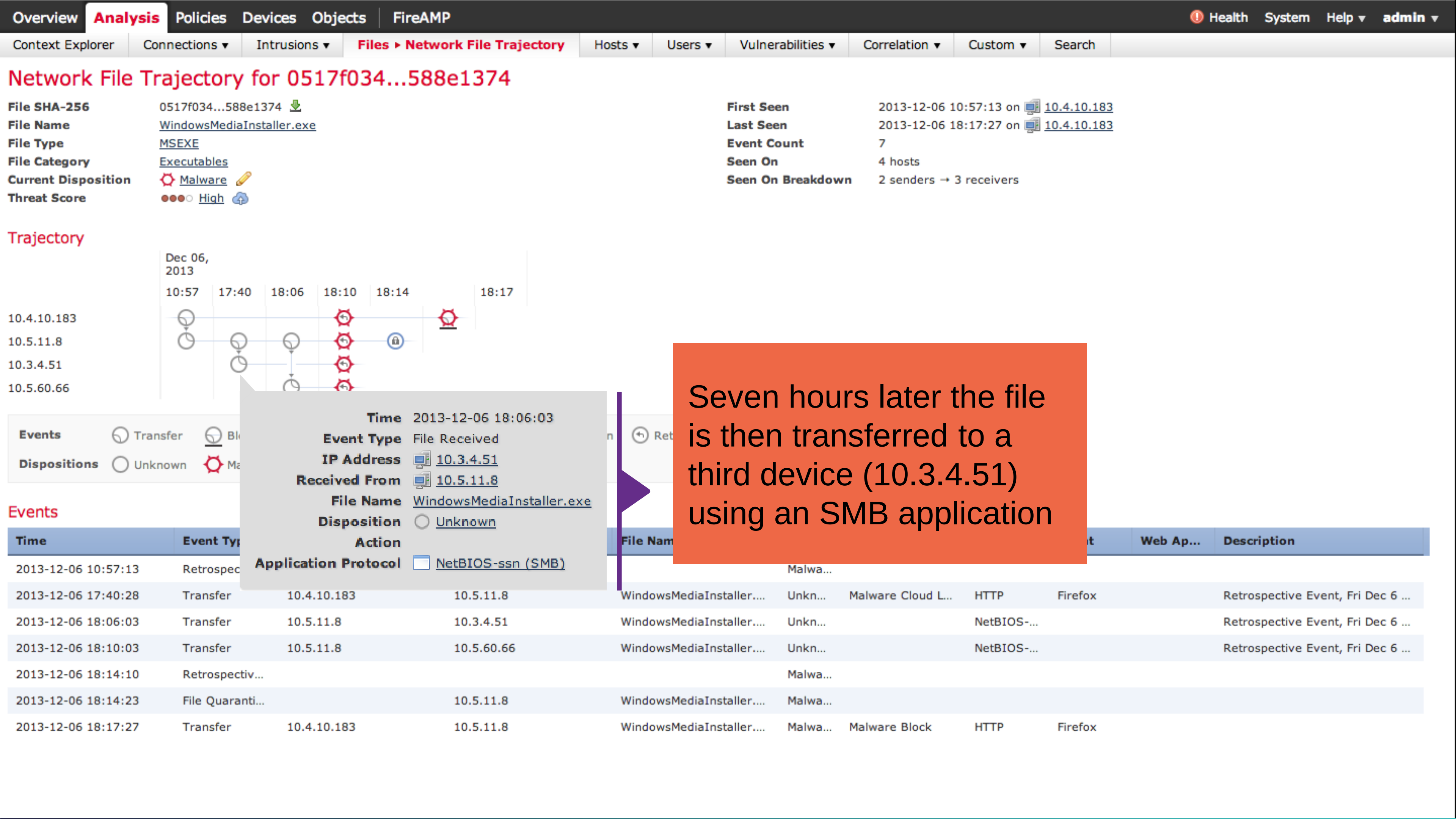
Trajectory

Time	2013-12-06 17:40:28
Event Type	File 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

Time	E						ocol	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		

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



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

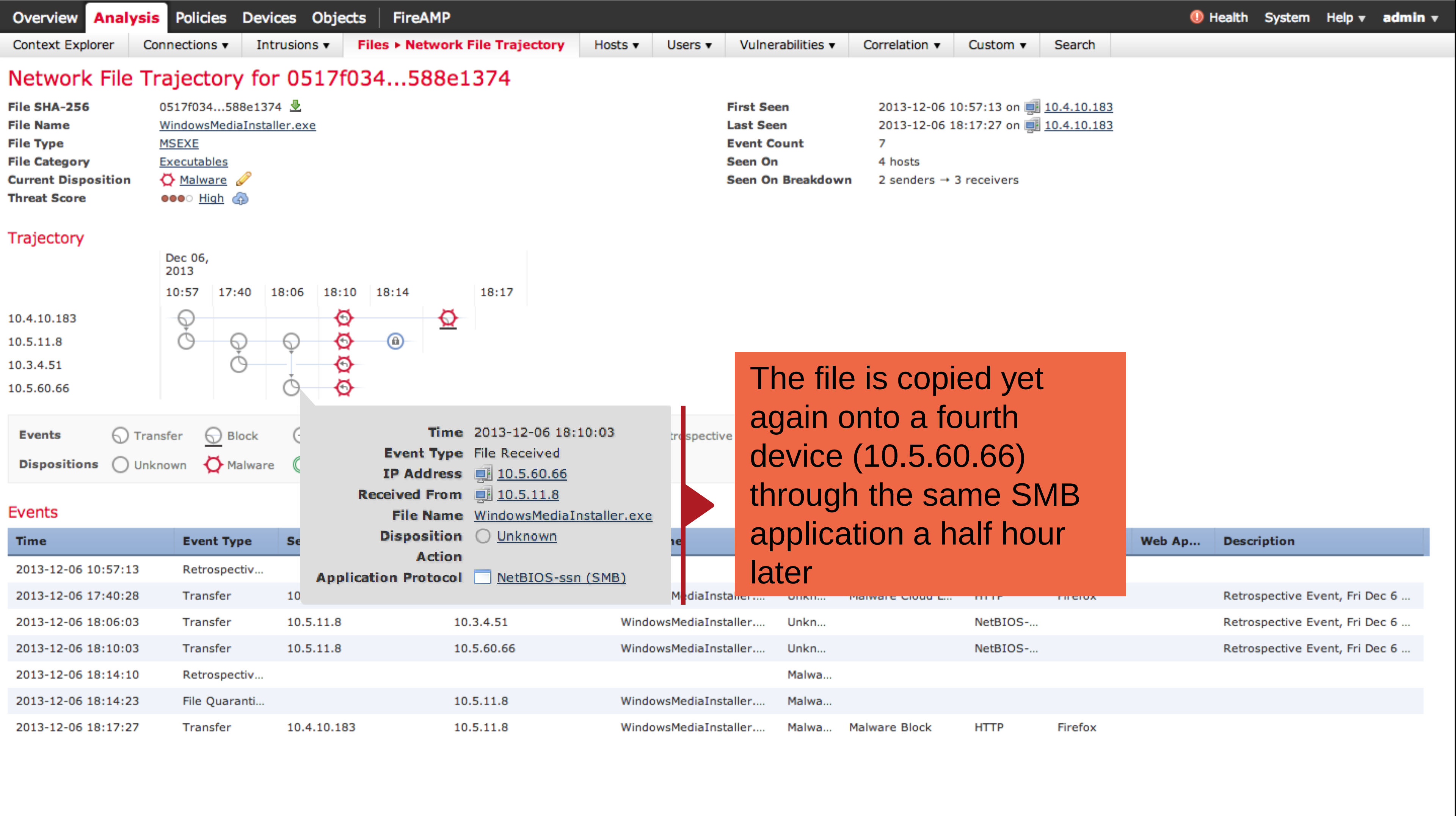
First Seen	2013-12-06 10:57:13 on 10.4.10.183
Last Seen	2013-12-06 18:17:27 on 10.4.10.183
Event Count	7
Seen On	4 hosts
Seen On Breakdown	2 senders → 3 receivers

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 Typ			File Nam				t	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

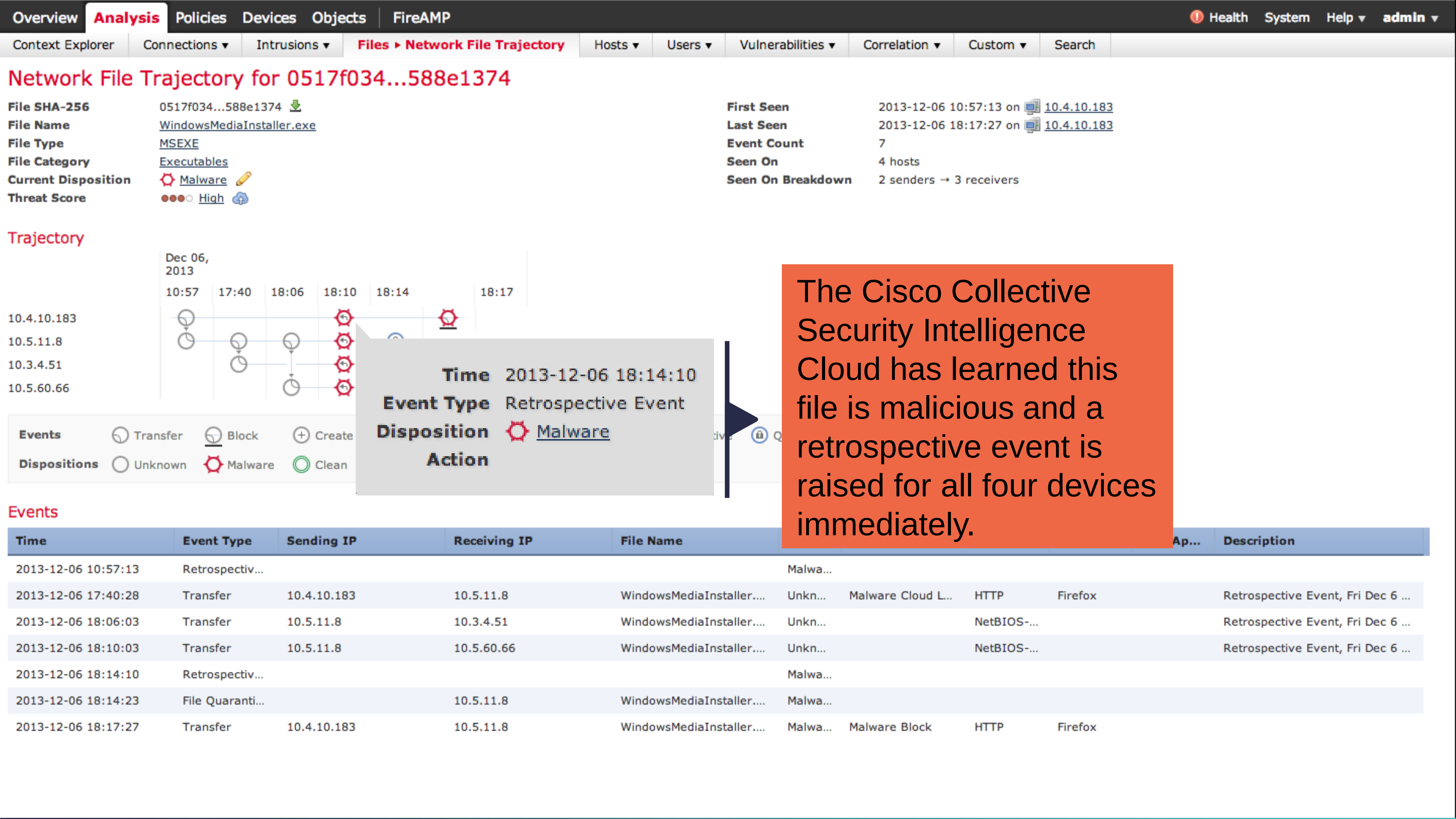
Trajectory

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		...e					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

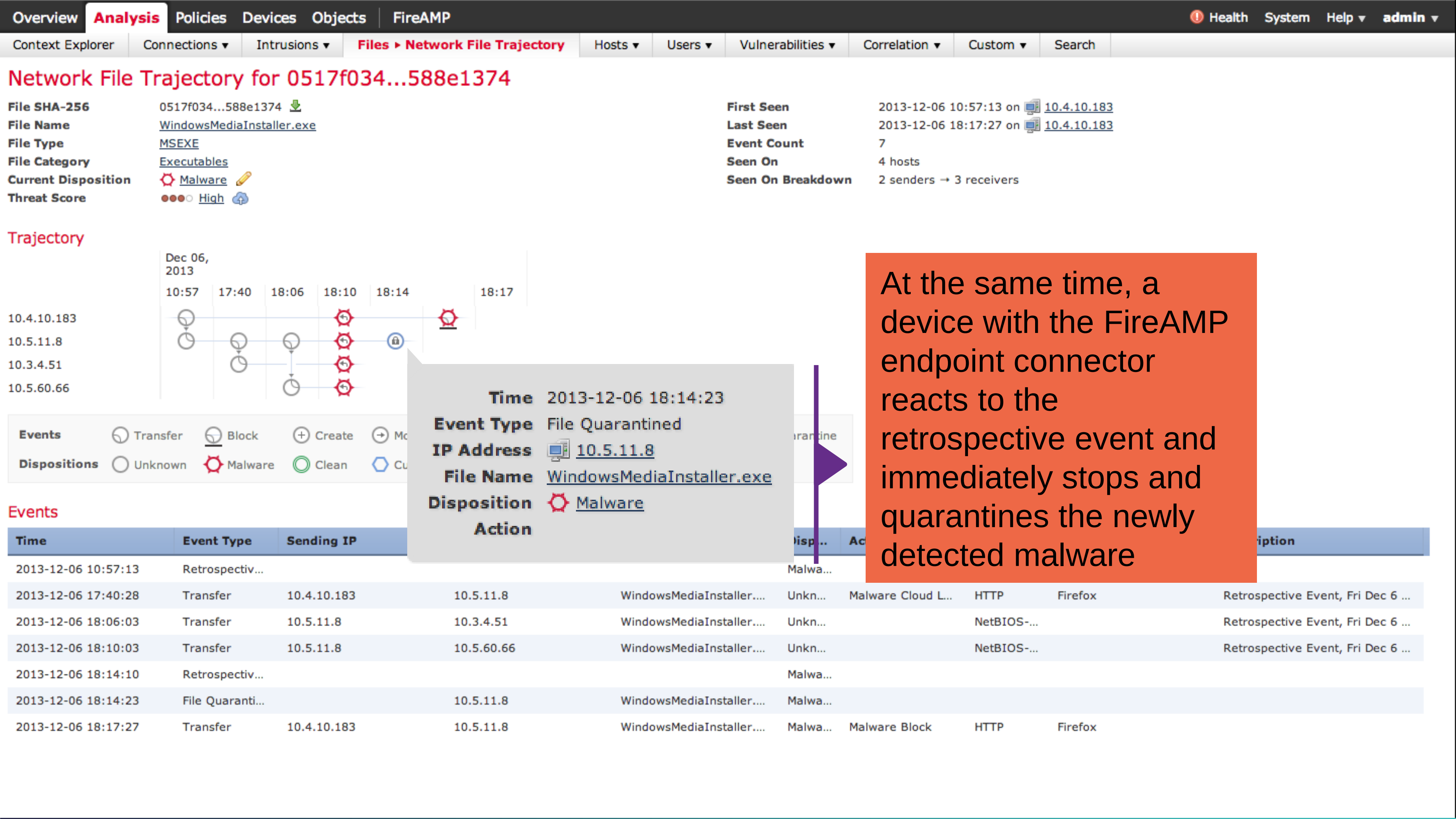
Trajectory

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

Events

Time	Event Type	Sending IP	Receiving IP	File Name					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
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

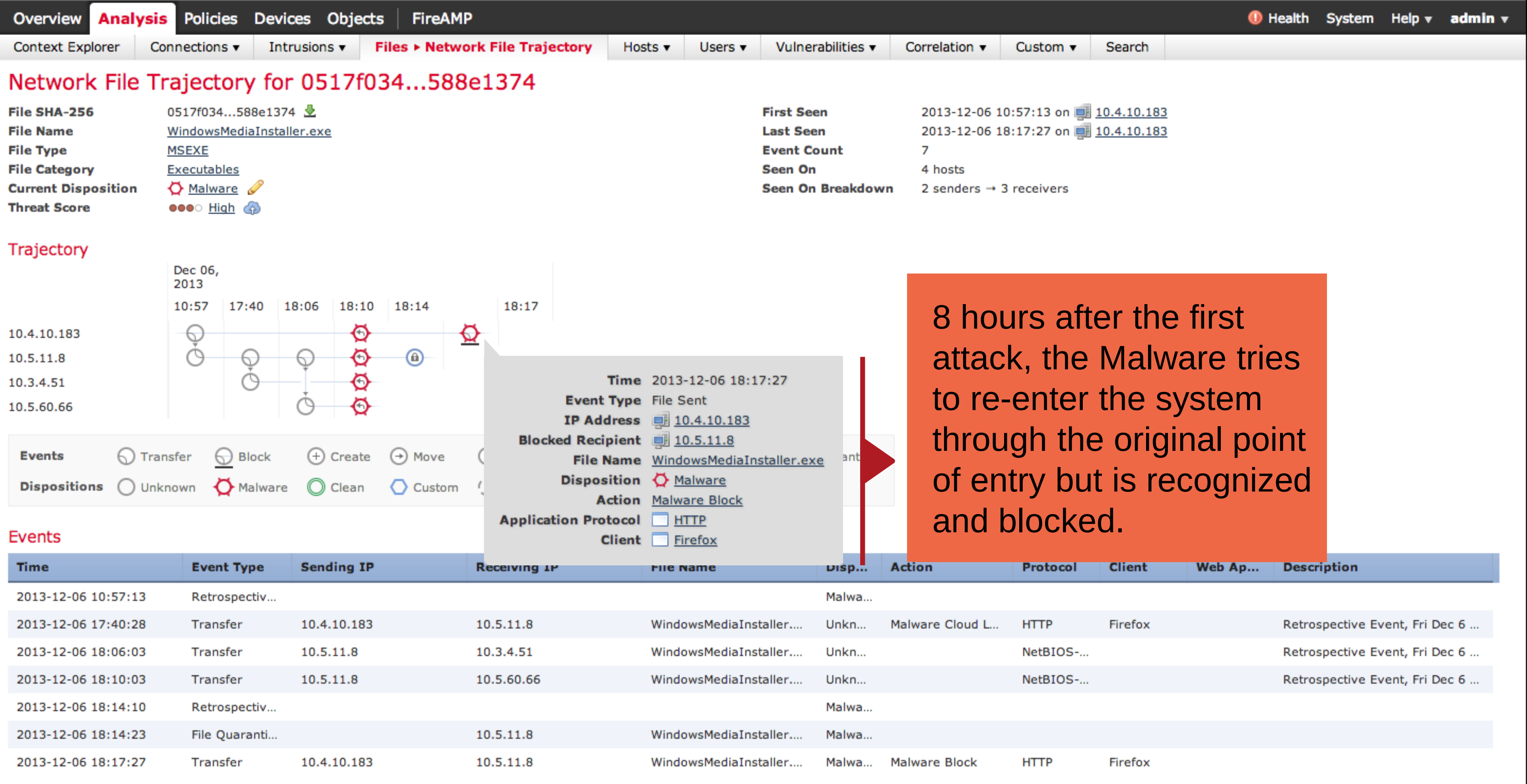
Trajectory

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

Events

Time	Event Type	Sending IP			isp..	Ac			iption
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 FireAMP 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	**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 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.

Thank you