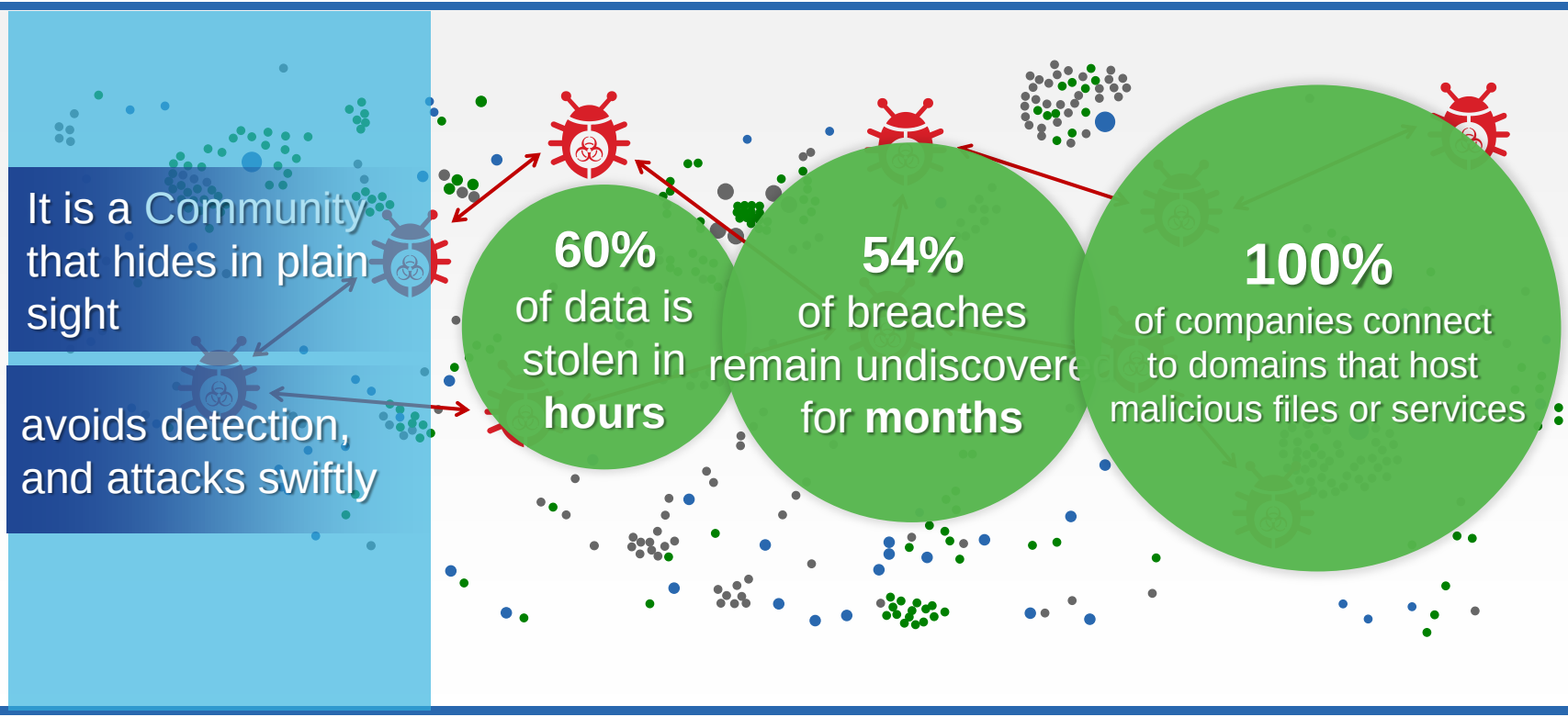
資訊安全趨勢與因應策略

郭旭傑 Joey Kuo
思科台灣 產品經理


There are two types of companies: those who have been hacked, and those who don't yet know they have been hacked.
John Chambers
Chief Executive Officer of Cisco

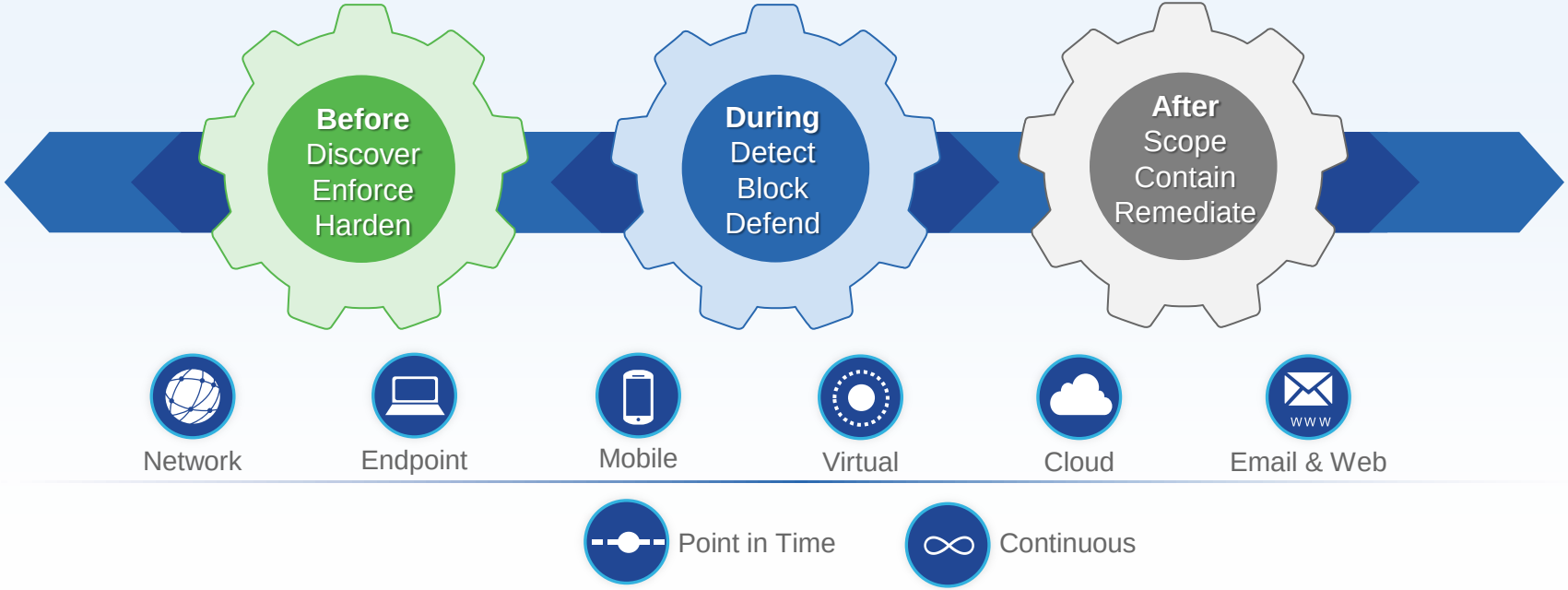
Security Challenges



What would you do differently if you knew you were going to be compromised?

To defend against these advanced threats requires greater visibility and control across the full attack continuum

Attack Continuum



Before

See It, Control It

You can't protect what you can't see

Threats

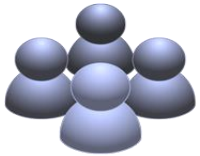
Devices

Applications

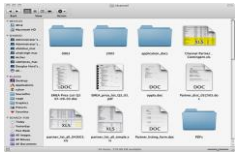
Flow

Vulnerabilities

OS



Users



Files

fireSIGHT Technology

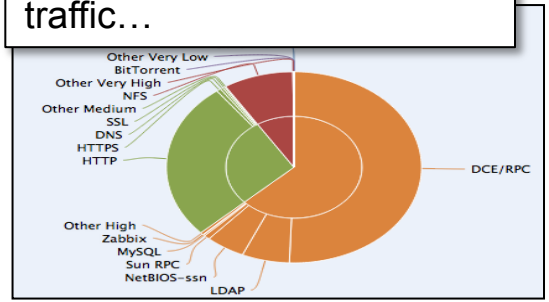
Network and endpoint awareness and context that provides environmental insights and automatically strengthens protection

Before

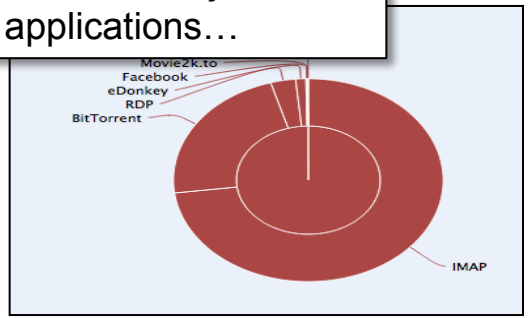
See It, Control It

Before the Threat: Discover Your Environment

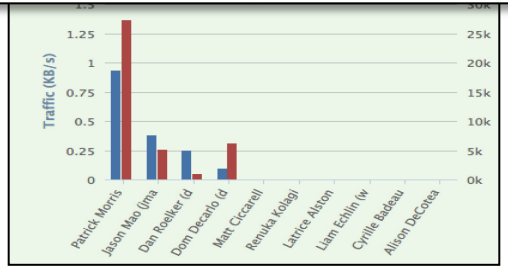
Browse all application traffic…



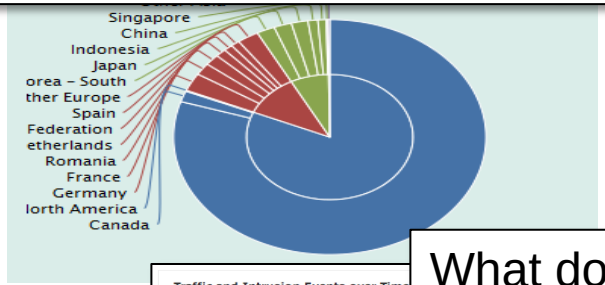
Look for risky applications…



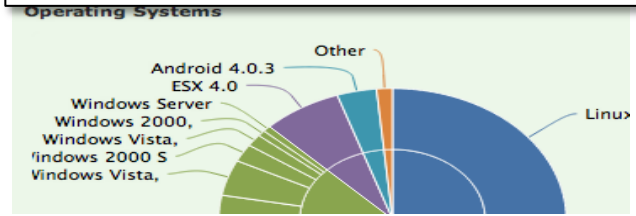
Who is using them?



Connections by Initiator Country

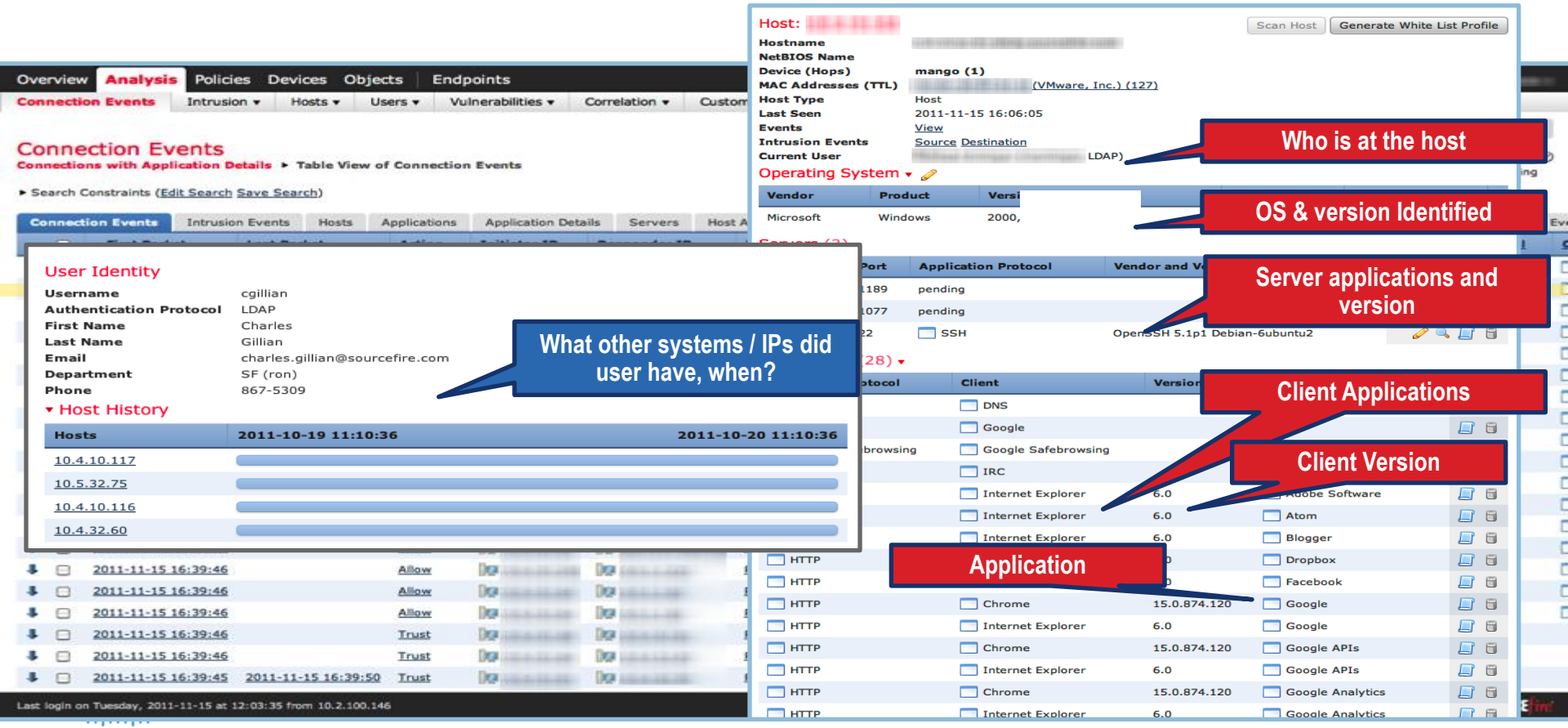


On what operating systems?

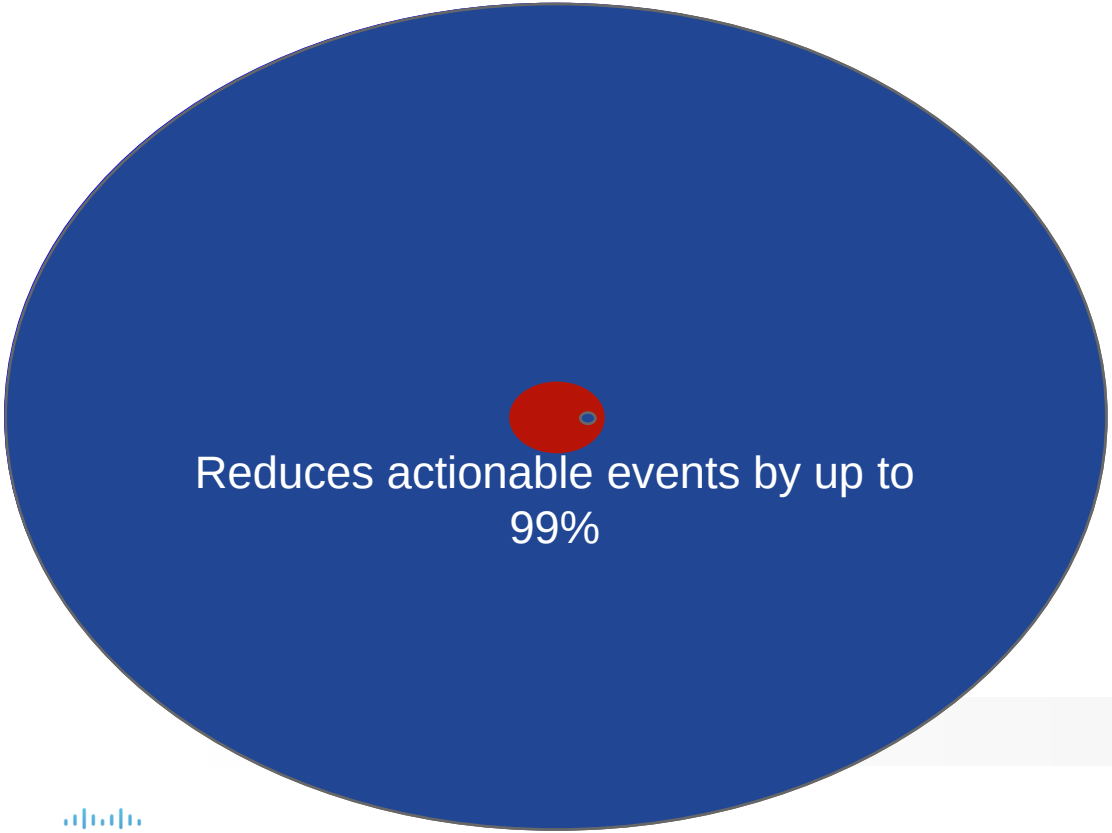


What does their traffic look like over time?

FireSIGHT™ Awareness



事件管理？ How to manage thousands event per day?



Intrusion event

Vulnerable
(exploit targets known vulnerability)

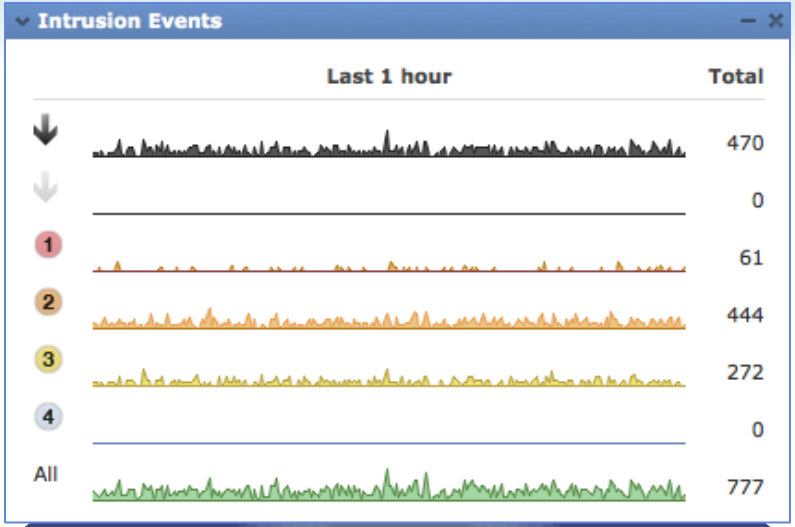
Possibly vulnerable
(exploit targets OS and/or service)

Not vulnerable
(no service present)

Not present
(no host present)

Correlation & Automation (自動化及關聯分析)- Cost Saving

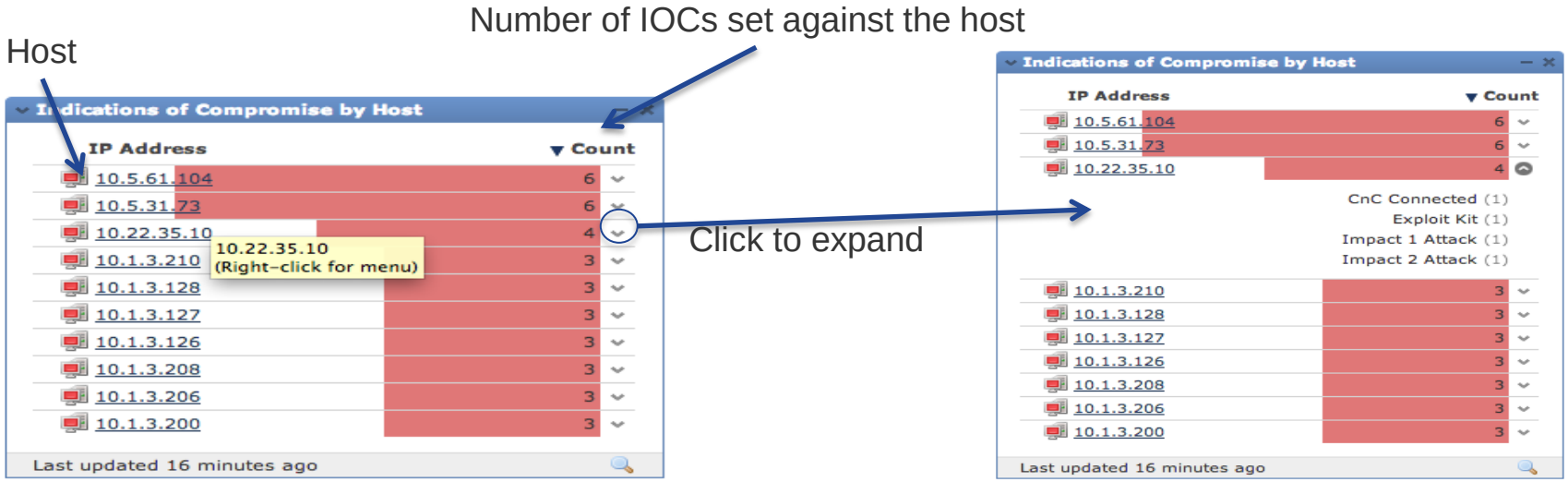
Correlates all intrusion events
to an impact of the attack against the target



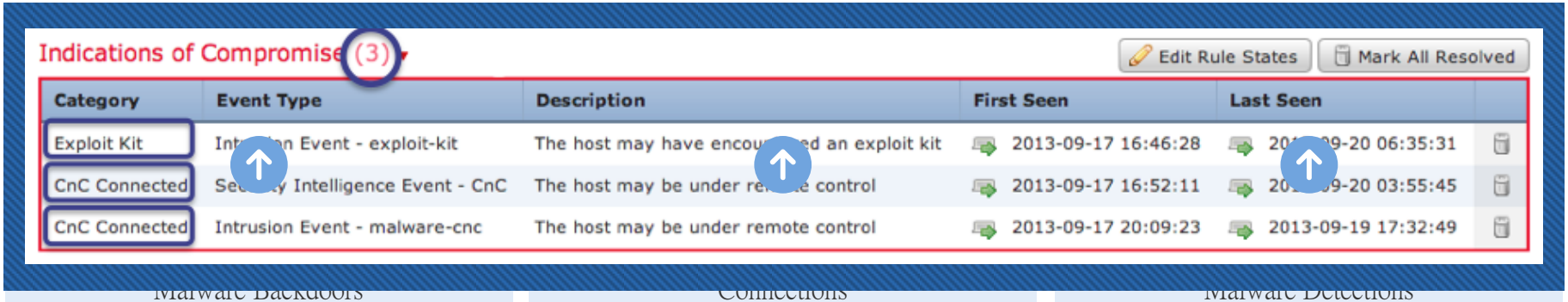
Impact Flag	Administrator Action	Why
1	Act immediately, vulnerable	Event corresponds to vulnerability mapped to host
2	Investigate, potentially vulnerable	Relevant port open or protocol in use, but no vuln mapped
3	Good to know, currently not vulnerable	Relevant port not open or protocol not in use
4	Good to know, unknown target	Monitored network, but unknown host
0	Good to know, unknown network	Unmonitored network

Indicators of Compromise (感染指標) Dashboard

- Because IOCs enable a quick way of classifying a host’ s potentially compromised state, having this data on a dashboard is desirable



Indicators of Compromise (感染指標)



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

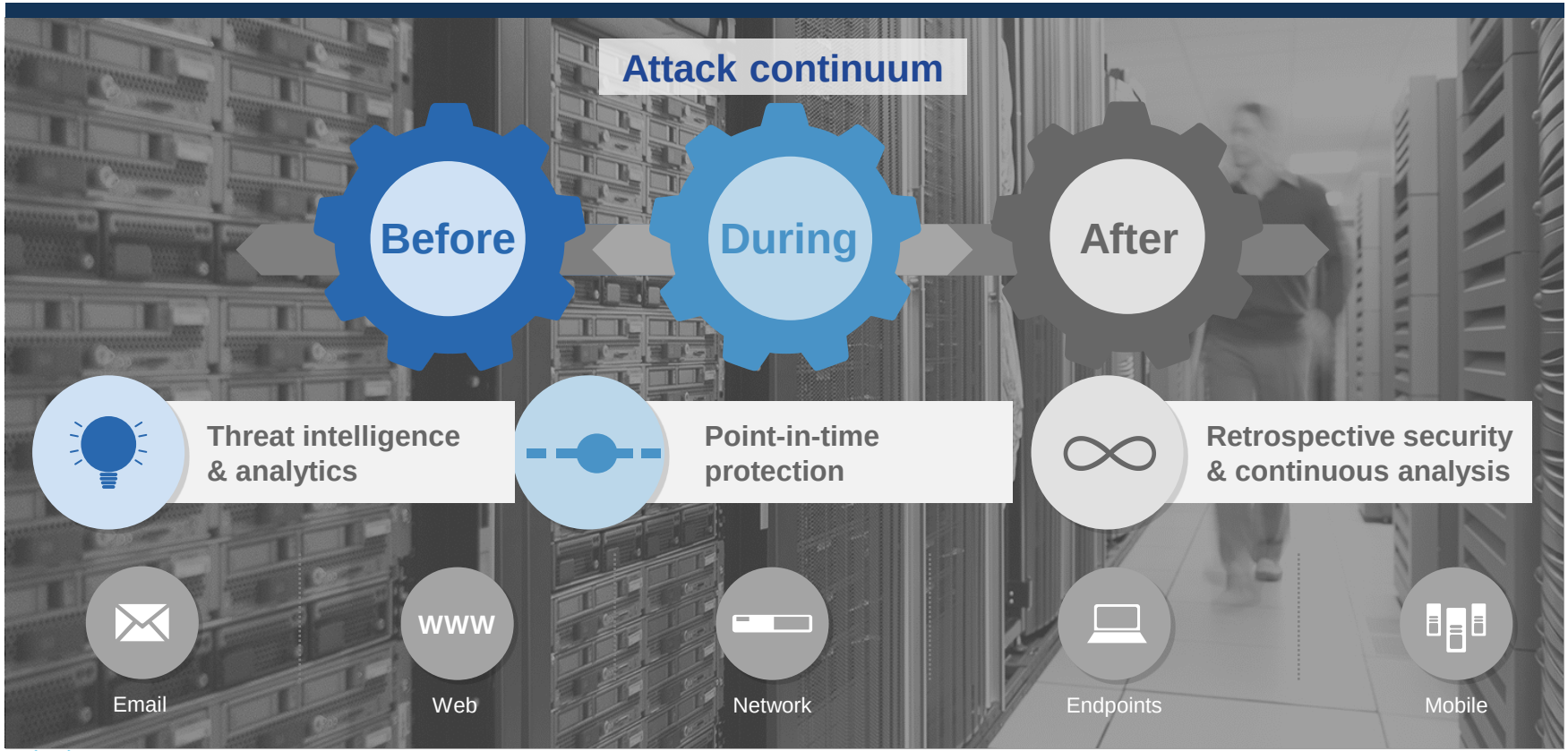
Dropper Infections

Advanced Persistent Threat & Advanced Malware

Is now a tool for financial gain

- Uses formal Development Techniques
  - Sandbox aware
  - Quality Assurance to evade detection
  - 24/7 Tech support available
- Has become a math problem
  - End Point AV Signatures ~20 Million
  - Total KNOWN Malware Samples ~100 M
  - AV Efficacy Rate ~50%

Cisco Advanced Malware Protection (AMP) across the entire attack continuum



Cisco Advanced Malware Protection

Built on unmatched collective security intelligence

Cisco® Collective Security Intelligence

1001 1101 1110011 0110011 101000 0110 00 1001 1101 1110011 0110011 101000 0110 00 0111000 111010011 101 1100001 110 101000 0110 00 0111 1100001110001110 1001 1101 1110011 0110011 101000 0110 00 1100001110001110

Cisco Collective Security Intelligence Cloud

Email Endpoints Web Networks IPS Devices

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

1.1 million incoming malware samples per day

AMP Community

Private/Public Threat Feeds

Talos Security Intelligence

AMP Threat Grid Intelligence

AMP Threat Grid Dynamic Analysis
10 million files/month

Advanced Microsoft and Industry Disclosures

Snort and ClamAV Open Source Communities

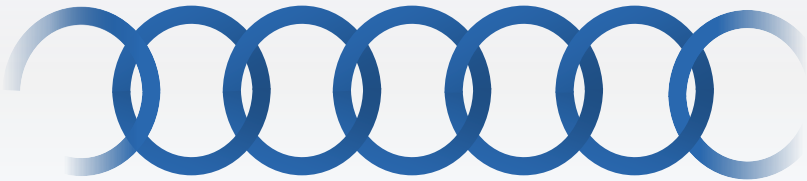
AEGIS Program

Automatic Updates in real time

AMP
Advanced Malware Protection

Cisco AMP Delivers A Better Approach

Point-in-Time Detection 一次性偵測 & Retrospective 回朔分析

Point-in-Time Protection 一次性偵測	Retrospective Security 回朔分析
	
File Reputation, Sandboxing	Continuous Analysis

Unique to Cisco® AMP

⊕ Possible ZeuS Variant Detected	Severity: 100	Confidence: 100
⊖ Process Modified an Executable File	Severity: 95	Confidence: 95

Malware will modify executables on a system, to hide logs or other evidence. Also, by modifying various executables it can disable functionality in the system which may detect or hamper the operation of the malware. Lastly, it may be attempting to hide an executable, so that it appears to be a legitimate file. Please review the 'Disk Artifacts' section in order to view additional details about this file.

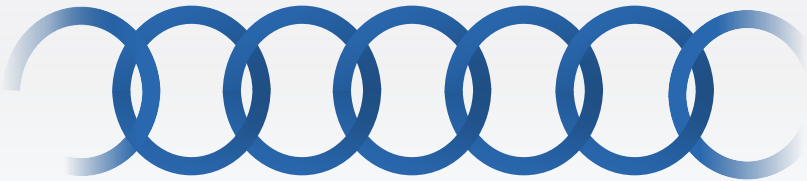
Categories persistence, obfuscation
Tags executable, file, process, PE

Path	Process Name	Process ID
\Documents and Settings\Administrator\Application Data\Byumqu\nayb.exe	LATEST_ZeuS.exe	1120 (LATEST_ZeuS.exe)

⊕ Process Modified Autorun Registry Key Value	Severity: 80	Confidence: 60
⊕ Process Modified File in a User Directory	Severity: 70	Confidence: 80
⊕ Potential Sandbox Detection - Enumeration of ProductID	Severity: 60	Confidence: 70
⊕ Process Created an Executable in a User Directory	Severity: 60	Confidence: 95
⊕ Command Exe File Execution Detected	Severity: 50	Confidence: 80
⊕ Potential Code Injection Detected	Severity: 50	Confidence: 50
⊕ Executable with Encrypted Sections	Severity: 30	Confidence: 30

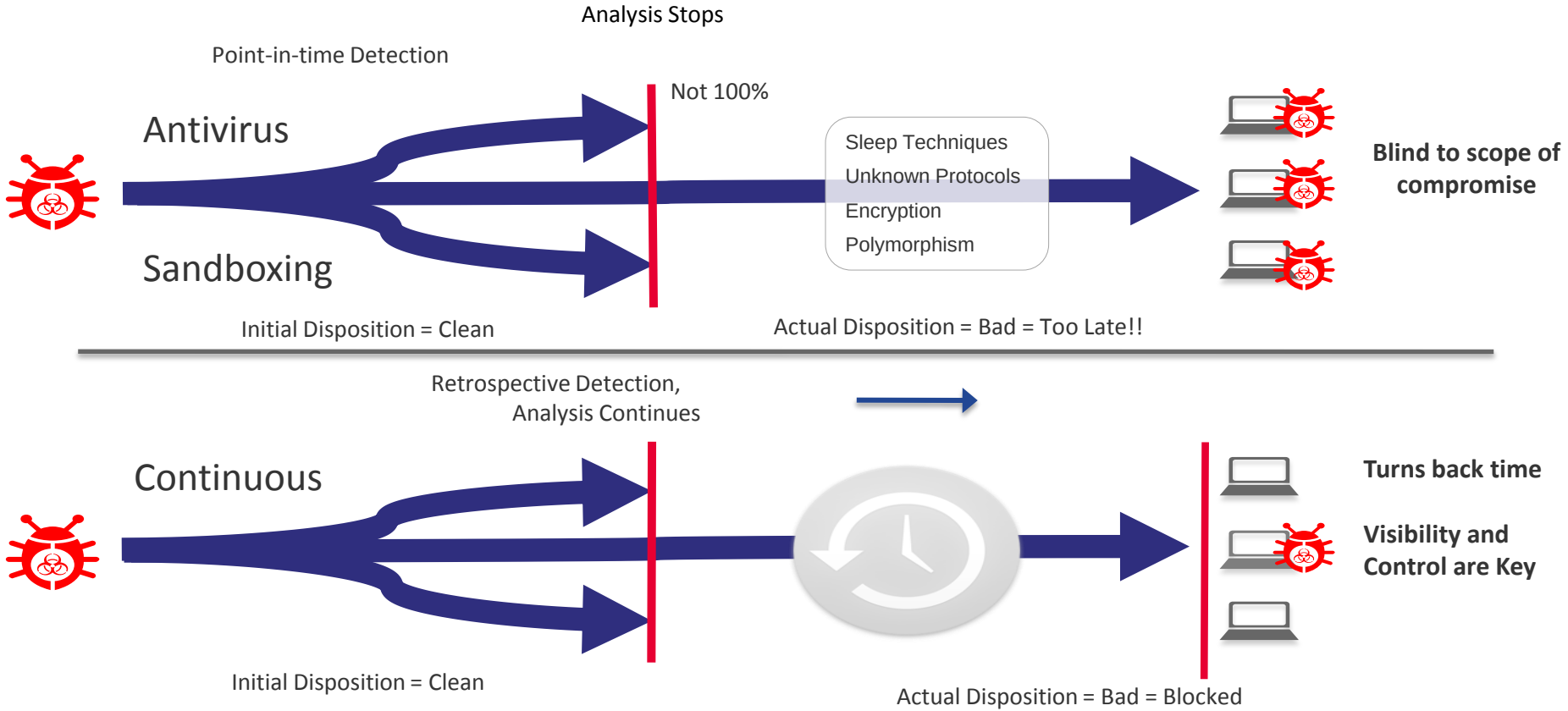
Cisco AMP Delivers A Better Approach

Point-in-Time Detection 一次性偵測 & Retrospective 回朔分析

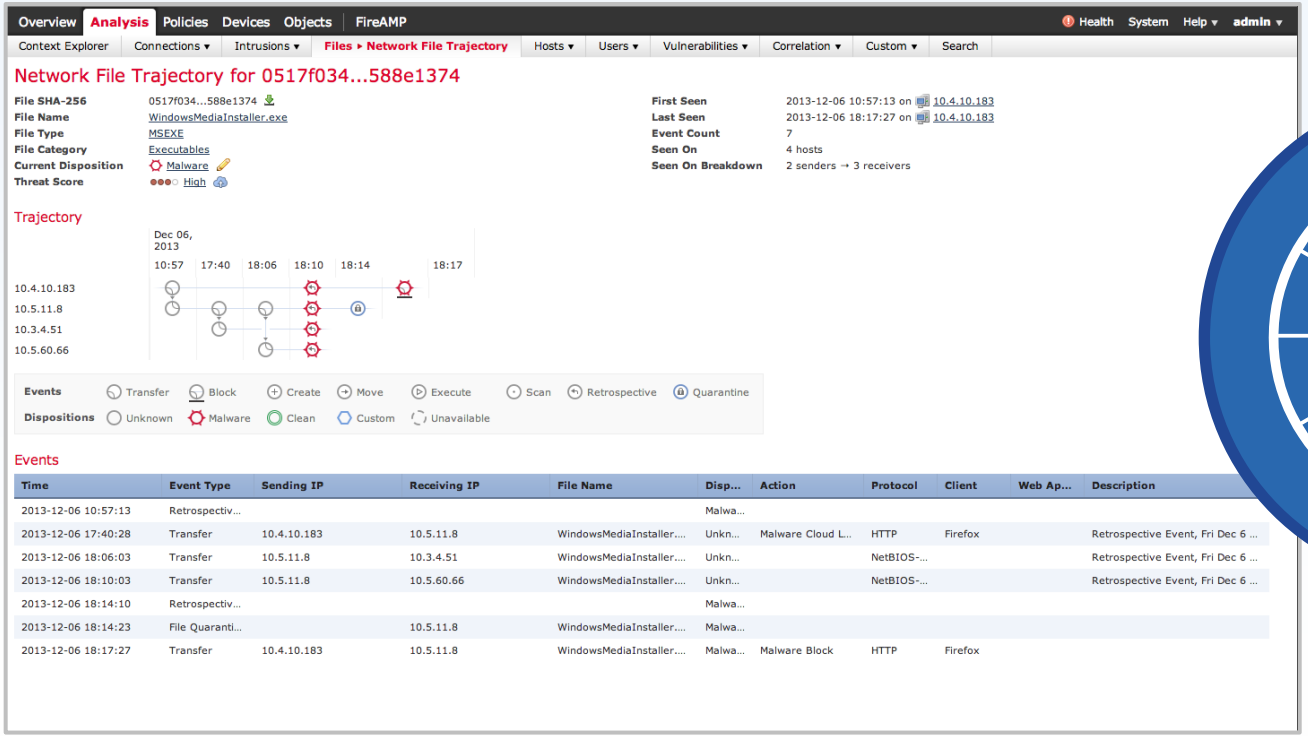
Point-in-Time Protection 一次性偵測	Retrospective Security 回朔分析
	
File Reputation, Sandboxing	Continuous Analysis

Unique to Cisco® AMP

Retrospective (可回朔）持續分析 vs. Point-in-Time Detection 一次性偵測



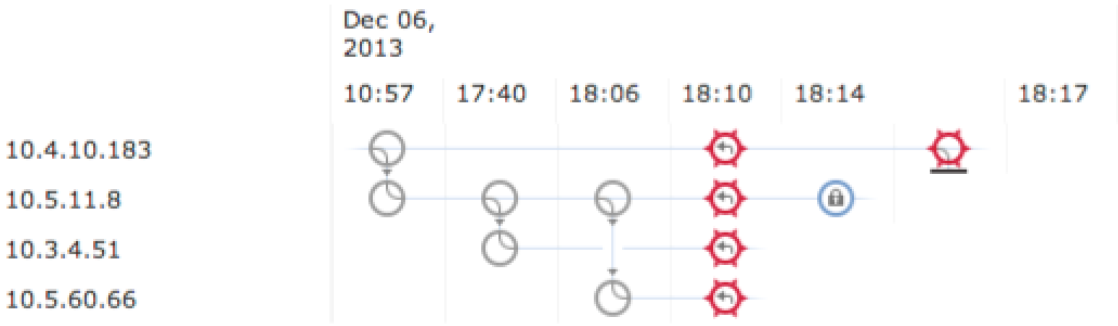
How Cisco AMP Works:
Network File Trajectory Use Case



Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374	**First Seen**	
File Name	WindowsMediaInstaller.exe	**Last Seen**	
File Type	MSEXE	**Event Count**	
File Category	Executables	**Seen On**	
Current Disposition	Malware	**Seen On Breakdown**	
Threat Score	High		

Trajectory



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

Dispositions Unknown | Malware | Clean | Custom | Unavailable

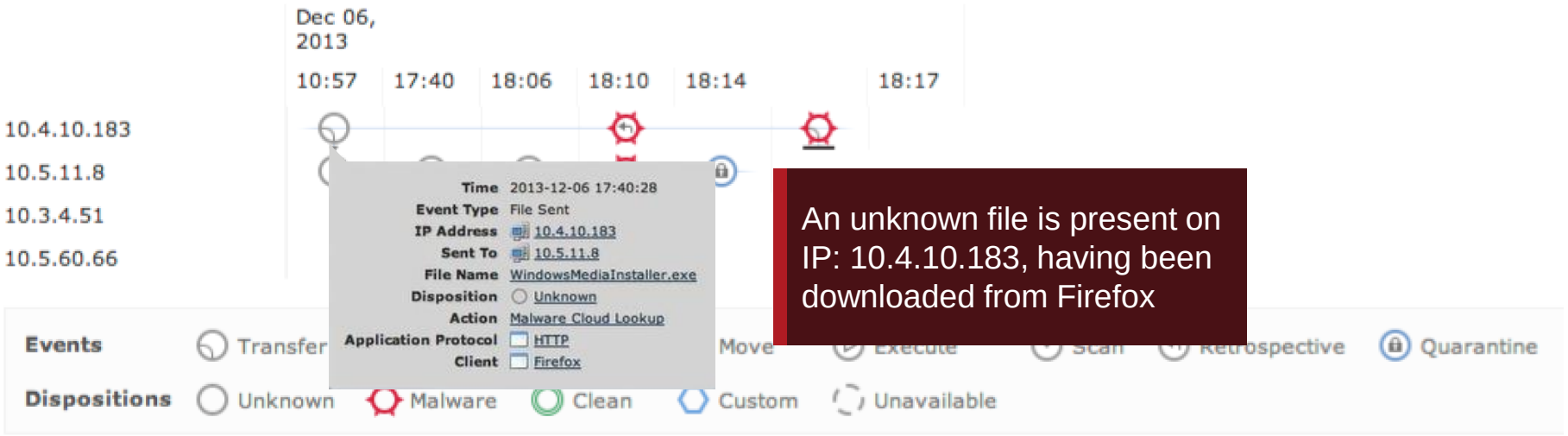
Overview | Analysis | Policies | Devices | Objects | FireAMP

Context Explorer | Connections ▾ | Intrusions ▾ | Files ▸ Network File Trajectory | Hosts ▾ | Users ▾ | Vulnerabilities ▾

Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374	**First Seen**	
File Name	WindowsMediaInstaller.exe	**Last Seen**	
File Type	MSEXE	**Event Count**	
File Category	Executables	**Seen On**	
Current Disposition	Malware	**Seen On Breakdown**	
Threat Score	High		

Trajectory

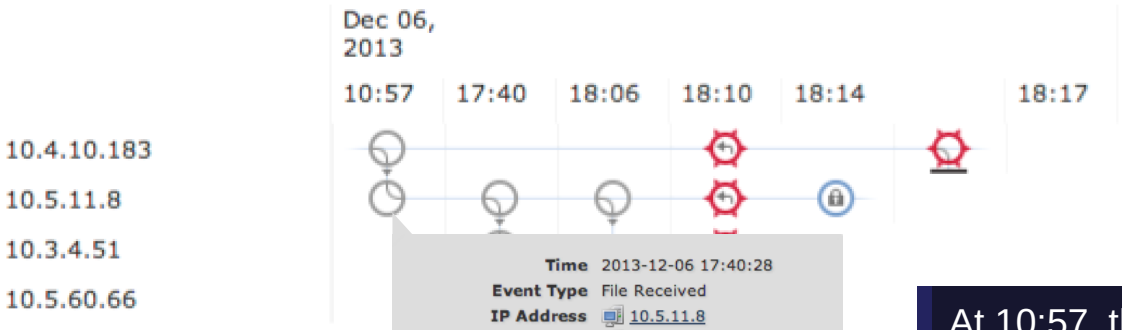


Network File Trajectory for 0517f034...588e1374

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

First Seen
Last Seen
Event Count
Seen On
Seen On Breakdown

Trajectory



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

Events Transfer ... Move ... ospective Quarantine

Dispositions Unknown ... Custom Unavailable

Overview | Analysis | Policies | Devices | Objects | FireAMP

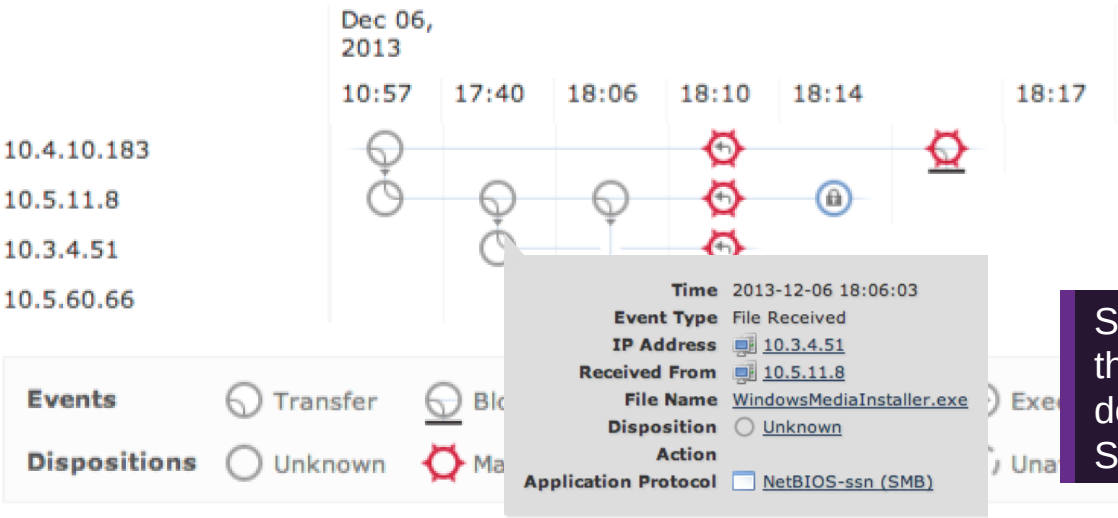
Context Explorer | Connections ▾ | Intrusions ▾ | Files ▸ Network File Trajectory | Hosts ▾ | Users ▾ | Vulnerabilities ▾

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
Last Seen
Event Count
Seen On
Seen On Breakdown

Trajectory



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

Overview | Analysis | Policies | Devices | Objects | FireAMP

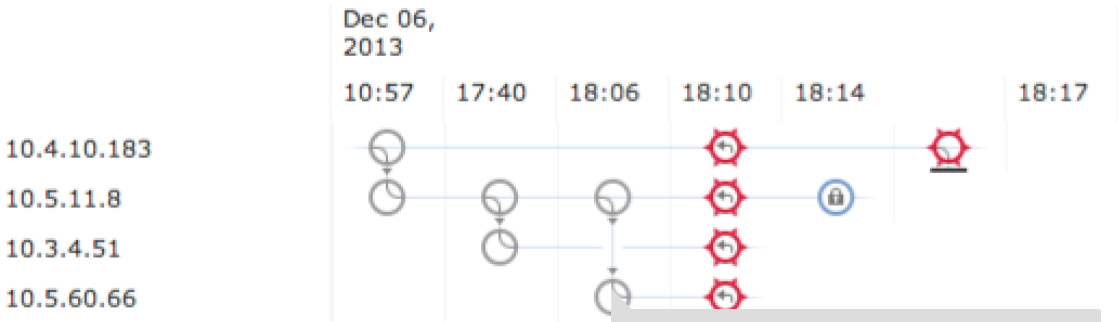
Context Explorer | Connections ▾ | Intrusions ▾ | Files ▸ Network File Trajectory | Hosts ▾ | Users ▾ | Vulnerabilities ▾

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
Last Seen
Event Count
Seen On
Seen On Breakdown

Trajectory



Events Transfer Block

Dispositions Unknown Malware

Quarantine

able

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

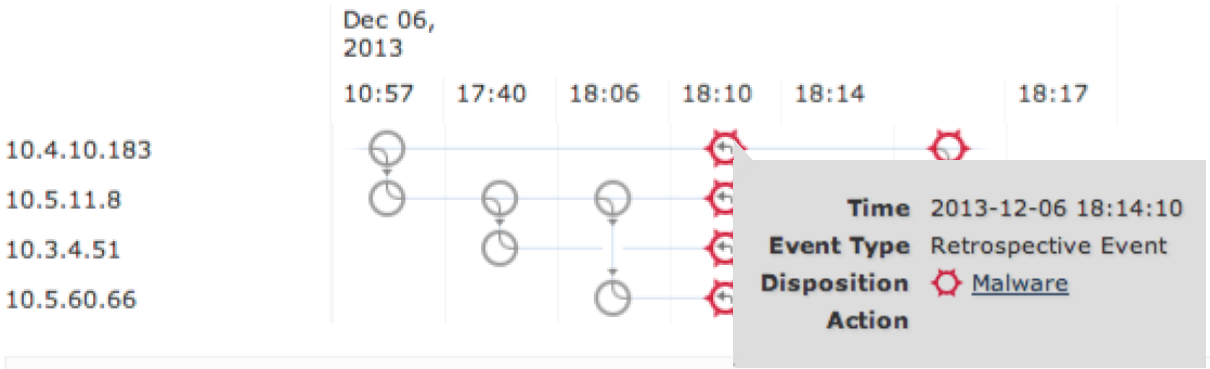
Overview | Analysis | Policies | Devices | Objects | FireAMP

Context Explorer | Connections ▾ | Intrusions ▾ | Files ▸ Network File Trajectory | Hosts ▾ | Users ▾ | Vulnerabilities ▾

Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374	**First Seen**	
File Name	WindowsMediaInstaller.exe	**Last Seen**	
File Type	MSEXE	**Event Count**	
File Category	Executables	**Seen On**	
Current Disposition	Malware	**Seen On Breakdown**	
Threat Score	High		

Trajectory



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

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

Dispositions Unknown | Malware | Clean | Custom | Unavailable

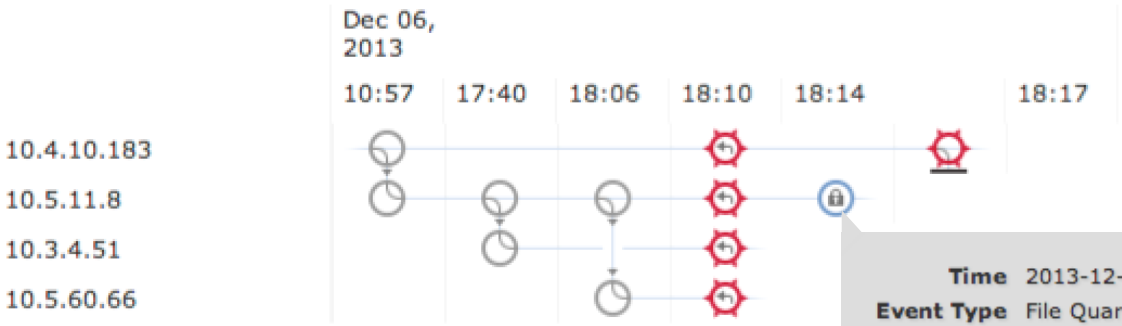
Overview | Analysis | Policies | Devices | Objects | FireAMP

Context Explorer | Connections ▾ | Intrusions ▾ | Files ▸ Network File Trajectory | Hosts ▾ | Users ▾ | Vulnerabilities ▾

Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374	**First Seen**	
File Name	WindowsMediaInstaller.exe	**Last Seen**	
File Type	MSEXE	**Event Count**	
File Category	Executables	**Seen On**	
Current Disposition	Malware	**Seen On Breakdown**	
Threat Score	High		

Trajectory



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

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 Transfer | Block | Create | Retrospective | Quarantine

Dispositions Unknown | Malware | Clean

Overview | Analysis | Policies | Devices | Objects | FireAMP

Context Explorer | Connections ▾ | Intrusions ▾ | Files ▸ Network File Trajectory | Hosts ▾ | Users ▾ | Vulnerabilities ▾

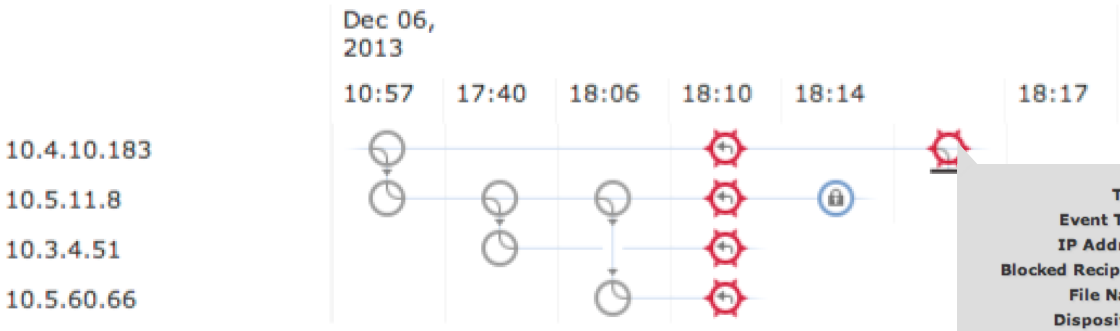
Network File Trajectory for 0517f034...588e1374

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

First Seen
Last Seen
Event Count
Seen On
Seen On Breakdown

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.

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 Transfer | Block | Create | Move | etrospective | Quarantine

Dispositions Unknown | Malware | Clean | Custom | Unavailable

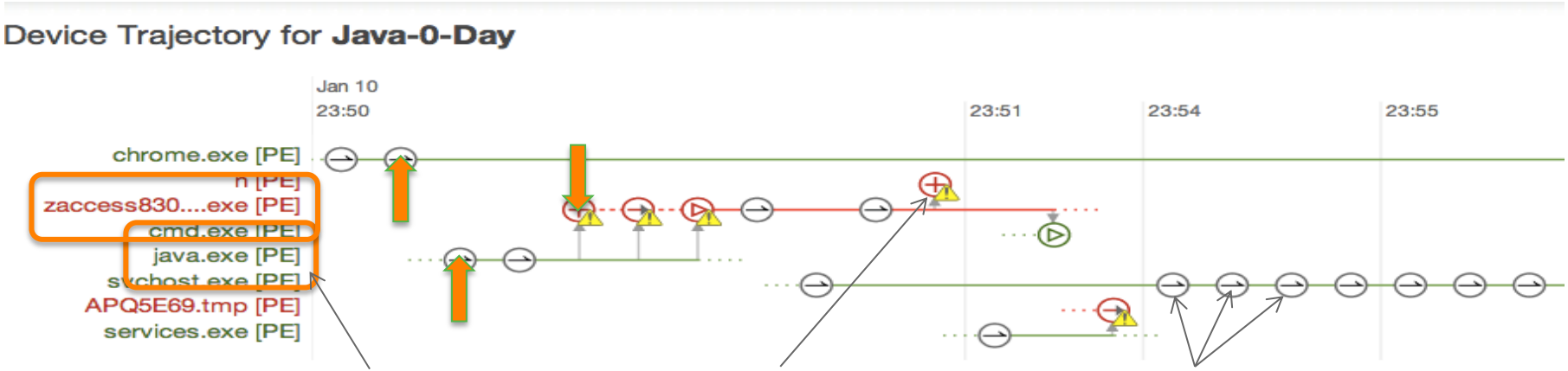
Device Trajectory

- Break the reinfection lifecycle with fast root cause analysis

Outgoing connection from Google Chrome 24.0.1312.52 (62ca2bc..59a3cb), most common filename chrome.exe, at TCP port 1156 to http://**10.180.0.144**:8888/exploit.html (10.180.0.144 port 8888).

Neutral disposition.

At 23:50:44, Thu Jan 10 2013 UTC



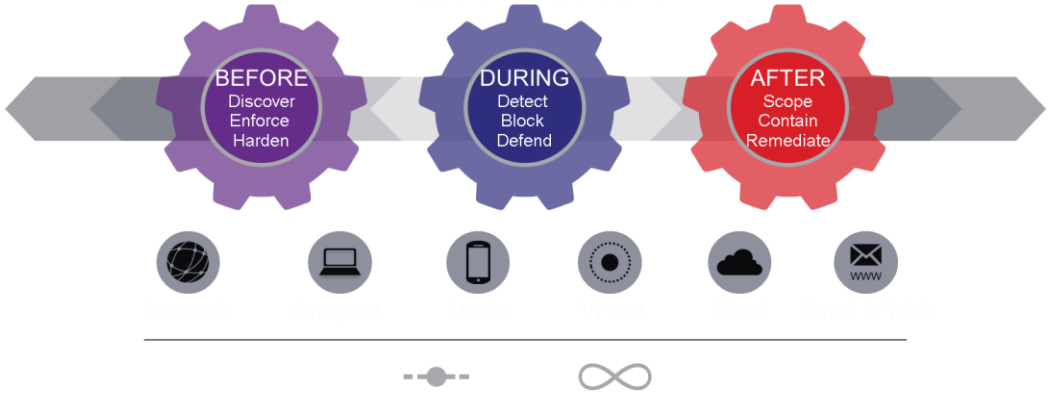
There Are Several Ways You Can Deploy AMP

AMP
Advanced Malware Protection

Deployment Options				
	Email and Web; AMP on Cisco® ASA CWS	AMP for Networks (AMP on FirePOWER Network Appliance)	AMP for Endpoints	AMP Private Cloud Virtual Appliance
Ideal for	New or existing Cisco CWS, Email /Web Security	IPS/NGFW/AMP Appliance	Windows, Mac, Android, virtual machines	High-Privacy Environments

Key Take Away

1. 能見度 (可視性)
2. 自動化
3. 可回溯、調查及鑑識



Point in Time Protection	Retrospective Security
File Reputation & Sandboxing	Continuous Analysis

TOMORROW starts here.

Thank You