Cisco Connect
Seoul, Korea
April 29-30, 2014

Threat Prevention with AMP (Advanced Malware Protection)

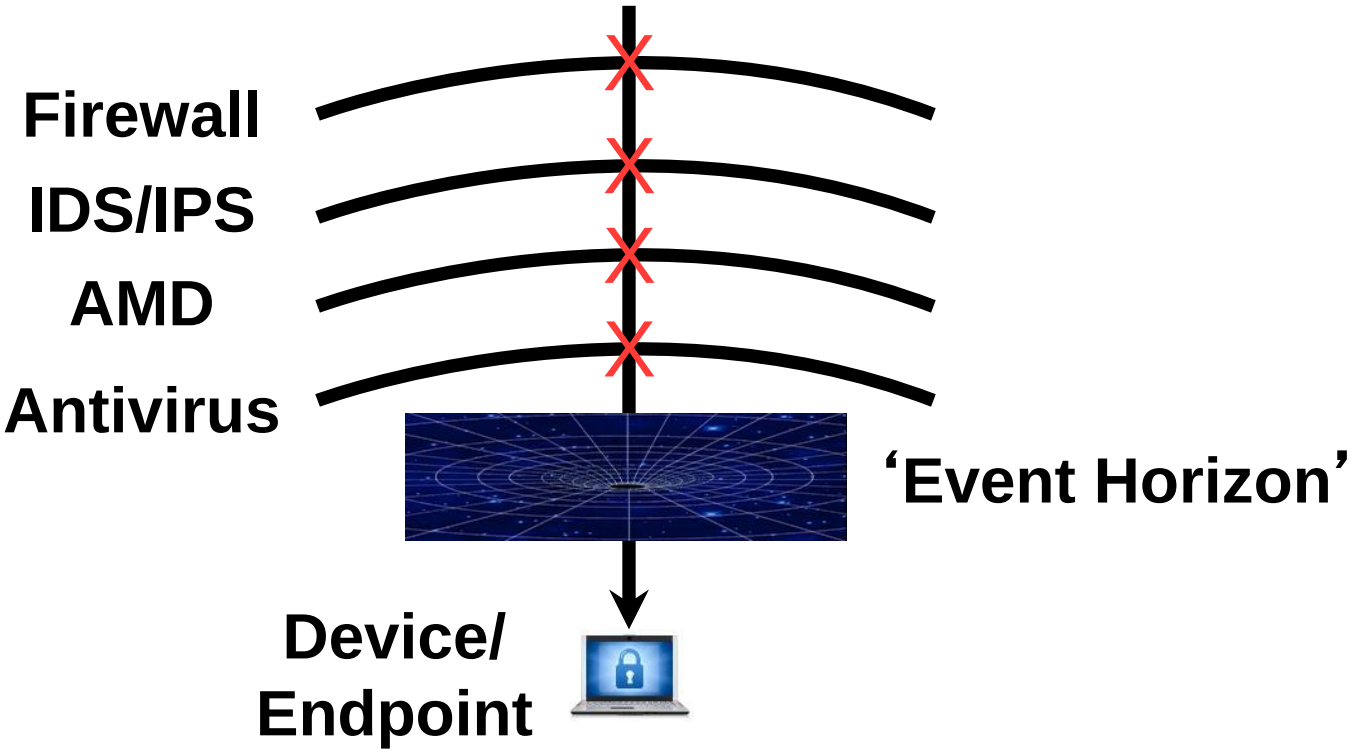
- **Gary Spiteri**
- gaspiter@cisco.com
- Cisco Systems

Agenda

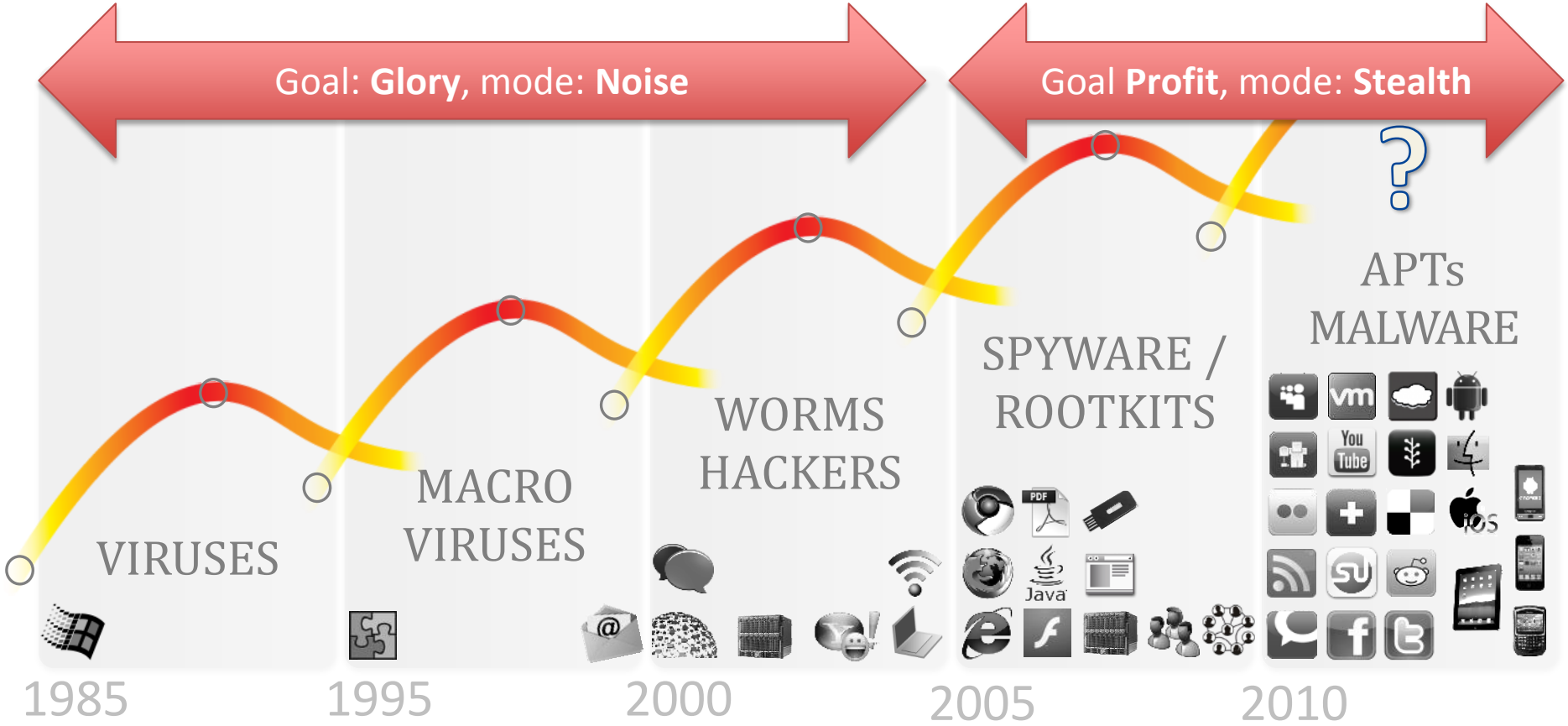
- The Malware Analysis Challenge
- Endpoint Malware Analysis
- Network Malware Analysis
- Host and Endpoint Correlation
- ZeroAccess Investigation (Supplemental Slides)

THE MALWARE ANAYLSIS CHALLENGE

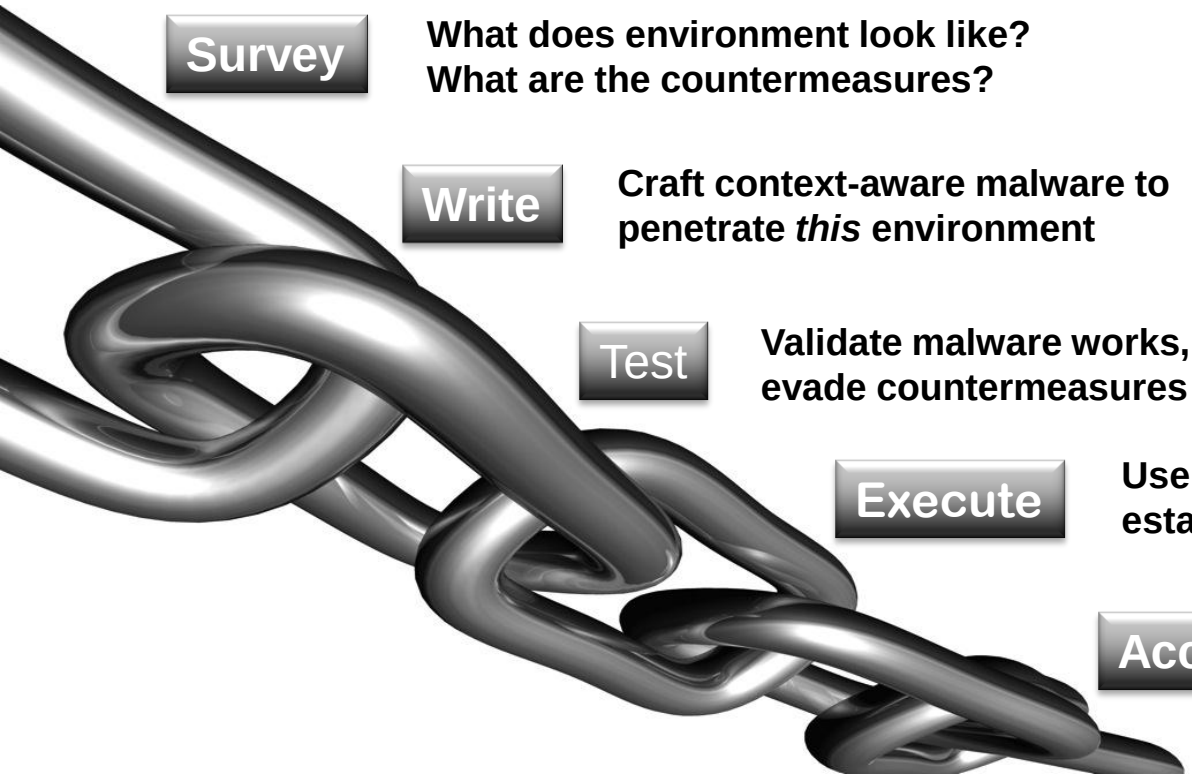
The Event Horizon



The Industrialisation of Hacking



Hacking, 21st Century Style – The Attack Chain



Survey

What does environment look like?
What are the countermeasures?

Write

Craft context-aware malware to penetrate *this* environment

Test

Validate malware works, can evade countermeasures

Execute

Use malware. Move laterally, establish secondary access,

Accomplish

The mission: Extract data, destroy, plant evidence, compromise.

Each stage may generate a *Weak Signal* indicating malicious activity.

We must find these signals in the noise.

Breaches Happen in Hours….

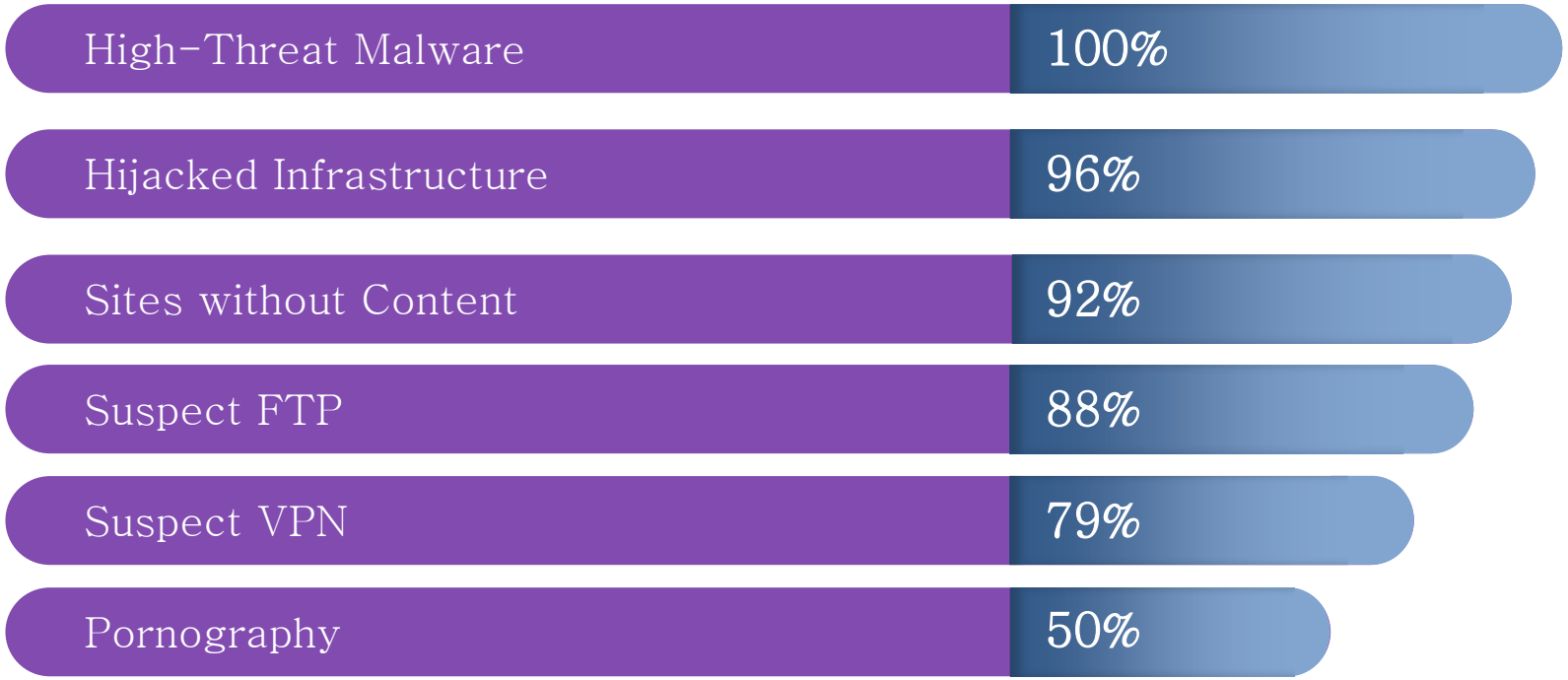
But Go Undetected For Weeks/Months

In 60% of breaches, data is stolen in hours.

85% of breaches are not discovered for weeks.

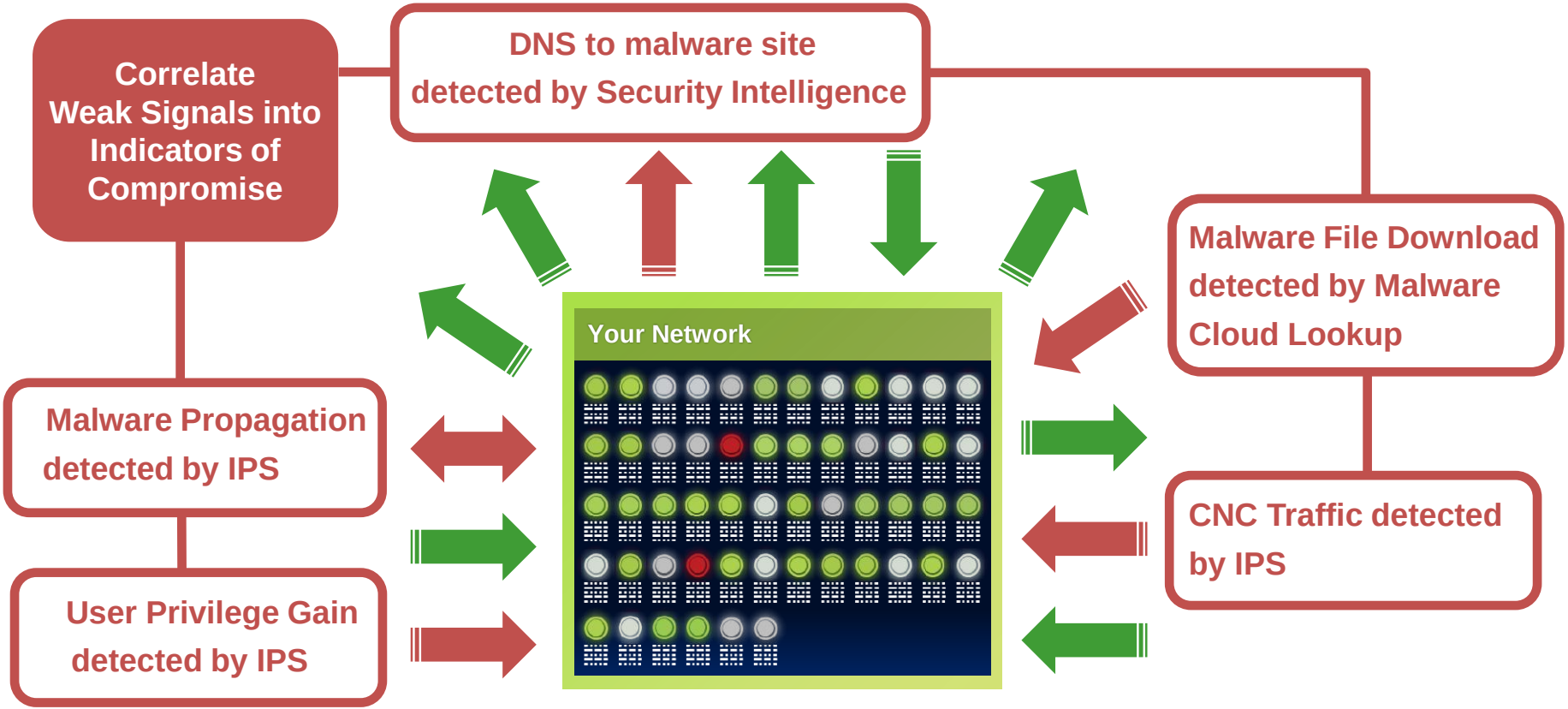
Timespan of events by percent of breaches – Source : Cisco Managed Threat Defense

The Pervasiveness of Malicious Traffic



Cisco Annual Security report

Correlating Weak Signals Into Indicators Of Compromise



"How would you do security differently if you knew you were going to be compromised?"

Martin Roesch

Sourcefire

Think differently about Security

Before

Reduce attack surface
Detect reconnaissance

During

Detect and prevent

EVENT HORIZON

Retrospective security

C O N T E X T U A L A W A R E N E S S

ENDPOINT MALWARE ANALYSIS

Sourcefire's Approach to Advanced Malware Protection

- Sourcefire AMP is not an Anti-virus solution
- Malware Analysis is a Big Data problem
- Collect as much information about Malware from the network and endpoint
- Aggregate this data into a cloud to take advantage of super-scale and collective intelligence
- Use machine learning and decision trees to process data and continuous datamine history
- Use this data to detect threats in realtime and retrospectively
- Use "Real-boxing" as the primary analysis system over Sand-boxing

Components of FireAMP

Visibility and Control

Mobile Connector

- Watches for apps
- Traps fingerprint & attributes

Lightweight Connector

- Watches for move/copy/execute
- Traps fingerprint & attributes

Web-based Manager

fireAMP™

- Transaction Processing
- Analytics
- Intelligence

Sensor / Connector Integration

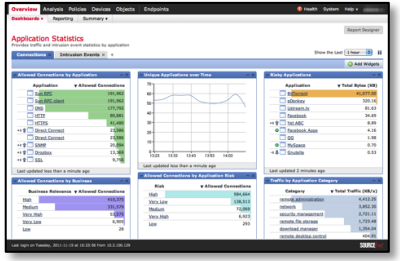
Network-based: AMP for firePOWER™

Detection
Analysis
Blocking

Device-based: fireAMP™

Detection
Analysis
Blocking
Remediation

fireSIGHT®



Collective
Threat
Intelligence

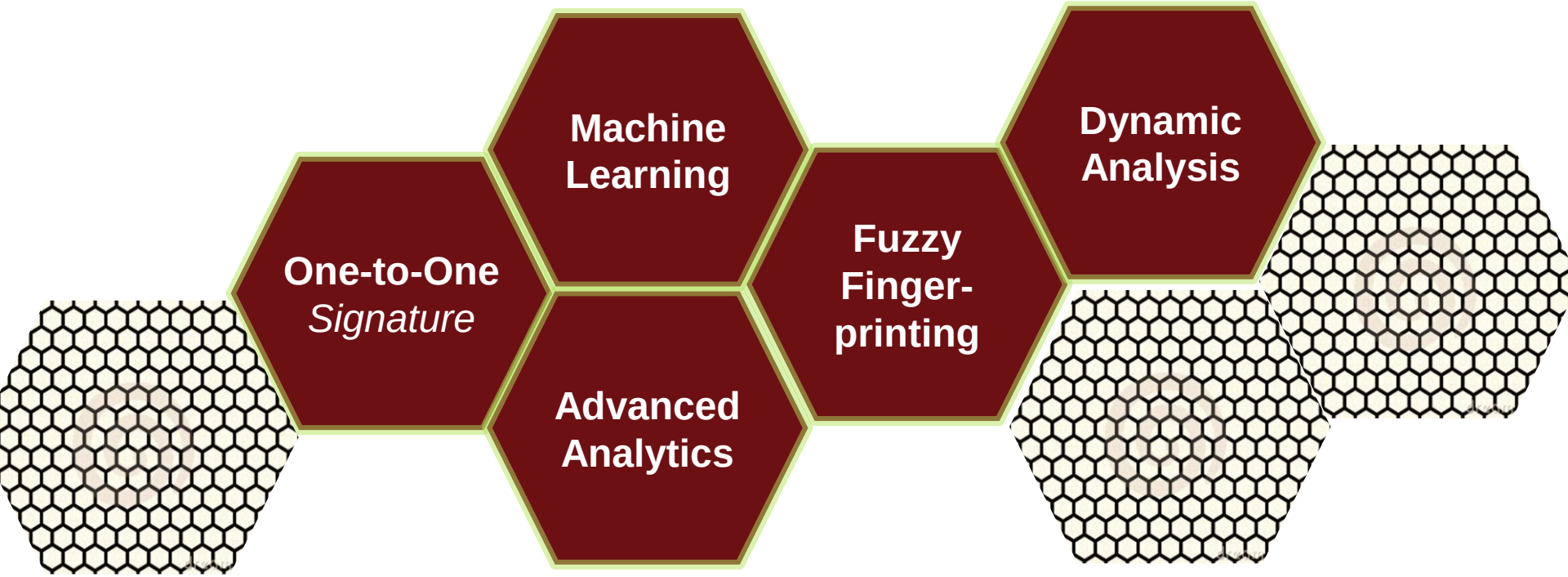
SOURCEfire®

REPUTATION

user
Device
IP
URL
domain

continuous
analysis

Cloud Detection Engines



One-to-One Signature Engine

- SHA256 Based Signature lookup
- Very fast Look Up (less then 200 milliseconds)
- Very fast distribution (realtime instantaneous)
- One-to-One matching
- Dispositions:
  - Known Good
  - Known Bad (block / quarantine)
  - Known Unknown (neither Good or Bad)
  - Never Seen Before
- Takes advantage of massive automated processing of third-party feeds and the 3+ million endpoint immunet community

Generic Signature Engine (ETHOS)

- Known as the Fuzzy Fingerprint
- One-to-Many matching
- Algorithmic detection engine
- Applied to Good and Bad Files
- Captures an infection and all variants
- Enables the Cloud to data-mine characteristics of good files and bad files
- Uses automated created of generic signatures

Machine Learning Engine (SPERO)

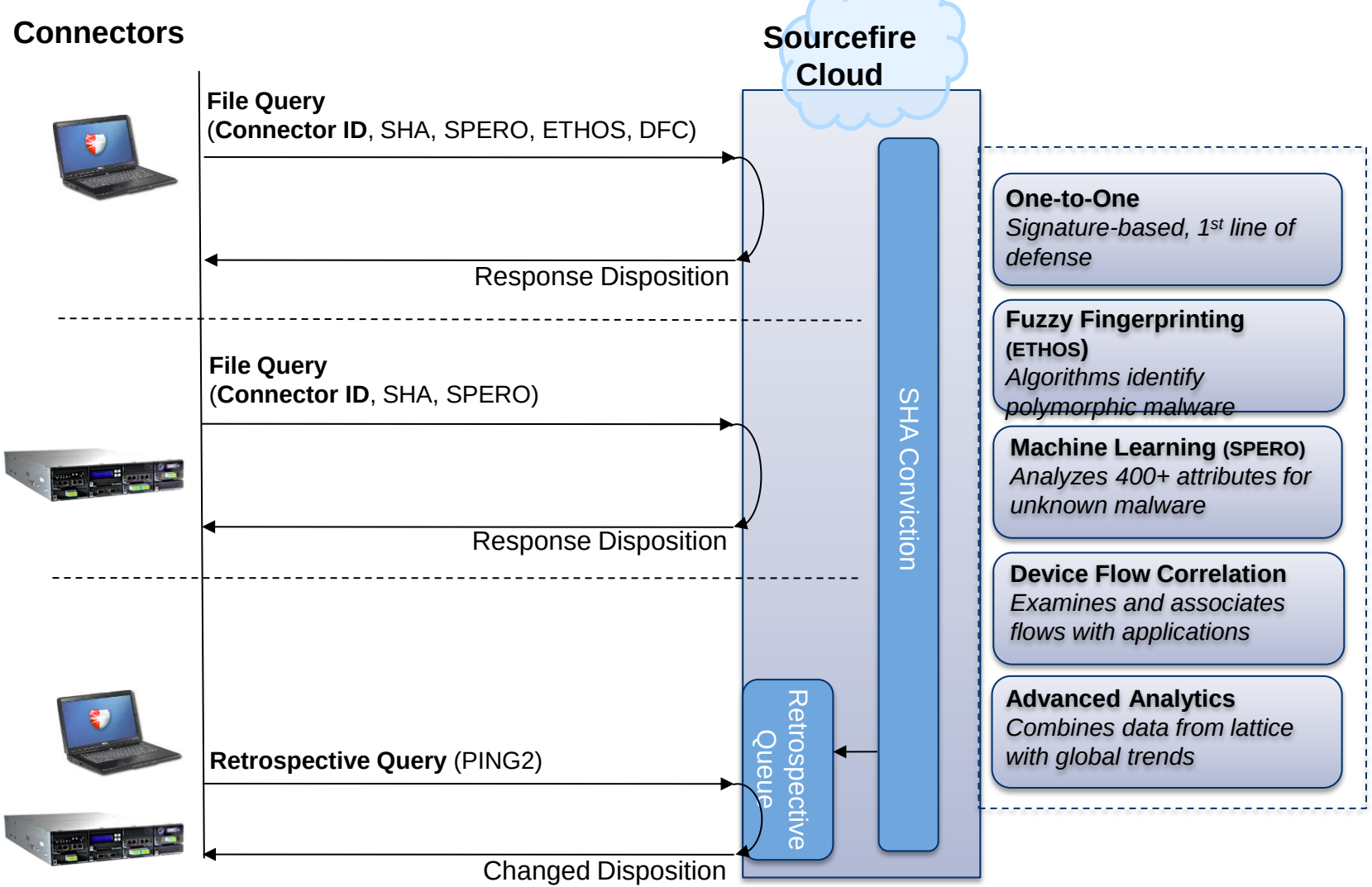
- Fast Heuristic Engine
- Classifies the PE from over 400 characteristics including:
  - PE Header
  - Referred DLLs
  - Common Object File Format (COFF) attributes
- Enables the Cloud to data-mine characteristics of good files and bad files
- Uses “Big Data” techniques to distinguish Good files from Bad files

Advanced Analytics Engine

- Takes a Global Intelligence approach (as opposed to file-centric approach)
- Uses patterns in all of the other engines collecting data
- Can identify new threats that normally can’t be detected
- Helps enhance ETHOS and SPERO by pushing a file from “may be malicious” to “malicious”
- Example: Drop Kick
  - If a File of Unknown disposition creates (drops) more malicious files than good files -> Make this file malicious

Device Flow Correlation

- Applications are tracked for first 100 connections
- Outbound and Inbound TCP/UDP
  - Localhost / Port / Protocol / Timestamp -> DestIP /Port / Protocol
- URL’s are tracked
- Domains are tracked (HTTP)
- Associated files downloaded over HTTP are tracked
- Internal network and external network monitored
- Can actively block connections against the VRT or custom black lists
- Detect and Block CNC and Attack Sites

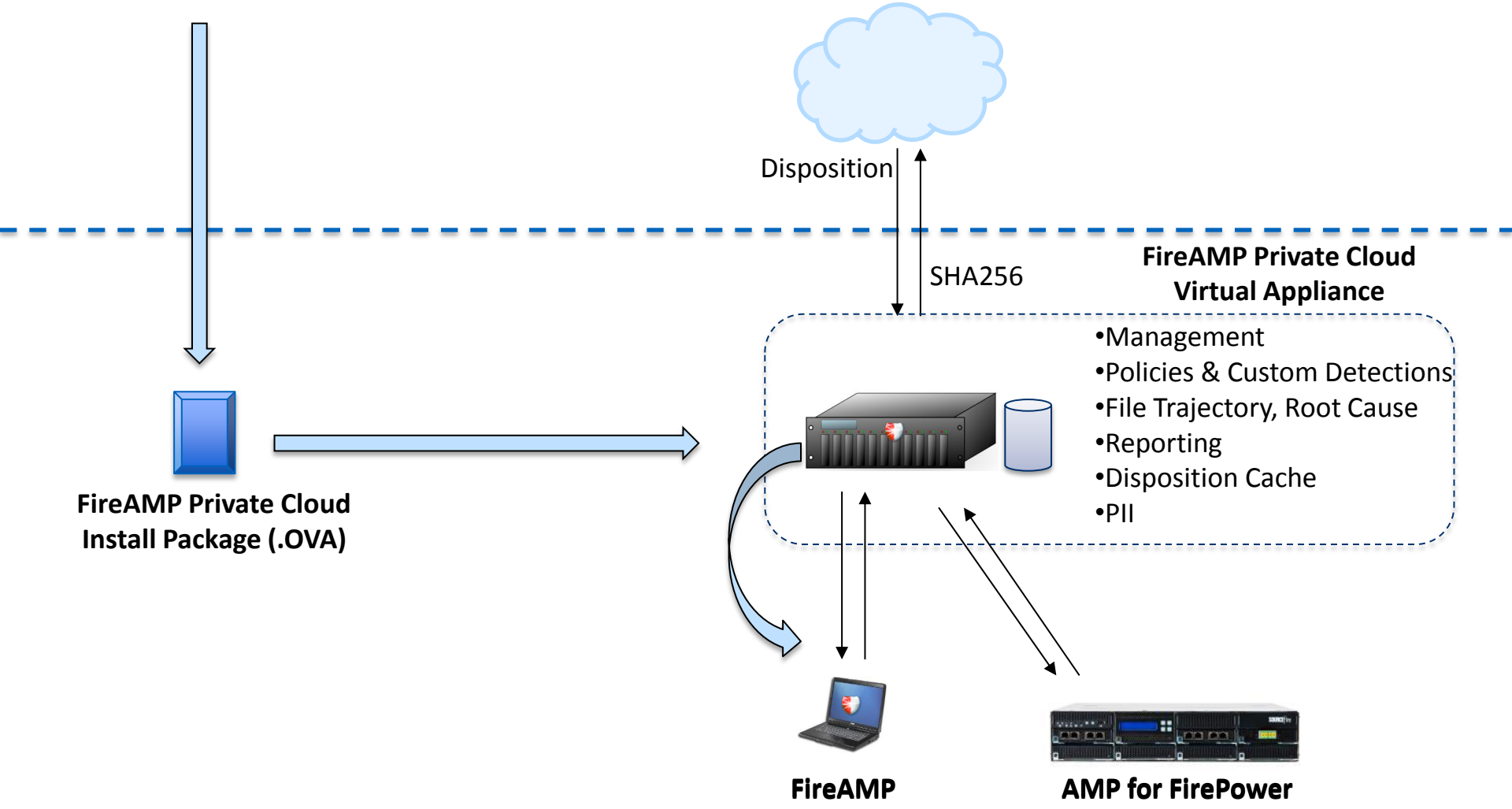

Connectors
Sourcefire Cloud
File Query
(Connector ID, SHA, SPERO, ETHOS, DFC)
Response Disposition
File Query
(Connector ID, SHA, SPERO)
Response Disposition
Retrospective Query (PING2)
Changed Disposition
SHA Conviction
Retrospective Queue
One-to-One
Signature-based, 1st line of defense
Fuzzy Fingerprinting (ETHOS)
Algorithms identify polymorphic malware
Machine Learning (SPERO)
Analyzes 400+ attributes for unknown malware
Device Flow Correlation
Examines and associates flows with applications
Advanced Analytics
Combines data from lattice with global trends

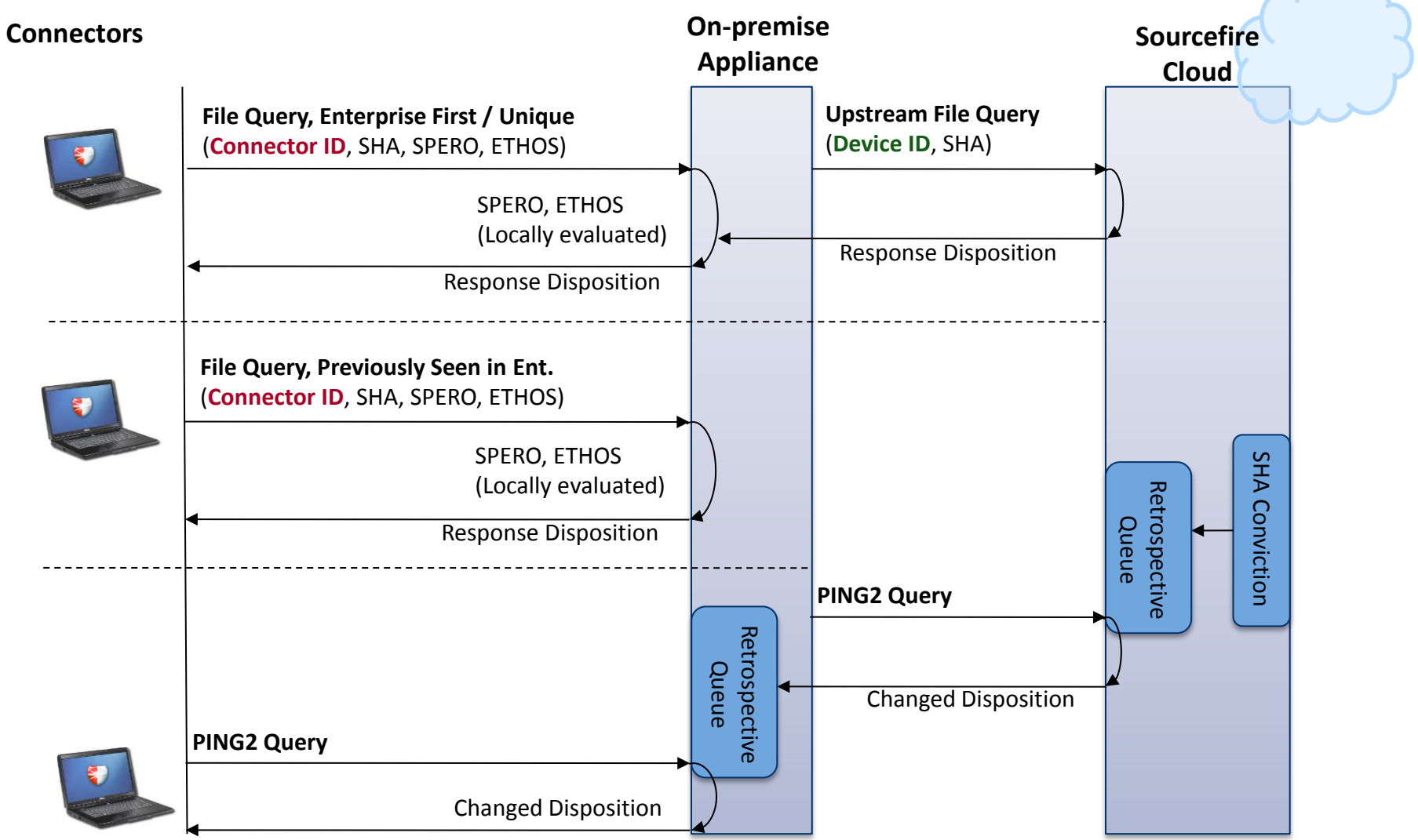
Data Produced

- **File Convictions**
  - Good
  - Bad
  - Unknown
- **File Trajectory**
  - How the file moves across the organisation over time
  - Patient Zero
- **Device Trajectory**
  - How files behave on an endpoint over time
  - Just like an Analyst’s Handbook
- **File Analysis**
  - Information on the nature of the file
- **Indicators of Compromise**

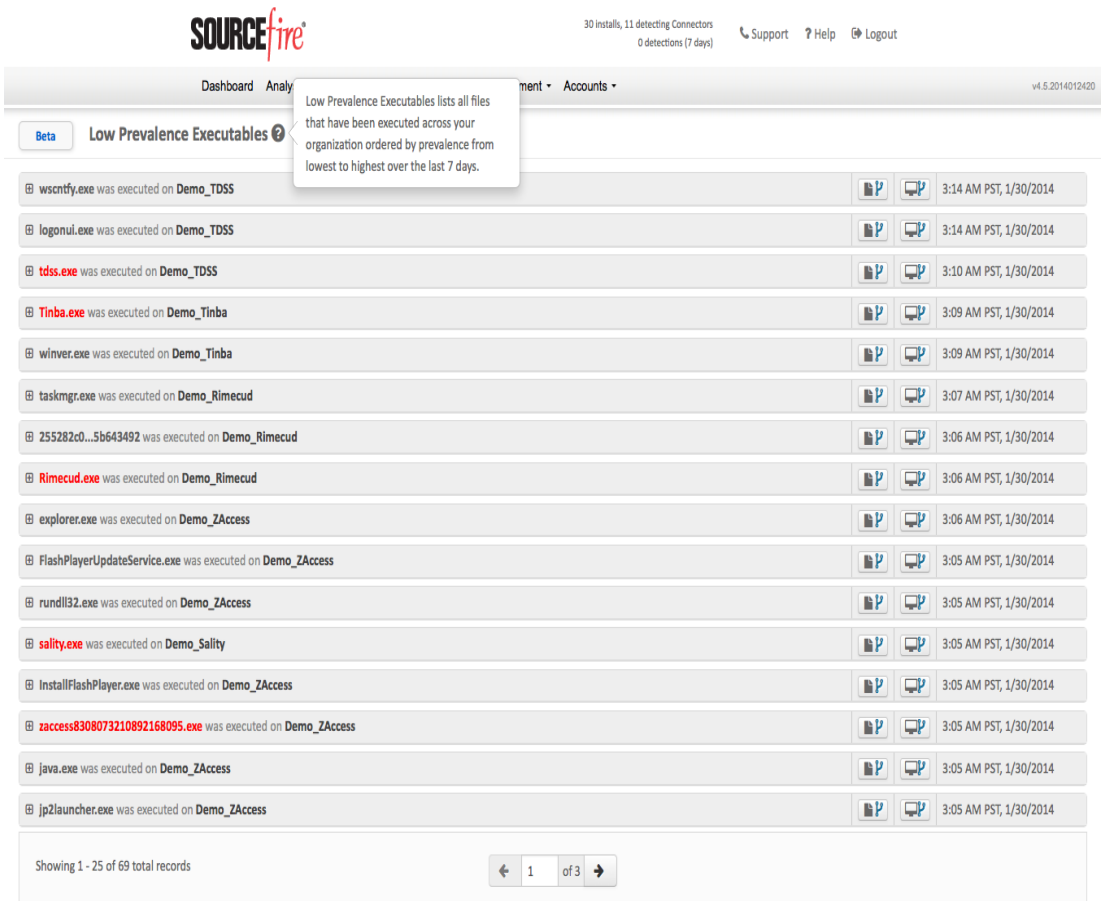
The AMP Private Cloud

- **FireAMP Cloud-in-a-(virtual) Box:**
  Virtual appliance that compresses FireAMP cloud portal and management into a single on-premises solution
- **Proxied Cloud:**
  Private Cloud will function as an anonymized proxy between connectors and our Public Cloud for file disposition look ups
- **Scale:**
  Each Private Cloud instance will support up to 10K connectors


Disposition
SHA256
FireAMP Private Cloud
Virtual Appliance
•Management
•Policies & Custom Detections
•File Trajectory, Root Cause
•Reporting
•Disposition Cache
•PII
FireAMP Private Cloud
Install Package (.OVA)
FireAMP
AMP for FirePower

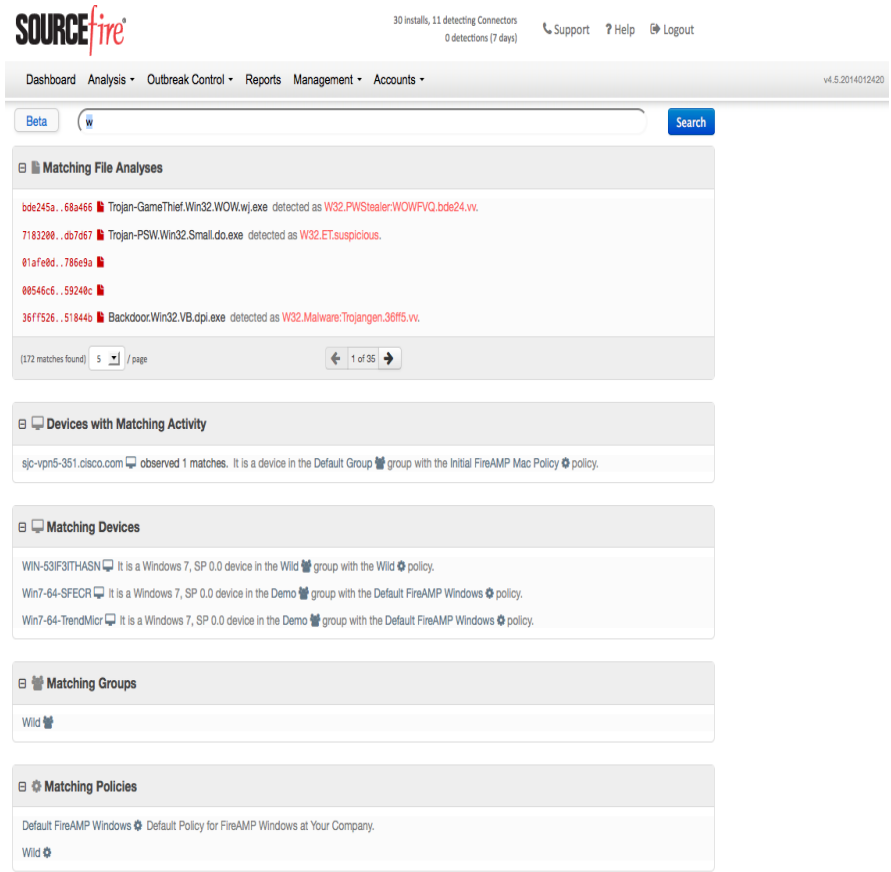

Connectors
On-premise Appliance
Sourcefire Cloud
File Query, Enterprise First / Unique
(Connector ID, SHA, SPERO, ETHOS)
Upstream File Query
(Device ID, SHA)
SPERO, ETHOS
(Locally evaluated)
Response Disposition
Response Disposition
File Query, Previously Seen in Ent.
(Connector ID, SHA, SPERO, ETHOS)
SPERO, ETHOS
(Locally evaluated)
Response Disposition
SHA Conviction
Retrospective Queue
PING2 Query
Retrospective Queue
Changed Disposition
PING2 Query
Changed Disposition

Low Prevalence Reports



- **Reports on Low Prevalence Executables**
- **Helps Identify Weak Signal Events**

Elastic Search



- **Quickly search entire FireAMP cloud based on any string length**

FIREAMP DEMO

NETWORK MALWARE ANALYSIS

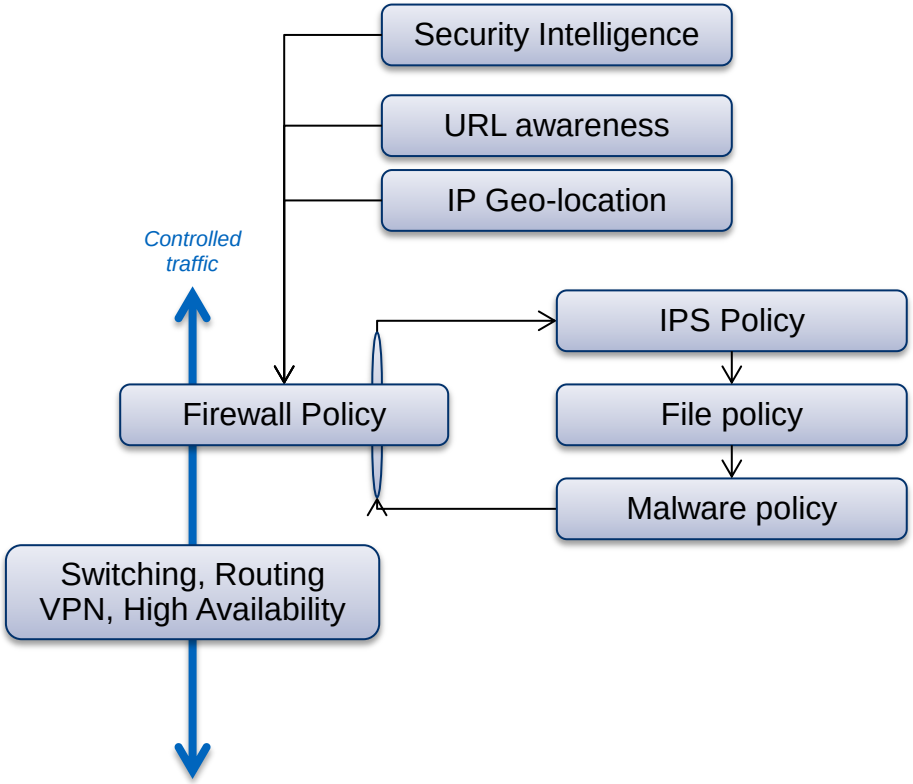
Detection Capabilities

Sourcefire Cloud

Security Intelligence IP Reputation, URL Category Updates	L2/L3	Connection Logs, Flows
Malware Cloud Lookups (AMP), Sandbox, Trajectories	Files	File Types, File Transfers
Application Definitions, App Detectors	AppID	Server, Client and Web Apps
Vulnerability Updates, OS Definitions	FireSIGHT	Discovery Events – Hosts, Users, OS, Services, Vulnerabilities
Snort Rule Updates	Snort	IDS/IPS Events – Snort Rule IDs

Policy Constructs

- **NGIPS** – content inspection
- **FireSIGHT** – context awareness
- **Security Intelligence** - blacklist co ntrol
- **Comprehensive access control**
  - By network zone, VLAN, IP, port, prot ocol, application, user, URL, Geo
- **Seamlessly integrated**
  - With IPS policies
  - File control policies
  - Malware policies



Event Types

- **Connection Events** – Source, Destination, Port, User, URL, App, Proto, User
- **Discovery Events** – OS, Client App, Service, Server, Usernames
- **Intrusion Events** – Snort Rule ID, Impact, Source, Destination, Packet Level
- **File Events** – Filename, File Type, Direction, Client App, Protocol
- **Correlation Events** – White List / Black List compliance
- **Security Intelligence Events** – IP Reputation
- **Malware Events** – Malware Cloud Lookups, FireAMP Endpoint events
- **Network File Trajectories** – Tracking of Files as they traverse the network

Context through FireSIGHT

- FireSIGHT discovers Host, Application and User information in realtime, continuously, passively
- Derives a worst-case Vulnerability Map of the monitored Network
- Correlates all Intrusion Events to an Impact of the attack against the target
- Drastically reduces False Positives, eliminates False Negatives

IMPACT FLAG RATING	ADMINISTRATOR ACTION
1	Act Immediately, Vulnerable
2	Investigate, Potentially Vulnerable
3	Good to Know, Currently Not Vulnerable
4	Good to Know, Unknown Target
0	Good to Know, Unknown Network
B	Good to Know, Blocked

Dynamic Analysis: Process Overview

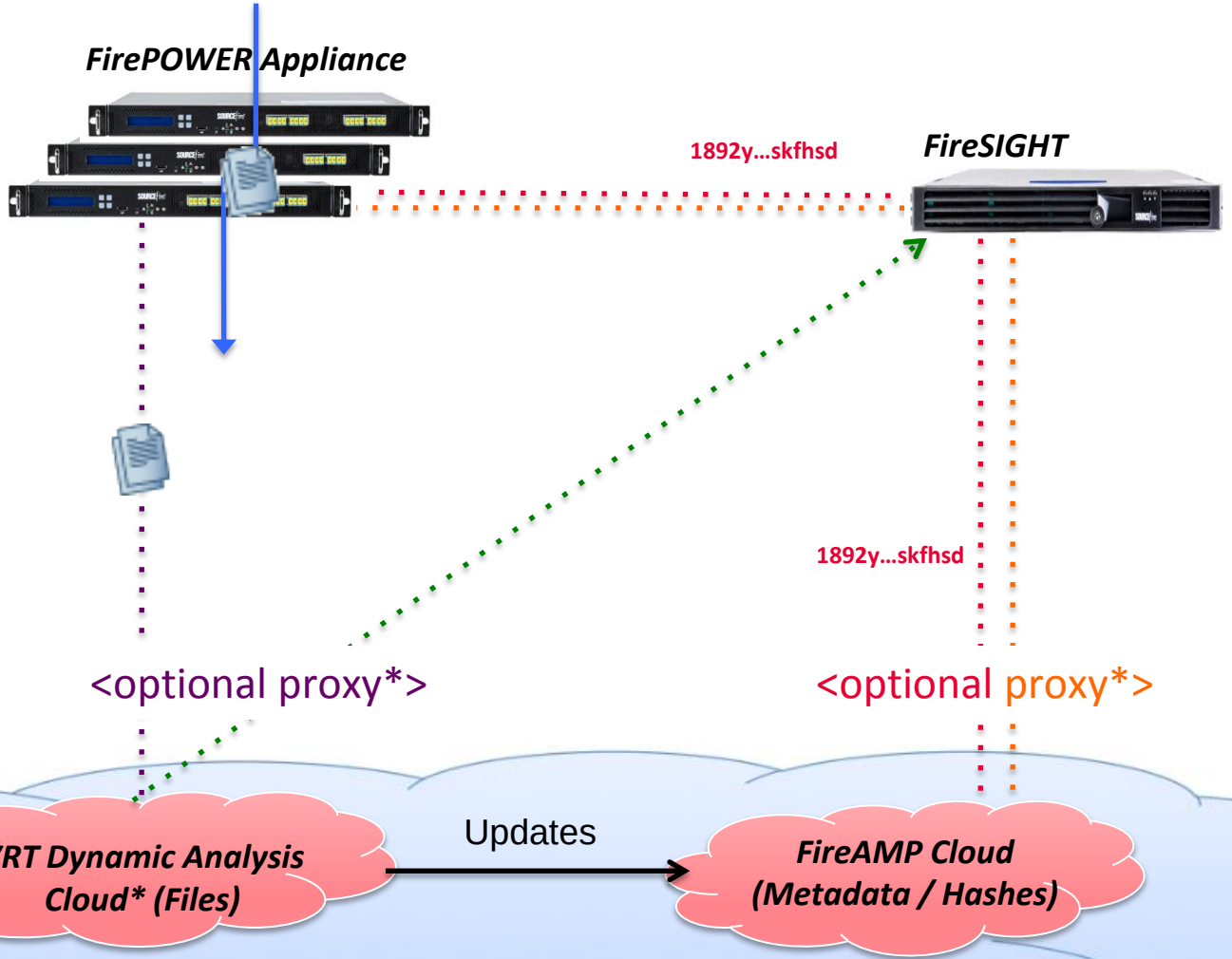
File Detected on FirePOWER
- Calculates hashes
- Saves a copy if policy dictates*

Hash metadata sent to AMP Cloud

AMP Cloud Response: E.g.
- Disposition = Unknown
- Threat Score = Unknown *

File is sent to VRT Services Cloud for Dynamic Analysis* (if policy dictates)

Dynamic analysis:*
- Analysis queue Status
- Error Status
- Threat Score



NETWORK AMP DEMO

HOST AND ENDPOINT CORRELATION

Sourcefire AMP Detection Systems

- 1-to-1 File Matching from the cloud (**Network** and **Endpoint**)
- IP Reputation Matching from the cloud (**Network - Security Intelligence Feed**, **Endpoint - Device Flow Correlation**)
- SPERO Fuzzy File Matching from the cloud (Network and **Endpoint**)
- Vulnerability-facing Traffic Rules (**Network**)
- Malware Propagation Detections Rules (**Network**)
- CnC Blacklist Rules (**Network**)
- Cloud-based machine learning engines (supports the **Network** and **Endpoint**)
- Custom File Detections (**Endpoint**)
- Custom File Blocking (**Network**)
- Application Control (**Network**)
- Application Execution Blocking (**Endpoint**)
- File Quarantine (**Endpoint**)
- Network File Trajectory (**Network**)
- Device Trajectory (**Endpoint**)
- File Trajectory (**Endpoint**)
- Cloud-based Sandboxing (supports the **Network** and **Endpoint**)
- Indication of Compromise correlation (**Network** and **Endpoint**)
- Passive Device Discovery (**Network**)
- URL Detection and Control (**Network**)

Host and Event Correlation

- Today we have many different ‘event’ sources in Defense Center. For example:
  - IPS events (**Snort**)
  - FireAMP events (**endpoint**)
  - Malware events (**network**)
  - Security Intelligence (**network** + **endpoint**)
- Different events can tell an analyst different things about the state of a host or the network
  - Has it been targeted a type of network attack (**snort**)
  - Has it downloaded malware? (**Snort**, **FireAMP**, **Malware**)
  - Has it executed malware (**FireAMP**)
  - Has it connected to a CNC server (**Snort**, **FireAMP**, **SI**)
- This feature combines these event sources and correlates them based on the hosts involved with the events

Indicators of Compromise Table

- Shows all IOCs set on all Hosts over the network
  - Workflow: Hosts with the most IOCs set (most likely compromised) - Good dashboard widget for this as well
  - Actions you can take on this table:
    - View the Host Profile
    - Mark the IOC as resolved
    - Drill into the triggering event(s)
- Events can different sources all sit in this table
  - Example: CNC via SI, CNC via FireAMP, CNC via Snort
- New Host Icon used for when host has displayed IOCs

No IOCs set

Has IOCs set

Example IOC

- **IOC Tag Category:** *“CNC Connected”*
- **Description:** *“This host may be under remote control”*
- **What could set this tag?**
  - **Security Intelligence**: A host connects to a device marked as a CNC server
  - **IPS event**: An IPS event from the category “Malware-CNC” is triggered by this host
  - **FireAMP event**: FireAMP detects that a device may have connected to a CNC server via DFC

IOC Host Profile View

Host Profile

Scan Host | Generate White List Profile

IP Addresses	**10.5.61.104** (wolfe.englab.sourcefire.com)
NetBIOS Name	
Device (Hops)	mango.englab.sourcefire.com (0)
MAC Addresses (TTL)	00:D0:03:13:88:00 (COMDA ENTERPRISES CORP.) (254) **90:B1:1C:25:9F:55 (Dell Inc.) (255)** BA:EA:5E:3D:DE:F7 (61) 00:50:56:90:70:8A (VMware, Inc.) (62)
Host Type	Router
Last Seen	2013-09-20 06:40:44
Current User	
View	Context Explorer | Connection Events | Intrusion Events | File Events | Malware Events

Indications of Compromise (3) = 3

Edit Rule States | Mark All Resolved

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	

Systems (4)

Edit Operating System | View Operating Systems

Hardware	OS Vendor	OS Product	OS Version	Source
	Google	Chromium	3701.81.2	FireSIGHT

IOC Table

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

Context Explorer | Connections ▾ | Intrusions ▾ | Files ▾ | Hosts ▸ Indications of Compromise | Users ▾ | Vulnerabilities ▾ | Correlation ▾ | Custom ▾ | Search

- Network Map
- Hosts
- Indications of Compromise
- Applications
- Application Details
- Servers
- Host Attributes
- Discovery Events

Bookmark This Page | Report Designer | View Bookmarks | Search

Indications of Compromise by Host (switch

Indications of Compromise by Host › Table View of Indications of

No Search Constraints (Edit Search)

Jump to... ▾

IP Address	Category	Event Type	Description	First Seen	Last Seen
10.5.1.18	Impact 2 Attack	Impact 2 Intrusio	The host was attacked and is potentially vulnerable	2013-09-17 12:56:32	2013-09-17 13:26:58
10.5.30.108	Impact 2 Attack	Impact 2 Intrusion Event - attempted-admin	The host was attacked and is potentially vulnerable	2013-09-17 12:56:32	2013-09-17 13:26:58
10.5.61.152	Impact 2 Attack	Impact 2 Intrusion Event - attempted-user	The host was attacked and is potentially vulnerable	2013-09-17 13:20:32	2013-09-17 13:20:32
10.5.32.191	Impact 2 Attack	Impact 2 Intrusion Event - attempted-user	The host was attacked and is potentially vulnerable	2013-09-17 13:18:02	2013-09-17 13:18:02
10.6.12.72	Impact			45	2013-09-17 13:17:02
10.5.32.162	Impact			02	2013-09-17 13:17:02
10.22.75.18	CnC Co			49	2013-09-17 13:16:49

Triggering Event Summary

Source Security Intelligence Events

Initiator IP	Responder IP	Security Intelligence Category	Application Protocol
10.22.75.18	54.230.192.199	CnC	Unknown

View Security Intelligence Event

Close

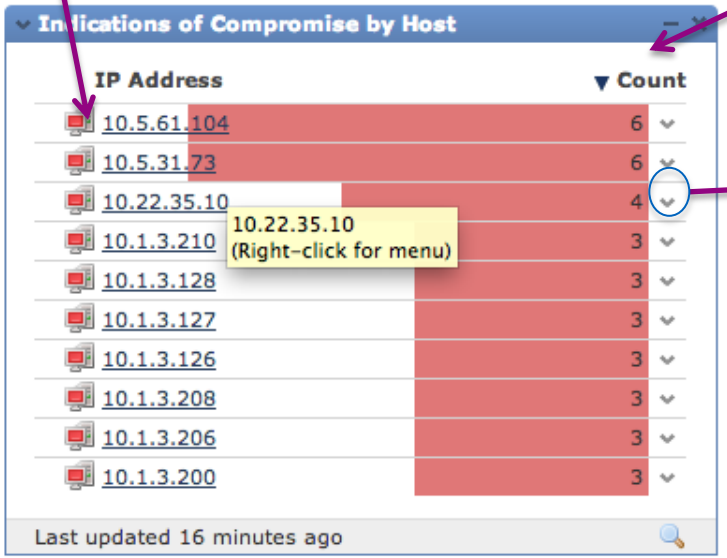
Link to original event(s)

IOC Dashboard Widget

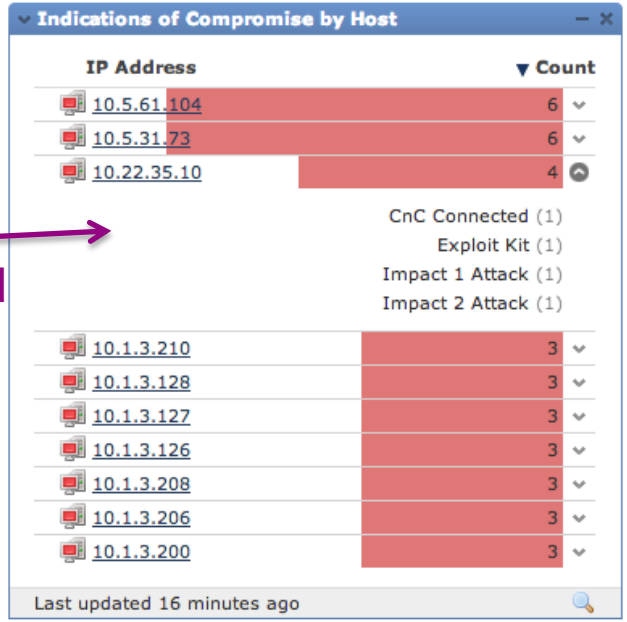
- Because IOCs enable a quick way of classifying a host's potentially comprom ised state, having this data on a dashboard is desirable

Number of IOCs set against the host

Host



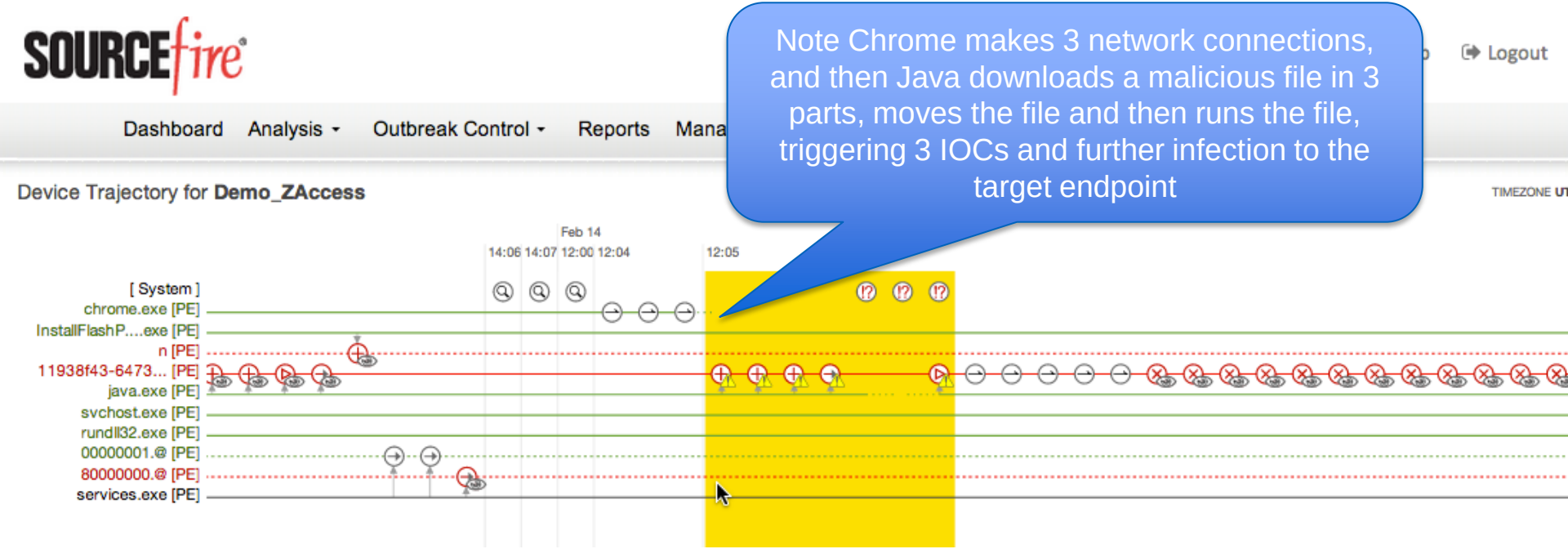
Click to expand



IOC DEMO

CISCO™

Supplemental Slides
ZeroAccess Investigation



Note Chrome makes 3 network connections, and then Java downloads a malicious file in 3 parts, moves the file and then runs the file, triggering 3 IOCs and further infection to the target endpoint

FireAMP correlates Java being compromised, creating a malicious file and then executing it

SOURCEfire

Support ? Help Logout

Dashboard Analysis Outbreak Control

Device Trajectory for **Demo_ZAccess**

TIMEZONE **UTC**

Feb 14

14:06 14:07 12:00 12:04 12:05

[System]
chrome.exe [PE]
InstallFlashP....exe [PE]
n [PE]
11938f43-6473... [PE]
java.exe [PE]
svchost.exe [PE]
rundll32.exe [PE]
00000001.@ [PE]
80000000.@ [PE]
services.exe [PE]

Possible compromise. Java VM created and executed a malicious or neutral disposition executable file.

11938f43-647341ab, (87715c2..041f20) was created and executed by **java.exe**, Java(TM) Platform SE 7 U10 7.0.100.18 (0b4eefc..1ccbd9) at 12:05:09, Fri Feb 14 2014 UTC.

At 15:20:11, Fri Feb 14 2014 UTC

SOURCEfire

? Help Logout

Dashboard Analysis Outbreak Control Reports

Here is the connection Chrome made to a malicious web site, hosting a web page with an embedded java exploit that compromised the version of Java installed on this endpoint

Device Trajectory for **Demo_ZAccess**

TIMEZONE

Feb 14

14:06 14:07 12:00 12:04 12:05

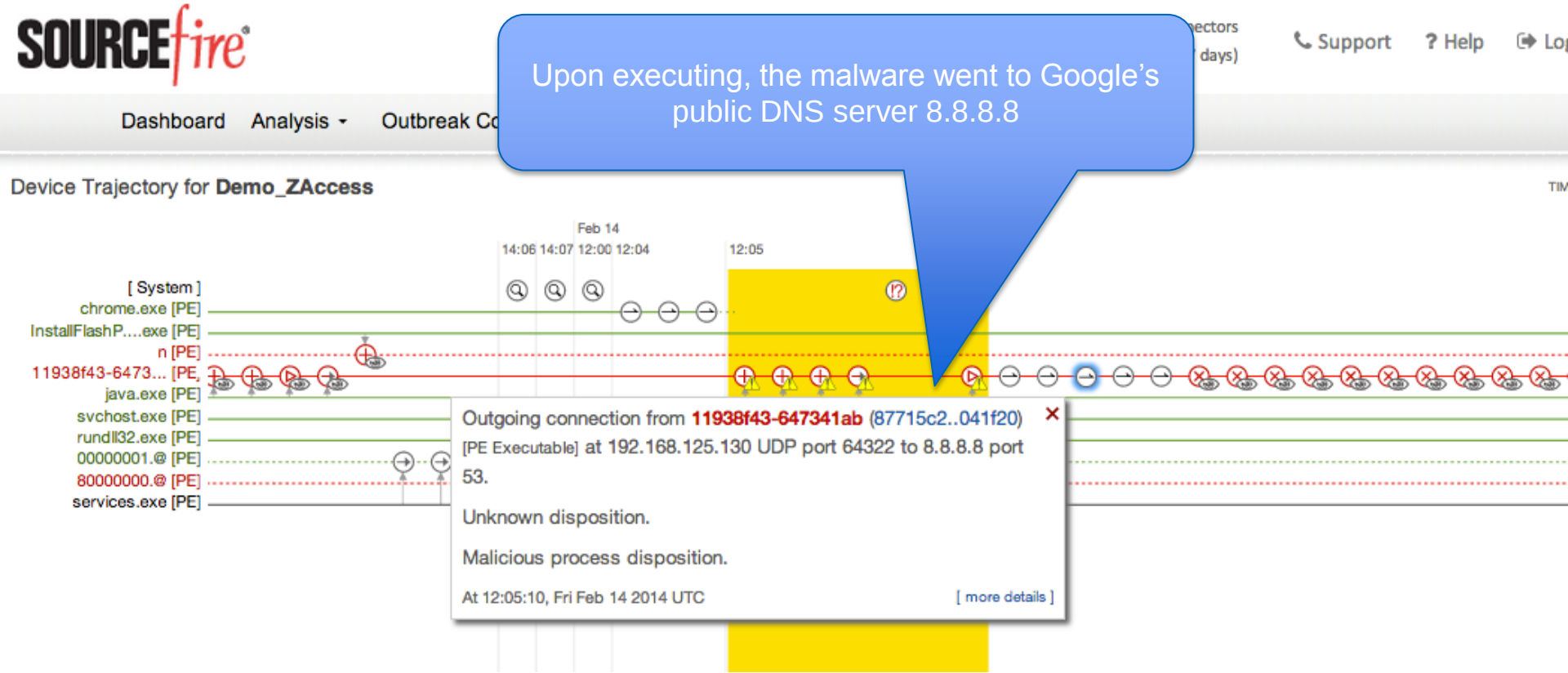
[System]
chrome.exe [PE]
InstallFlashP....exe [PE]
n [PE]
11938f43-6473... [PE,
java.exe [PE]
svchost.exe [PE]
rundll32.exe [PE]
00000001.@ [PE]
80000000.@ [PE]
services.exe [PE]

Outgoing connection from **chrome.exe** [common filename], Google Chrome 24.0.1312.52 (62ca2bc..59a3cb) [PE Executable] at 192.168.125.130 TCP port 49413 to http://**pwnme.com**:8888/exploit.html (10.180.0.144 port 8888).

Unknown disposition.

Unknown process disposition.

At 12:04:58, Fri Feb 14 2014 UTC [more details]


SOURCEfire
Support
? Help
Dashboard
Analysis
Outbreak Co
Upon executing, the malware went to Google's public DNS server 8.8.8.8
Device Trajectory for Demo_ZAccess
Feb 14
14:06 14:07 12:00 12:04
12:05
[System]
chrome.exe [PE]
InstallFlashP....exe [PE]
n [PE]
11938f43-6473... [PE,
java.exe [PE]
svchost.exe [PE]
rundll32.exe [PE]
00000001.@ [PE]
80000000.@ [PE]
services.exe [PE]
Outgoing connection from 11938f43-647341ab (87715c2..041f20) [PE Executable] at 192.168.125.130 UDP port 64322 to 8.8.8.8 port 53.
Unknown disposition.
Malicious process disposition.
At 12:05:10, Fri Feb 14 2014 UTC
[more details]

It also connected to a publically available geolocation script to discover the geo of the infected endpoint as part of its enrollment to the CnC

SOURCEfire

Dashboard Analysis Outl

onnectors
s (7 days)

Support ? Help Logout

Device Trajectory for **Demo_ZAccess**

TIMEZONE UTC

Feb 14

14:06 14:07 12:00 12:04 12:05

[System]
chrome.exe [PE]
InstallFlashP....exe [PE]
n [PE]
11938f43-6473... [PE]
java.exe [PE]
svchost.exe [PE]
rundll32.exe [PE]
00000001.@ [PE]
80000000.@ [PE]
services.exe [PE]

Outgoing connection from **11938f43-647341ab** (87715c2..041f20) [PE Executable] at 192.168.125.130 TCP port 49422 to http://j.**maxmind.com**/app/geoip.js (50.22.196.70 port 80).

Unknown disposition.

Malicious process disposition.

At 12:05:10, Fri Feb 14 2014 UTC [more details]

Once it enrolls and downloads more components, the malware pulls down a version of Flash which it will exploit to root the endpoint further

SOURCEfire

Support ? Help

Dashboard Analysis Outbreak Control

Device Trajectory for **Demo_ZAccess**

[System]
InstallFlashP....exe [PE]
n [PE]
11938f43-6473... [PE]
java.exe [PE]
svchost.exe [PE]
rundll32.exe [PE]
00000001.@ [PE]
80000000.@ [PE]
services.exe [PE]

Outgoing connection from **InstallFlashPlayer.exe**, Flash® Player Installer/Uninstaller 11.0.1.152 (672ec8d..b24429) [PE Executable] at 192.168.125.130 TCP port 49460 to http://**fpdownload.macromedia.com**/get/flashplayer/update/current/install/install_all_win_cab_ax_sgn.z (23.55.242.70 port 80).

Unknown disposition.

Unknown process disposition.

At 12:05:15, Fri Feb 14 2014 UTC [more details]

Once rooted by Flash, rundl32 makes more network connections, and a new malicious payload is downloaded.

SOURCEfire

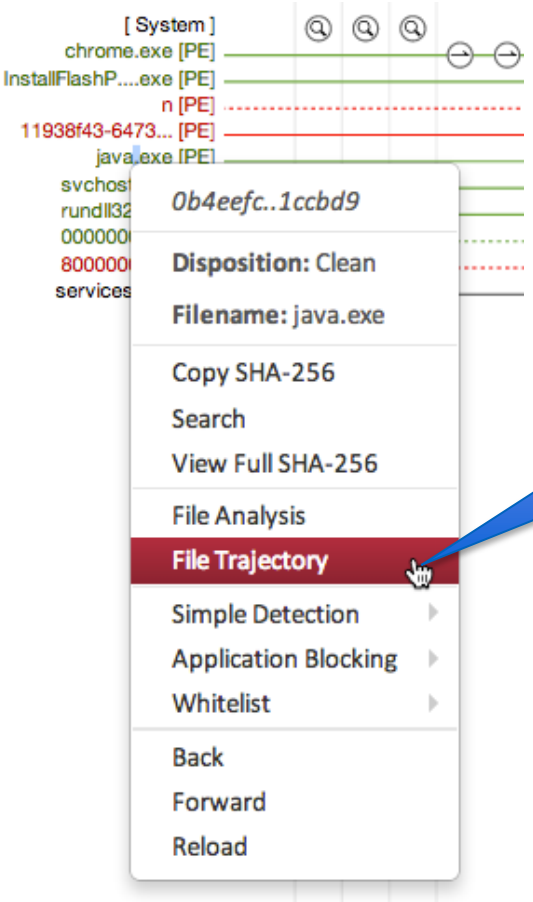
Dashboard Analysis Outbreak Control Reports Management Accounts

Device Trajectory for **Demo_ZAccess**

TIMEZONE UT

12:06

[System]
InstallFlashP....exe [PE]
n [PE]
11938f43-6473... [PE]
java.exe [PE]
svchost.exe [PE]
rundll32.exe [PE]
00000001.@ [PE]
80000000.@ [PE]
services.exe [PE]



Right-clicking on Java and selecting File Trajectory allows the analyst to check where this vulnerable version of Java, which is currently being compromised is also installed.

Beta

8.8.8.8

Search

By searching for connections to Google's public DNS, an analyst can determine endpoints and files making this suspicious traffic to discover new infected enpoints

Matching File Analyses

668255f..93e0d3 text.exe also known as 1A.tmp, E0E6.tmp, 1B.tmp. detected as FakeAlert:MalOb-tpd, W32.DFC.MalParent, FakeAlert:Trojan-tpd, W32.ET.fakealert.

081919d..effff6

081af69..5aeb5a

081c55e..761806

081dab5..d47d70

(79078 matches found) 5 / page

1 of 15816

Devices with Matching Activity

InfectMe93 observed 1 matches. It is a Windows XP, SP 3.0 device in the JB Agents group with the JB Policy policy.

Demo_ZAccess observed 26 matches. It is a device in the Default Group group with the Default Policy policy.

WXPSP3_IM_92 observed 3 matches. It is a Windows XP, SP 3.0 device in the JB Agents group with the JB Policy policy.

Demo_TDSS observed 52 matches. It is a device in the Default Group group with the Default Policy policy.

WXPSP3_IM_94 observed 1 matches. It is a Windows XP, SP 3.0 device in the JB Agents group with the JB Policy policy.

(7 matches found) 5 / page

1 of 2

Searching for connections to j.maxmind.com, an analyst can also determine endpoints making this suspicious traffic to discover new infected enpoints

Beta

http://j.maxmind.com/app/geoip.js

Search

Devices with Matching Activity

Demo_ZAccess observed 26 matches. It is a device in the Default Group group with the Default Policy policy.

Pete-PC observed 8 matches. It is a Windows 7, SP 1.0 device in the JV-Group group with the Default Policy policy.