TOMORROW starts here.

Design and Deployment of SourceFire NGIPS and NGFWL

BRKSEC - 2024

Marcel Skjald
Consulting Systems Engineer
Enterprise / Security Architect

Abstract

Overview of Session

- This technical session covers the FirePOWER security appliance product line and how it uniquely uses context to deliver true next generation network security capabilities including NGIPS, NGFW, and AMP (Next Generation IPS, Next Generation Firewall, and Advanced Malware Protection).

- The session will begin with a detailed review of the FirePOWER architecture including hardware acceleration, packet, flow and stream processing, and then move on to introduce why network context from FireSIGHT is a vital component in delivering these next generation services.

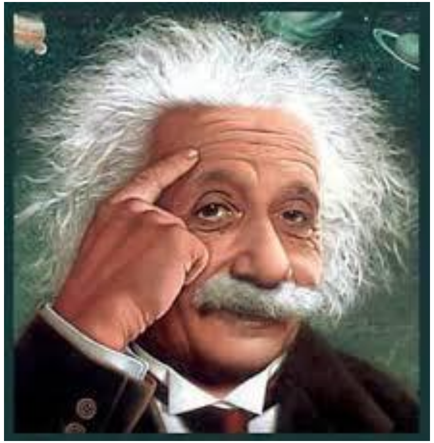
- Followed by a detailed review of Advanced Malware Protection, and how it uses context in detailing Malware behaviour.

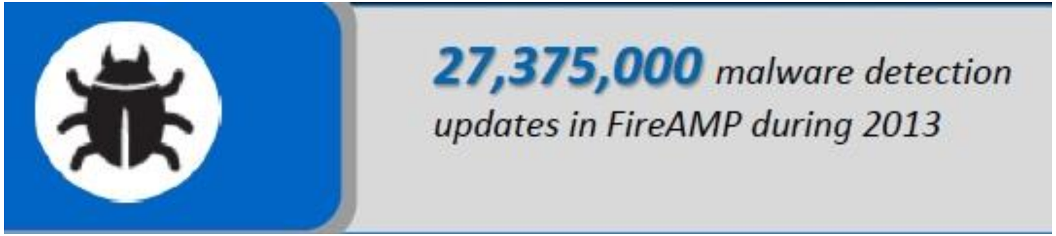
- Deployment Scenarios.

Agenda

- **Why do we need NGIPS or Advanced Malware Protection?**
- **What is FirePOWER**? Performance and functional characteristics
- Packet and flow processing (day in the life of a stream)
- Wh**at is FireSIGHT**?
- Awareness and the Network Map
- Why this context is vital in modern networks
- **FirePOWER: Security deployment modes**
- NGIPS
- NGFW
- Advanced Malware Protection (AMP)
- Deployment Scenarios / Considerations

Why do we Need NGIPS & Advanced Malware Detection?





27,375,000 malware detection updates in FireAMP during 2013

- Hackers
- State Based Actors
- Criminals
- Insider Threats
- Compliance
- Due Diligence
- Knowledge!

Where did it all Start?

Marty Roesch

Threat Focused Approach to Network Security

Access Control

- Remote Access VPN
- Gateway VPN Switching
- Routing
- NAT
- Stateful Inspection

App Control

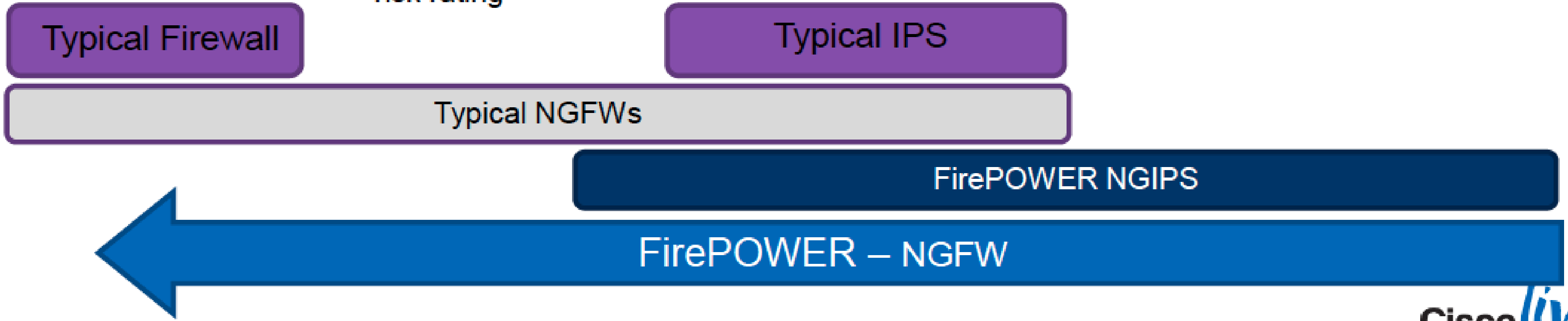
- Detection of applications
- Allow/block apps and app sub-functions
- Allow/block apps by user
- Allow/block apps by type, tag, category, risk rating

Threat Prevention

- Vulnerability facing rules
- Threat facing rules
- Enterprise accuracy and performance

Context Awareness

- Correlate host and user activity
- Passive OS Fingerprinting
- Passive Service Identification
- Passive Vulnerability mapping
- Passive Network Discovery
- Auto Policy Recommendations
- Auto Impact Assessment

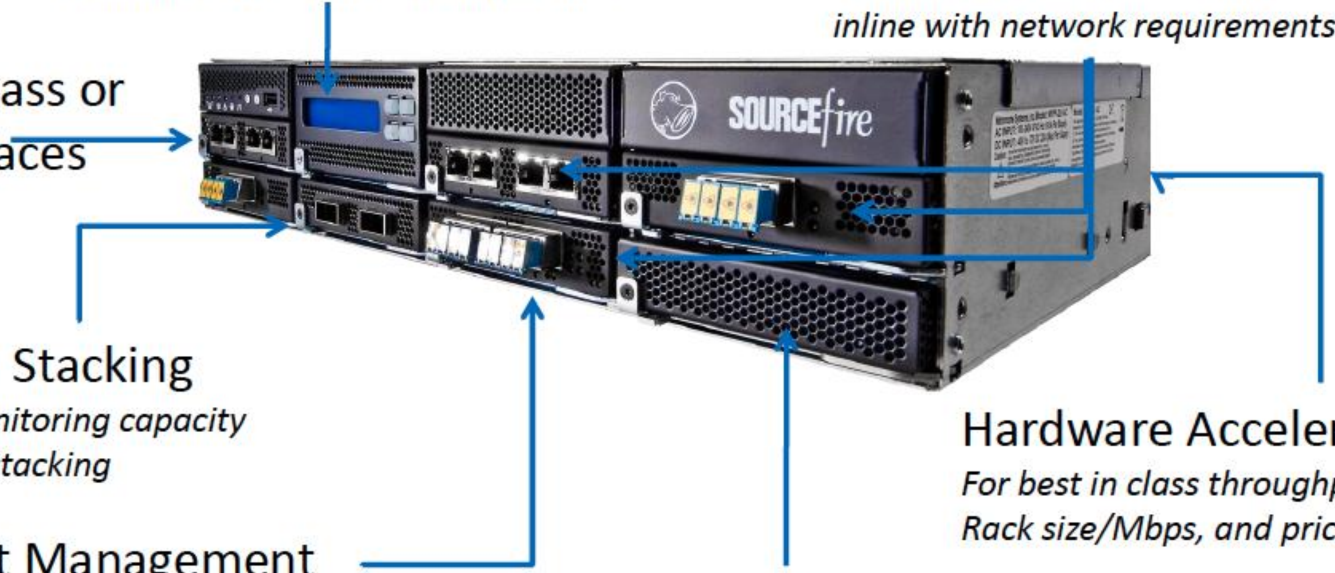


FirePOWER Platform - Overview

What is FirePOWER?

- Industry-leading security platform
- Unmatched performance from a single-pass, low-latency design
- Configuration flexibility
- Standard platform for delivering the Sourcefire network capability
- NGIPS, NGFW & AMP

FirePOWER Platform



LCD Display

Quick and easy headless configuration

Connectivity Choice

Change and add connectivity inline with network requirements

Configurable Bypass or Fail Closed Interfaces

For IDS, IPS or Firewall deployments

Device Stacking

Scale monitoring capacity through stacking

Hardware Acceleration

For best in class throughput, security, Rack size/Mbps, and price/Mbps

Lights Out Management

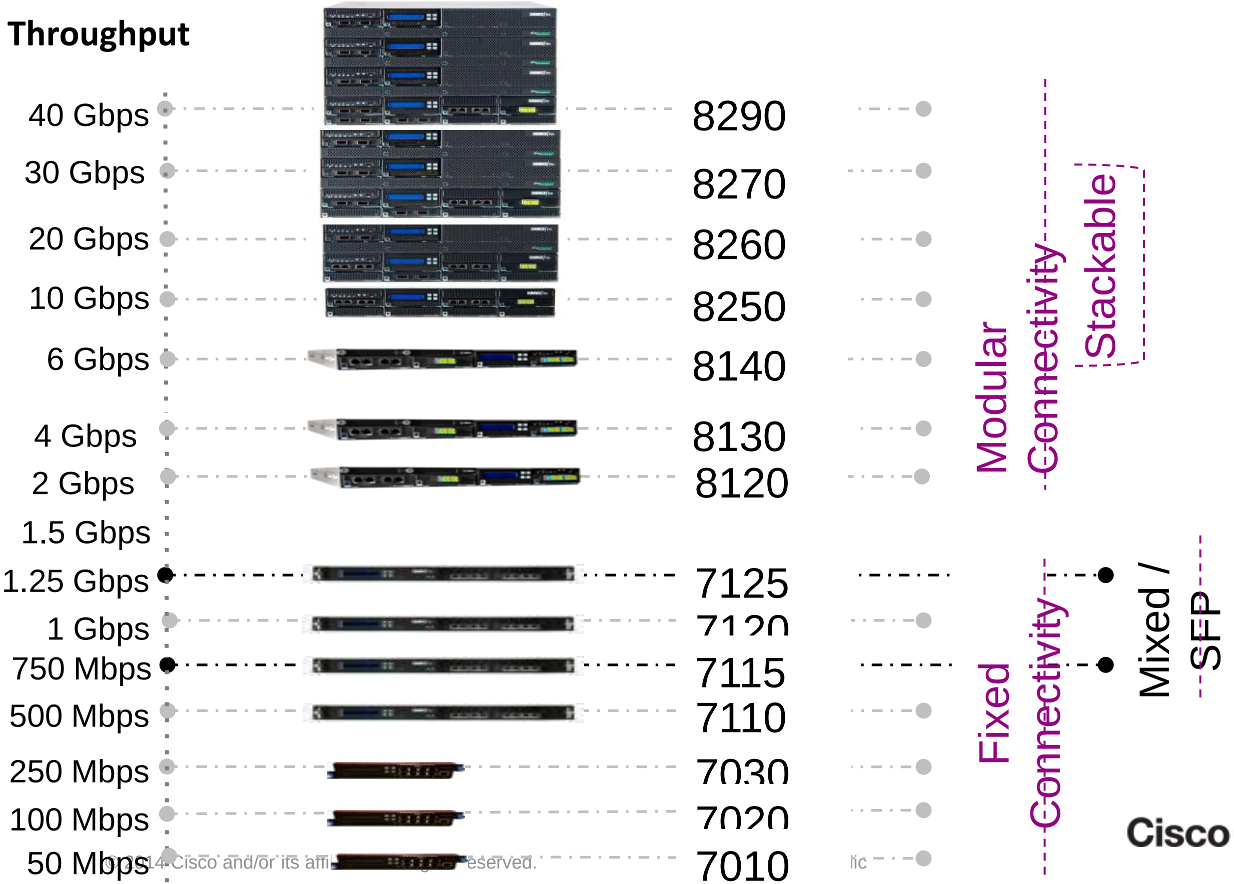
Minimal operational impact

SSD

FirePOWER Platform

All appliances include:

- Integrated lights-out management
- Sourcefire acceleration technology
- LCD display



IPS Throughput

40 Gbps	8290
30 Gbps	8270
20 Gbps	8260
10 Gbps	8250
6 Gbps	8140
4 Gbps	8130
2 Gbps	8120
1.5 Gbps	
1.25 Gbps	7125
1 Gbps	7120
750 Mbps	7115
500 Mbps	7110
250 Mbps	7030
100 Mbps	7020
50 Mbps	7010

Modular Connectivity

Stackable

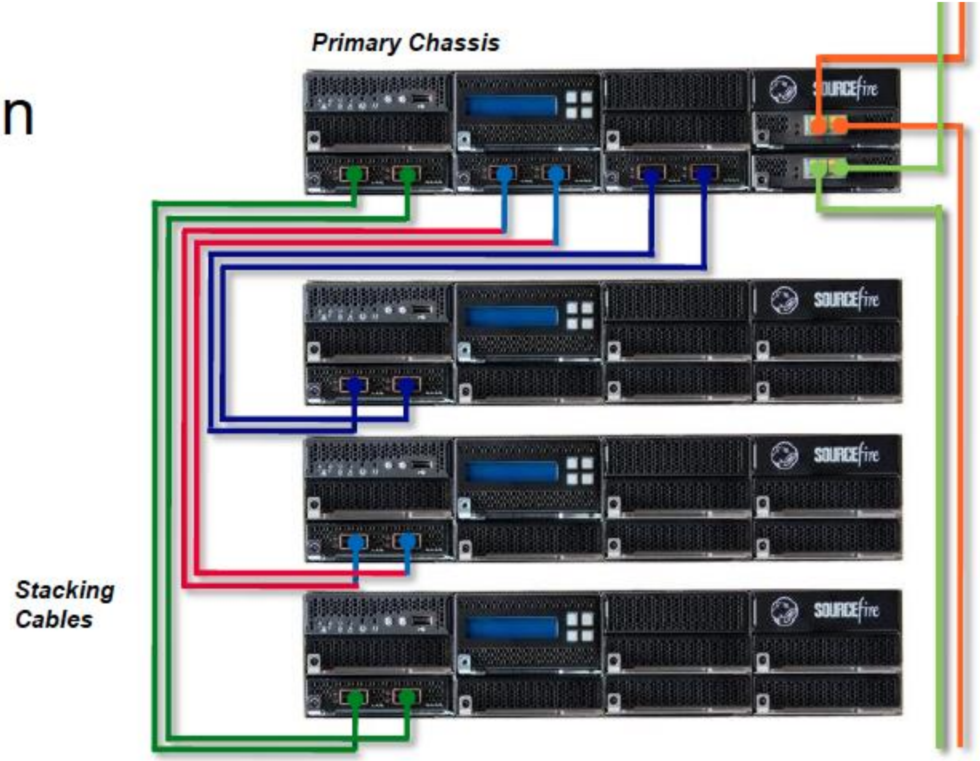
Fixed Connectivity

Mixed / SFP

FirePOWER Scalability

- Up to four 8250 chassis can be stacked

Number of chassis	IPS Throughput
1	10Gbps
2	20Gbps
3	30Gbps
4	40Gbps

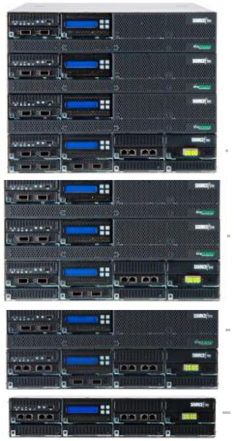


New FirePower Appliances – 8300 Series

Current 8200 Offerings

IPS Throughput	
40 Gbps	8290
30 Gbps	8270
20 Gbps	8260
10 Gbps	8250

New 8300 Offerings



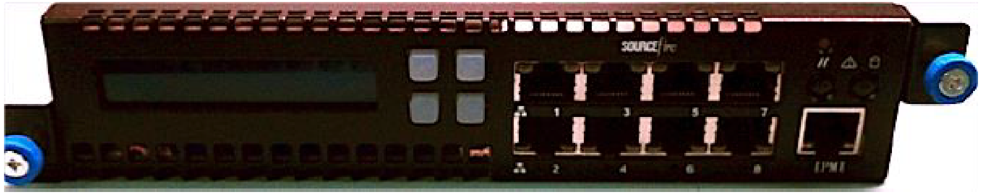
IPS Throughput	
60 Gbps	8390
45 Gbps	8370
30 Gbps	8360
15 Gbps	8350

8300 Series – Performance Specifications

	Rack Height	NGIPS Throughput	Maximum Monitoring Interfaces (1Gbs)	x86 Cores/ threads and # Microengines	Netmod Bays	Stacking
8350	2U	**15Gbps**	28	20/40 and 80	7	Yes, with additional 8350 appliances.
8360	4U	**30Gbps**	24	40/80 and 160	6	Yes, with additional 8350 appliances.
8370	6U	**45Gbps**	20	60/120 and 240	5	Yes, with additional 8350 appliances.
8390	8U	**60Gbps**	16	80/160 and 320	4	Yes, with additional 8350 appliances.

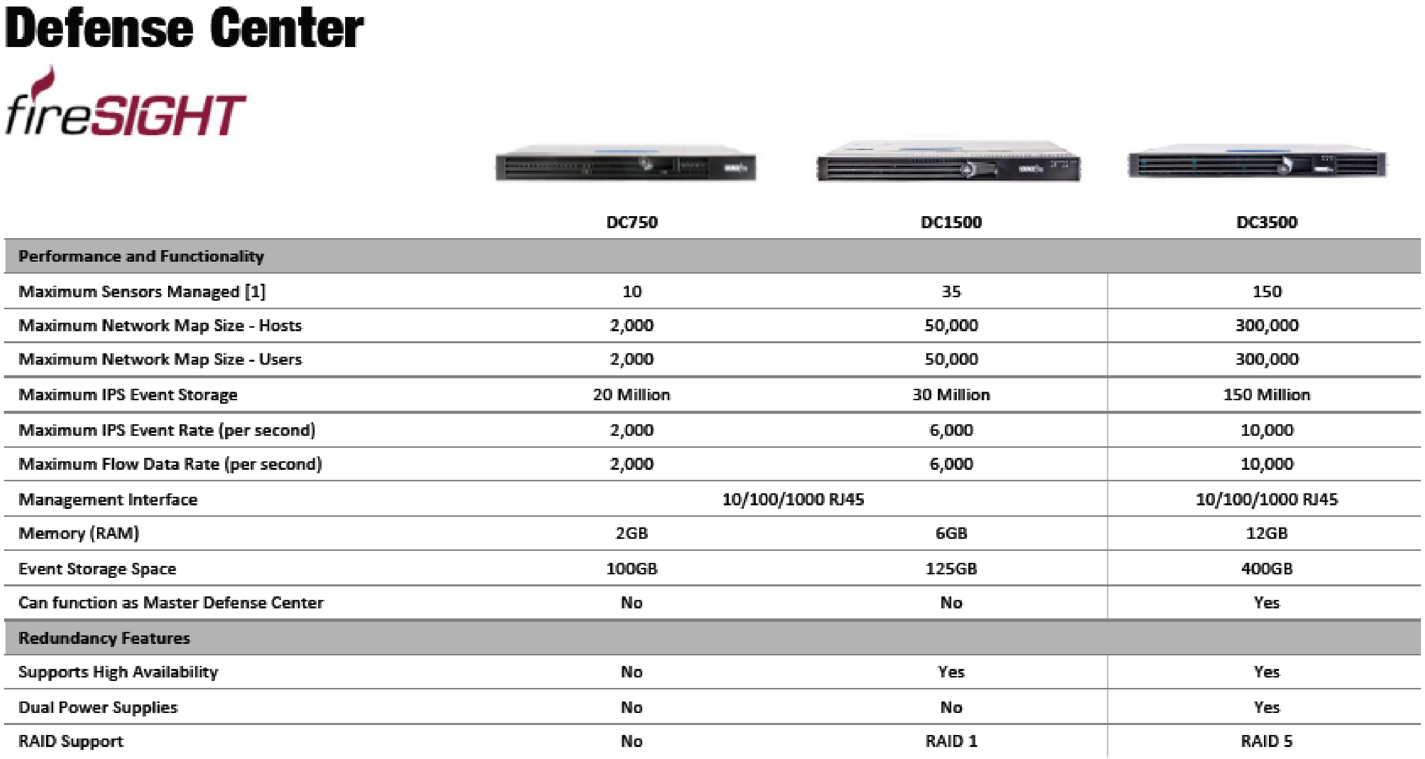
FirePOWER - 7010,7020,7030

- Half Width Chassis – Fixed 8 Port Copper
  - Low Latency
  - LCD Screen
  - Integrated LOM
  - Solid State Drive



Model	Acceleration	RAM	IPS Throughput	Modes
3D7030	firePOWER	4GB	250 Mbps	NGIPS, NGFW, AMP
3D7020	firePOWER	4GB	100 Mbps	NGIPS, NGFW, AMP
3D7010	firePOWER	4GB	50 Mbps	NGIPS, NGFW, AMP

FirePOWER – Defence Centres (Mgmt Console)

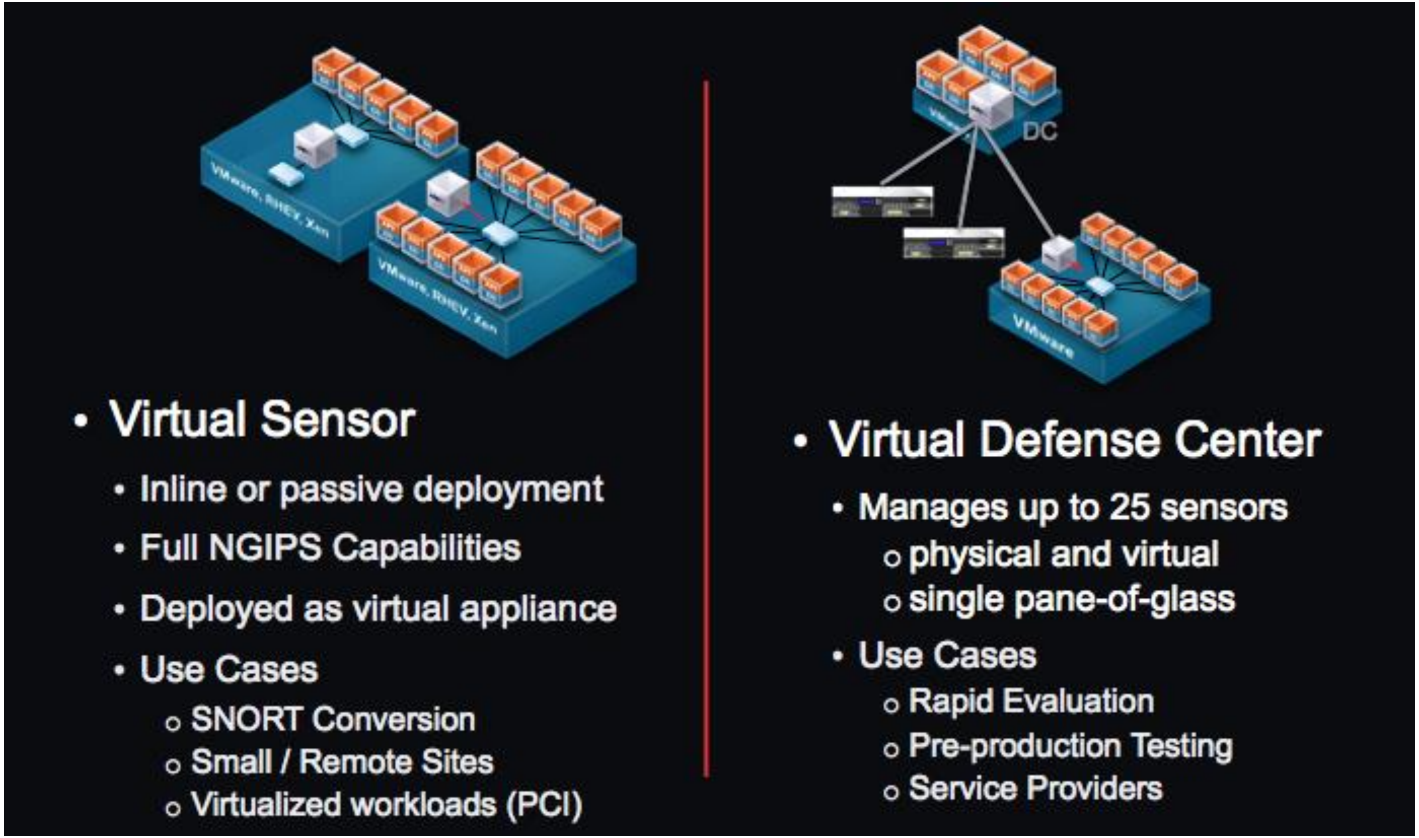


Defense Center

fireSIGHT

	DC750	DC1500	DC3500
Performance and Functionality			
Maximum Sensors Managed [1]	10	35	150
Maximum Network Map Size - Hosts	2,000	50,000	300,000
Maximum Network Map Size - Users	2,000	50,000	300,000
Maximum IPS Event Storage	20 Million	30 Million	150 Million
Maximum IPS Event Rate (per second)	2,000	6,000	10,000
Maximum Flow Data Rate (per second)	2,000	6,000	10,000
Management Interface	10/100/1000 RJ45		10/100/1000 RJ45
Memory (RAM)	2GB	6GB	12GB
Event Storage Space	100GB	125GB	400GB
Can function as Master Defense Center	No	No	Yes
Redundancy Features			
Supports High Availability	No	Yes	Yes
Dual Power Supplies	No	No	Yes
RAID Support	No	RAID 1	RAID 5

FirePOWER – Virtual

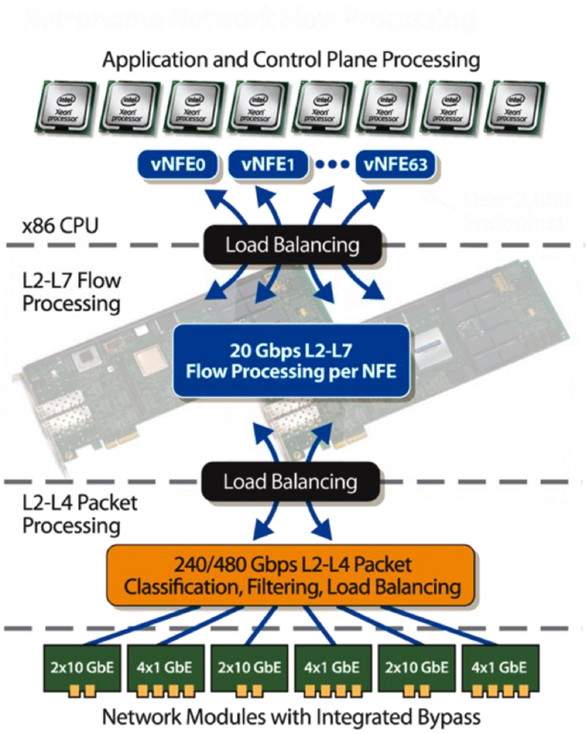


- Virtual Sensor
  - Inline or passive deployment
  - Full NGIPS Capabilities
  - Deployed as virtual appliance
  - Use Cases
    - SNORT Conversion
    - Small / Remote Sites
    - Virtualized workloads (PCI)

- Virtual Defense Center
  - Manages up to 25 sensors
    - physical and virtual
    - single pane-of-glass
  - Use Cases
    - Rapid Evaluation
    - Pre-production Testing
    - Service Providers

FirePOWER Architecture

The Power of Hardware & Software Combined

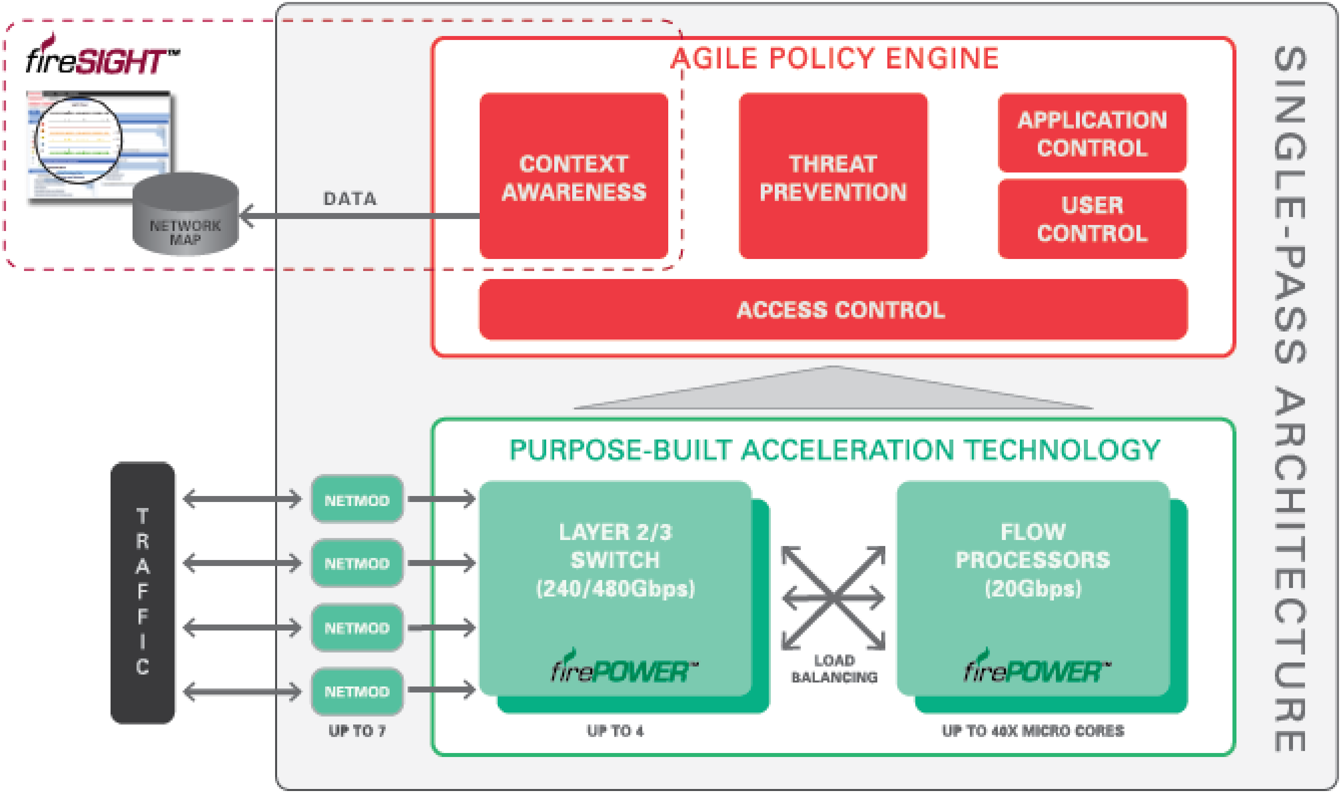

Netronome Network Flow Processing
Application and Control Plane Processing
vNFE0
vNFE1
vNFE63
Over 2,000 Endpoints
x86 CPU
Load Balancing
L2-L7 Flow Processing
20 Gbps L2-L7 Flow Processing per NFE
Load Balancing
L2-L4 Packet Processing
240/480 Gbps L2-L4 Packet Classification, Filtering, Load Balancing
2x10 GbE
4x1 GbE
2x10 GbE
4x1 GbE
2x10 GbE
4x1 GbE
Network Modules with Integrated Bypass

Enables industry leading, energy efficient performance for Sourcefire NGIPS | NGFW

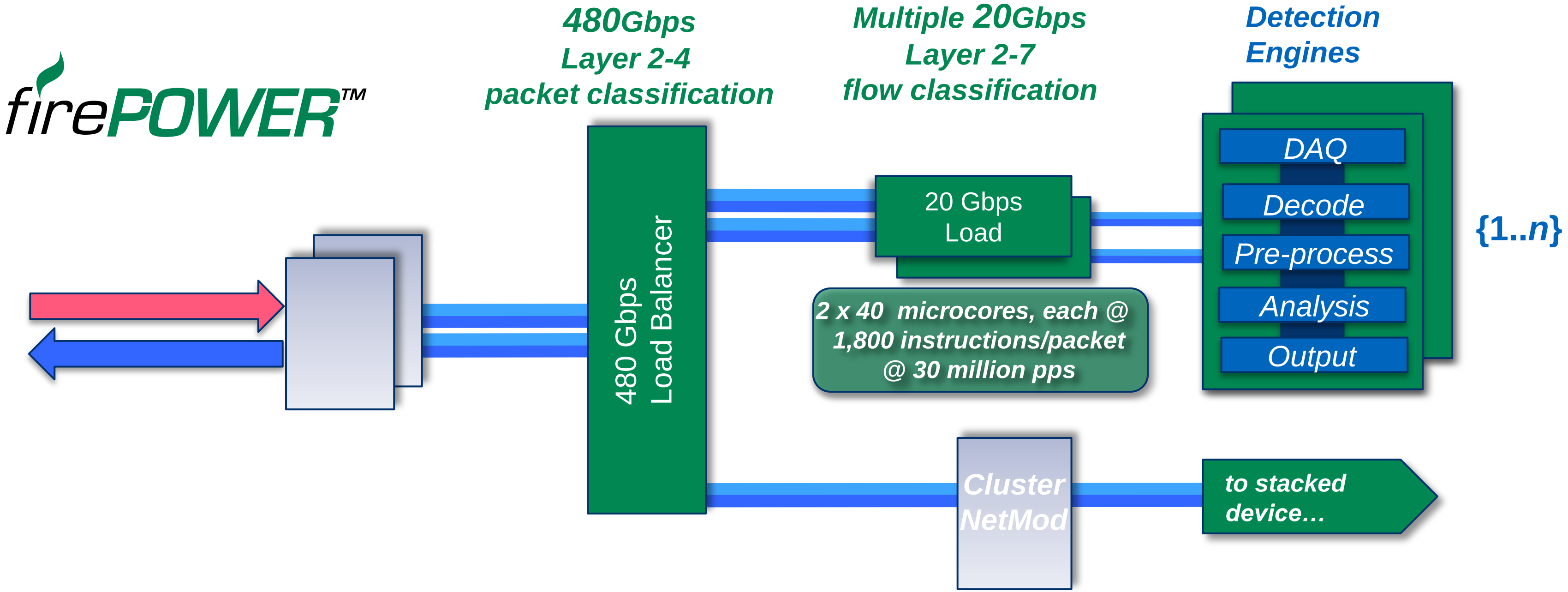
firePOWER™ *Technology*

Custom designed, specialised network processor accelerates data acquisition and classification.

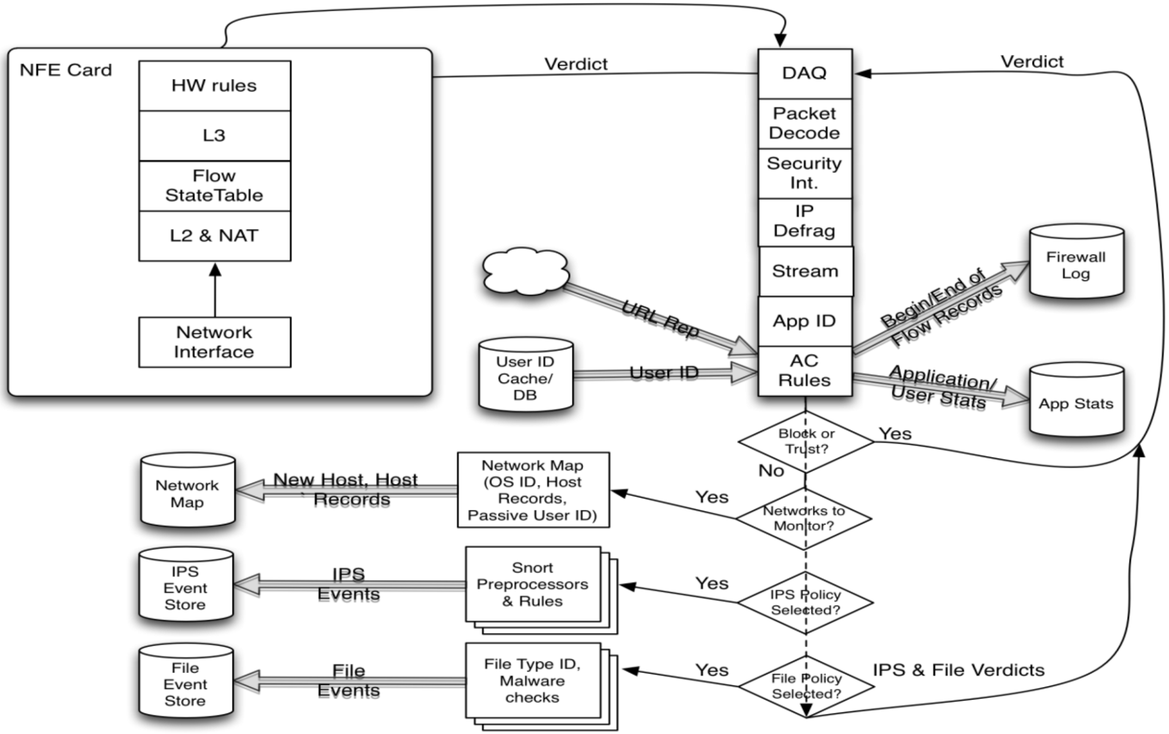
Single Pass Architecture



Single Pass Architecture

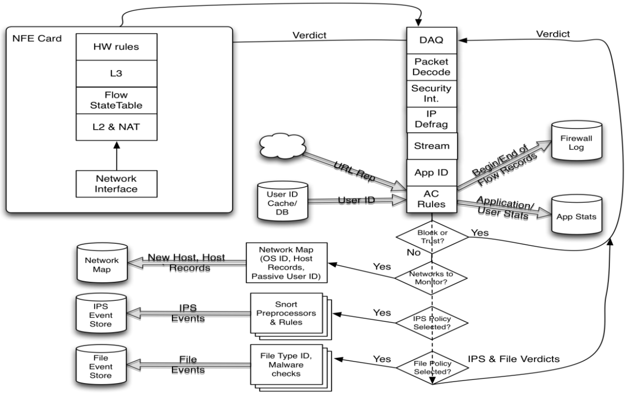


FirePOWER Architecture – V5.X



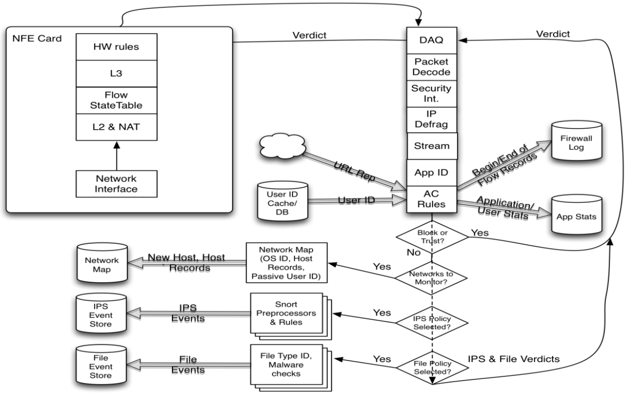
Life of a Flow

- Hardware processing
- Initial processing
  - IP Blacklist (Security Intelligence)
  - Flows that are blocked/trusted via AC rules
- Network Layer Processing
  - IP Defrag Frag, Stream, Rate Based Attack
- Application Identification
- AC Rule Evaluation
- Network Discovery
- IPS & File Processing



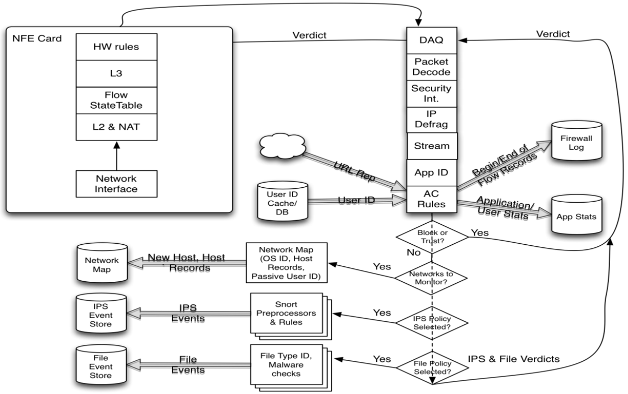
Life of a Flow

- Hardware Processing
  - Look for flow in flow state table
  - Create if not there
  - If flow has disposition of Block or Trust, take immediate action
- Evaluate hardware rules
- If block or trust, mark entry in flow state table
  - Take action on rule
- If inspect
  - Store information about AC rule and Start Inspection



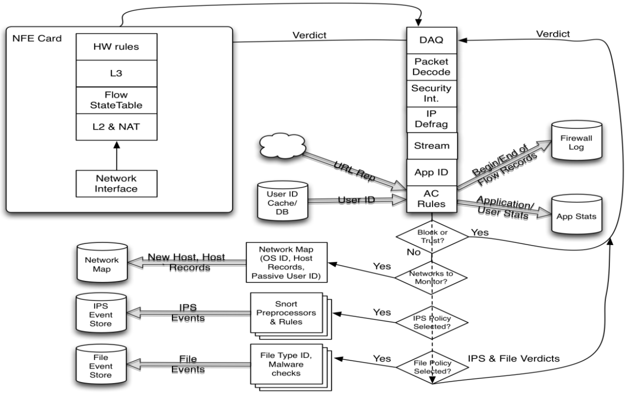
Life of a Flow

- Initial processing
  - Packet decoding
  - IP Blacklist (Security Intelligence)
  - immediately mark flow as blocked, update hardware flow state
  - monitor - mark flow, log later
- Network Layer Processing
  - IP Defragmentation/Connection Tracking/TCP Stream reassembly
  - Connection tracking by IPs, Ports, VLAN, IP Protocol, MPLS Label, In/Out zones unique ID
- Application Identification
  - When needed for AC rules



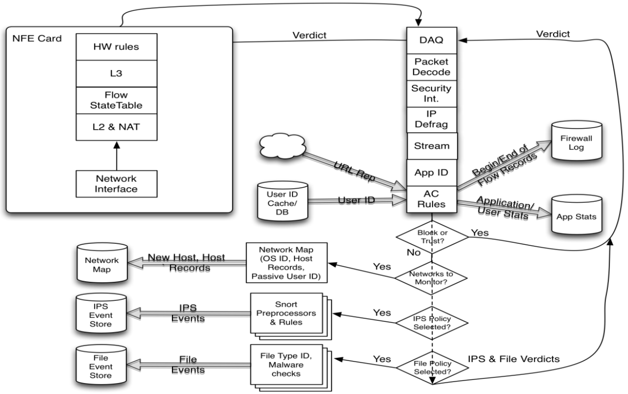
Life of a Flow

- AC Rule evaluation
  - Can match Zones, VLAN, IPs, Ports & User/Group based on packet header
- Need App ID for matching Applications and URLs
  - Packets continue to flow until Application is identified and the rule criteria can be matched or considered a non-match
  - If Application not yet determined, IPS policy from Default is used ("No Rules Active" if that is Block or Trust)
  - If action of block/trust
  - Immediately mark flow, update hardware flow state
- If action of allow
  - Select IPS policy?
  - Select File policy?



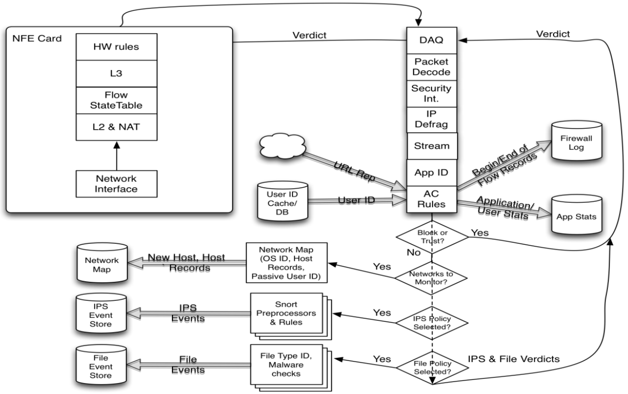
Life of a Flow

- Network Discovery
  - Only if within Networks Discovery Policy
  - Hosts, users, applications
- App ID
  - Leverage information from earlier if done for AC rule
- Network Map Events



Life of a Flow

- IPS
- IPS Event logging for Decode/Frag/Stream events
  - May block flow at this point
- Application Preprocessors
  - HTTP Inspect, FTP/Telnet, SMTP, POP, IMAP, DCE/RPC, DNS, DNP3, Modbus, GTP, SSH, SSL
  - IPS Rules
  - Leverage Application Protocol ID to select rules
- IPS Events
  - if block, mark flow as blocked, update hardware flow state



Life of a Flow

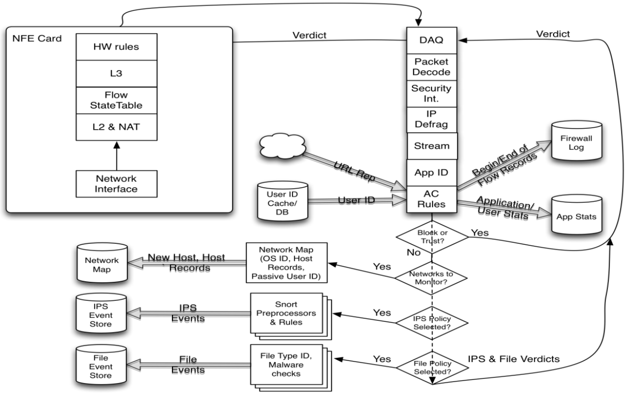
- File Processing

- Leverage HTTP, SMTP, POP, IMAP, FTP preprocessors

- File type ID
  - Usually within first part of the file

- Malware signature calculation & lookup
  - Requires entire file

- Blocking & Logging of File events



FireSight - Context

Got a lot of Data? – Well what was the question?

Why is Context Important?

Event + network & user context

Event:	Attempted Privilege Gain
Target:	96.16.242.135 (vulnerable)
Host OS:	Blackberry
Apps:	Mail, Browswer, Twitter
Location:	Whitehouse, US
User ID:	bobama
Full Name:	Barack Obama
Department:	Executive Office

Event + network context

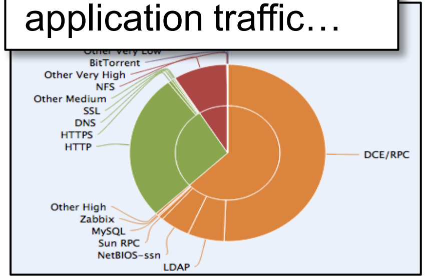
Event:	Attempted Privilege Gain
Target:	96.16.242.135 (vulnerable)
Host OS:	Blackberry
Apps:	Mail, Browser, Twitter
Location:	Whitehouse, US

Event

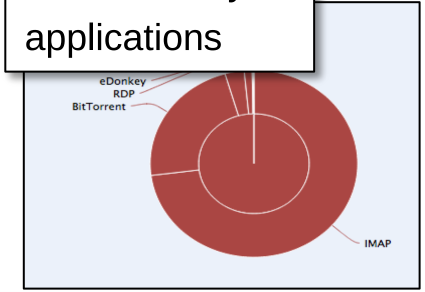
Event:	Attempted Privilege Gain
Target:	96.16.242.135

Dashboard - Context

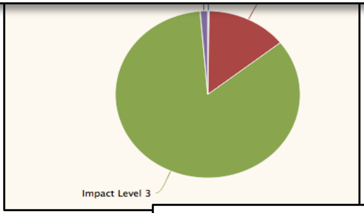
Browse all application traffic…



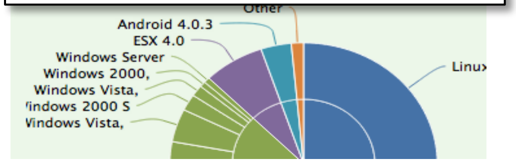
Look for risky applications



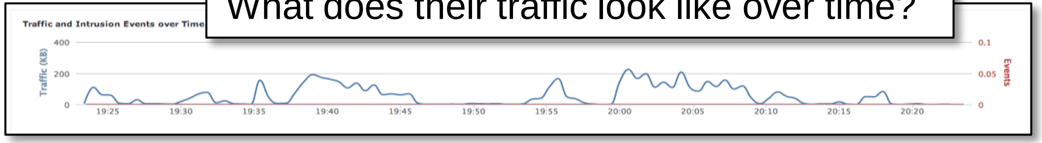
What else have these users been up to?



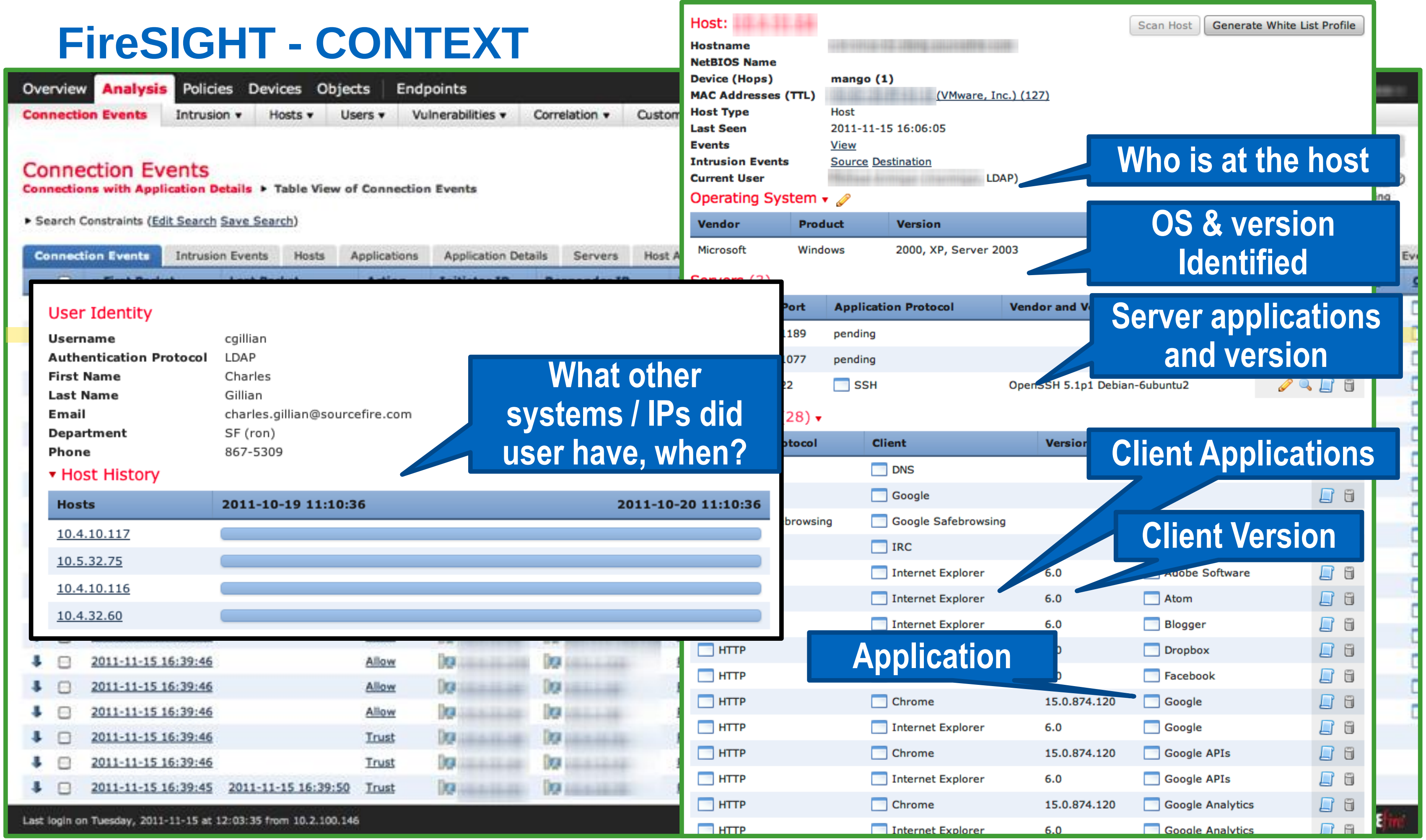
On what operating systems?



What does their traffic look like over time?



FireSIGHT - CONTEXT



Connection Events

Connections with Application Details ▸ Table View of Connection Events

▸ Search Constraints (Edit Search Save Search)

		First Packet	Last Packet	Action	Initiator IP	Responder IP
⬇	□	2011-11-15 16:39:46		Allow	[redacted]	[redacted]
⬇	□	2011-11-15 16:39:46		Allow	[redacted]	[redacted]
⬇	□	2011-11-15 16:39:46		Allow	[redacted]	[redacted]
⬇	□	2011-11-15 16:39:46		Trust	[redacted]	[redacted]
⬇	□	2011-11-15 16:39:46		Trust	[redacted]	[redacted]
⬇	□	2011-11-15 16:39:45	2011-11-15 16:39:50	Trust	[redacted]	[redacted]

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

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?

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	Version
Microsoft	Windows	2000, XP, Server 2003

OS & version Identified

Servers (3)

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

Server applications and version

(28) ▾

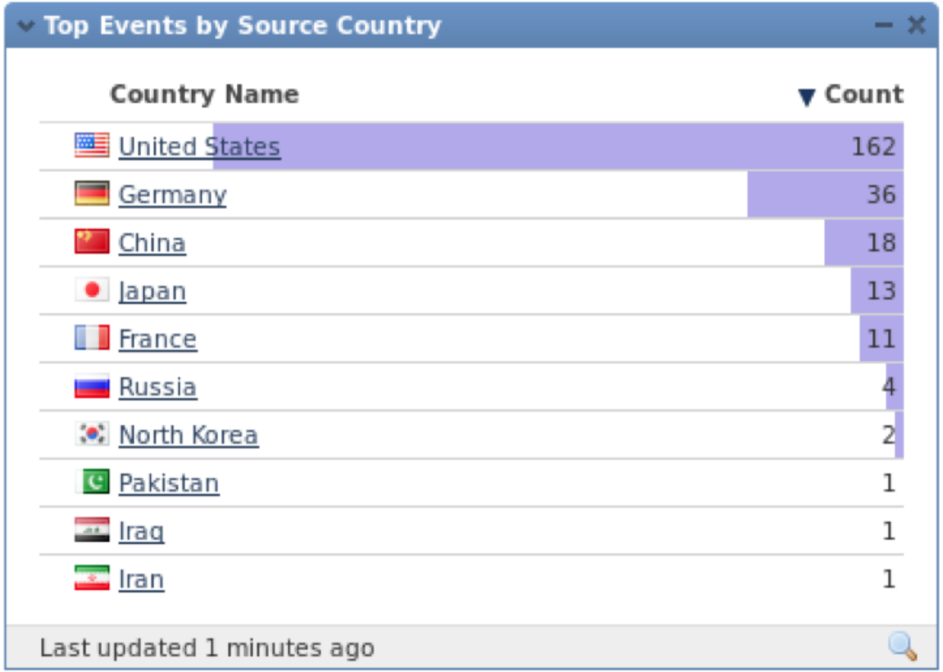
tocol	Client	Version	
	DNS		
	Google		
browsing	Google Safebrowsing		
	IRC		
	Internet Explorer	6.0	Adobe Software
	Internet Explorer	6.0	Atom
	Internet Explorer	6.0	Blogger
HTTP		0	Dropbox
HTTP		0	Facebook
HTTP	Chrome	15.0.874.120	Google
HTTP	Internet Explorer	6.0	Google
HTTP	Chrome	15.0.874.120	Google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

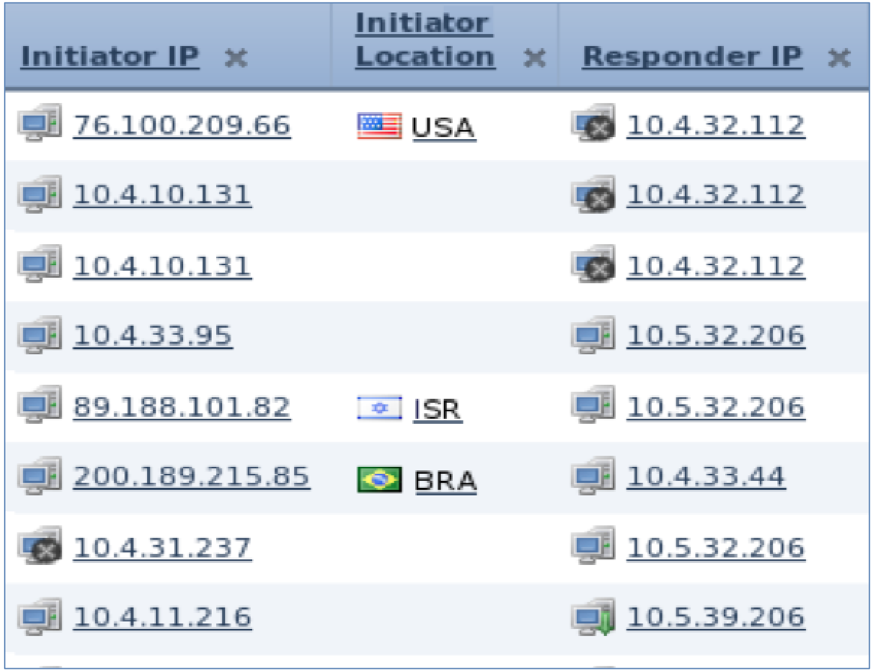
Context - Geolocation



Top Events by Source Country

Country Name	▼ Count
United States	162
Germany	36
China	18
Japan	13
France	11
Russia	4
North Korea	2
Pakistan	1
Iraq	1
Iran	1

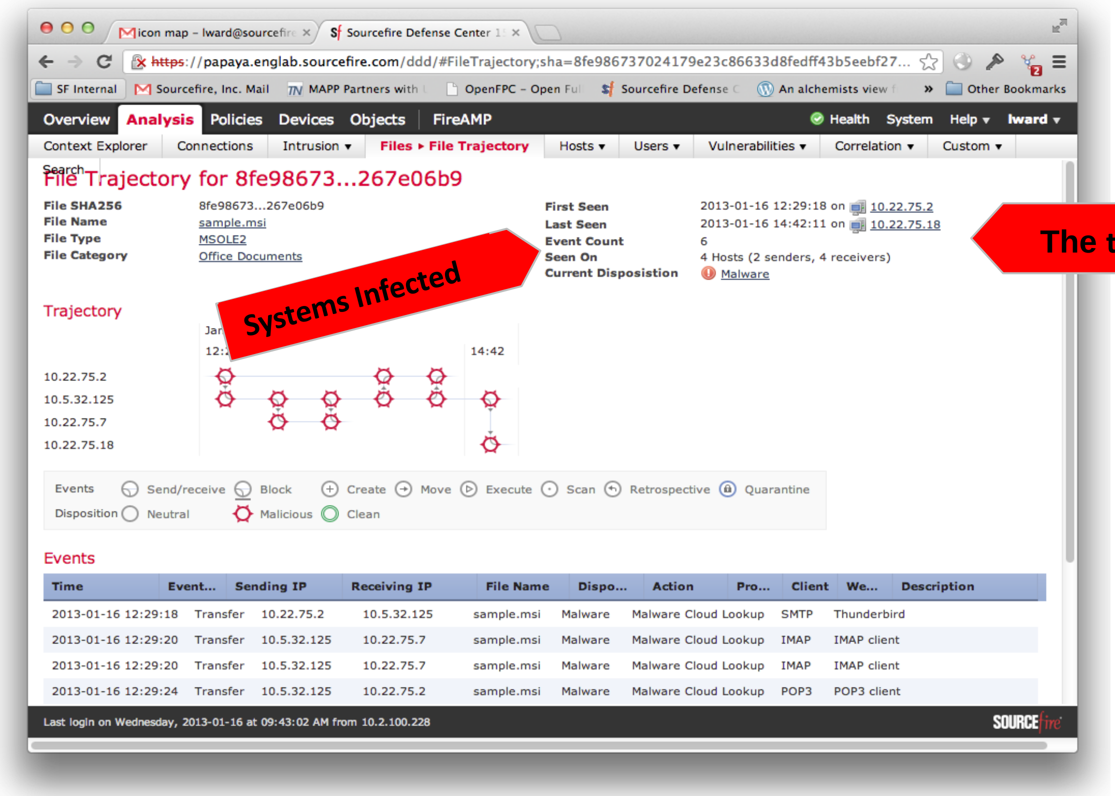
Last updated 1 minutes ago



Initiator IP	Initiator Location	Responder IP
76.100.209.66	USA	10.4.32.112
10.4.10.131		10.4.32.112
10.4.10.131		10.4.32.112
10.4.33.95		10.5.32.206
89.188.101.82	ISR	10.5.32.206
200.189.215.85	BRA	10.4.33.44
10.4.31.237		10.5.32.206
10.4.11.216		10.5.39.206

- Visualise and map countries, cities of hosts, events

Network AMP - Context



File Trajectory for 8fe98673...267e06b9

File SHA256	8fe98673...267e06b9
File Name	sample.msi
File Type	MSOLE2
File Category	Office Documents

First Seen	2013-01-16 12:29:18 on 10.22.75.2
Last Seen	2013-01-16 14:42:11 on 10.22.75.18
Event Count	6
Seen On	4 Hosts (2 senders, 4 receivers)
Current Disposition	Malware

Systems Infected

The time of entry

Trajectory

Events ○ Send/receive ○ Block ⊕ Create ⊖ Move ▷ Execute ⊙ Scan ○ Retrospective ○ Quarantine

Disposition ○ Neutral ○ Malicious ○ Clean

Events

Time	Event...	Sending IP	Receiving IP	File Name	Dispo...	Action	Pro...	Client	We...	Description
2013-01-16 12:29:18	Transfer	10.22.75.2	10.5.32.125	sample.msi	Malware	Malware Cloud Lookup	SMTP	Thunderbird		
2013-01-16 12:29:20	Transfer	10.5.32.125	10.22.75.7	sample.msi	Malware	Malware Cloud Lookup	IMAP	IMAP client		
2013-01-16 12:29:20	Transfer	10.5.32.125	10.22.75.7	sample.msi	Malware	Malware Cloud Lookup	IMAP	IMAP client		
2013-01-16 12:29:24	Transfer	10.5.32.125	10.22.75.2	sample.msi	Malware	Malware Cloud Lookup	POP3	POP3 client		

Last login on Wednesday, 2013-01-16 at 09:43:02 AM from 10.2.100.228

Advanced Malware Protection - AMP

AMP - Overview

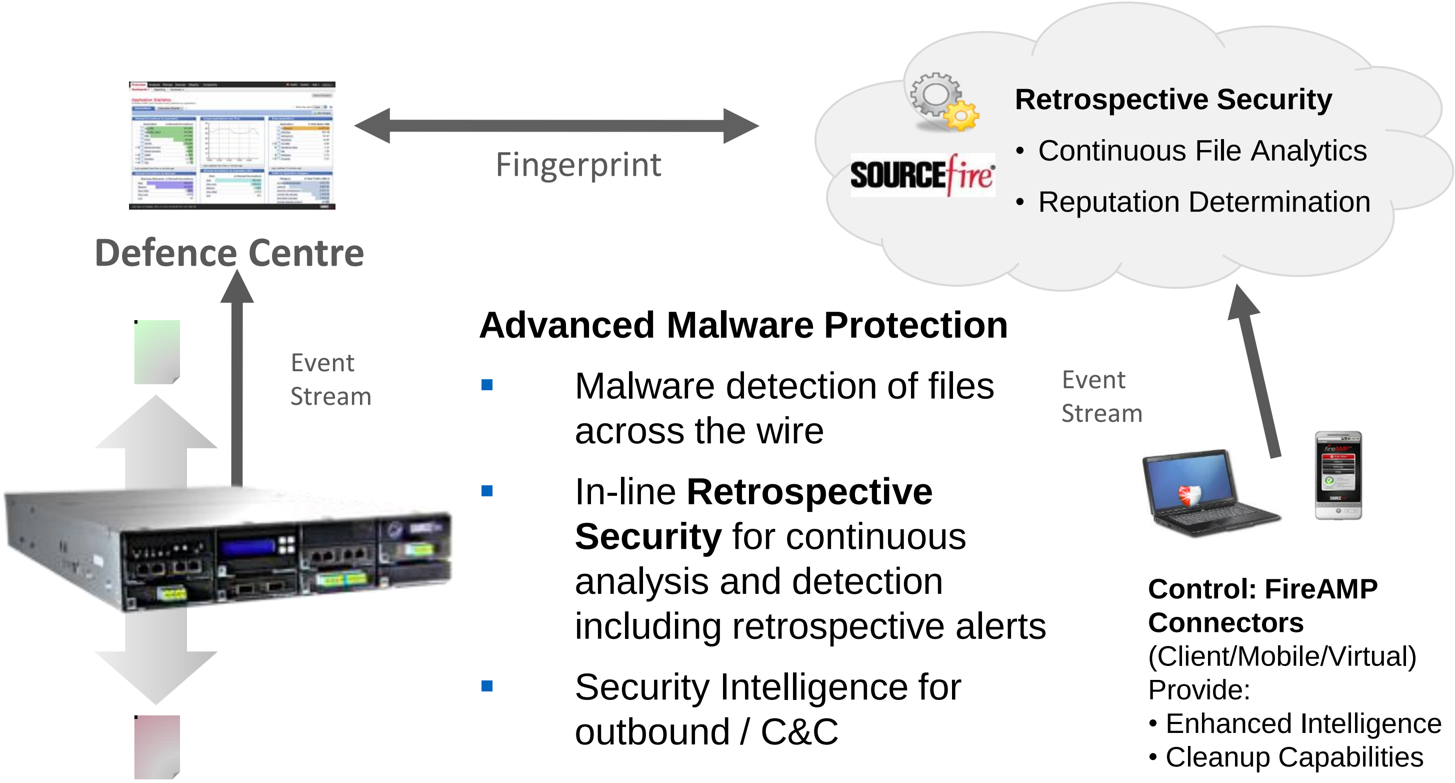
Complete advanced malware protection suite to protect networks and devices

fireAMP™

- Dedicated Advanced Malware Protection (AMP) appliance
- Advanced Malware Protection Subscription for FirePOWER appliances
- Advanced malware protection for hosts virtual and mobile devices

firePOWER™

AMP - Overview



Defence Centre

Fingerprint

Event Stream

Retrospective Security

- Continuous File Analytics
- Reputation Determination

Event Stream

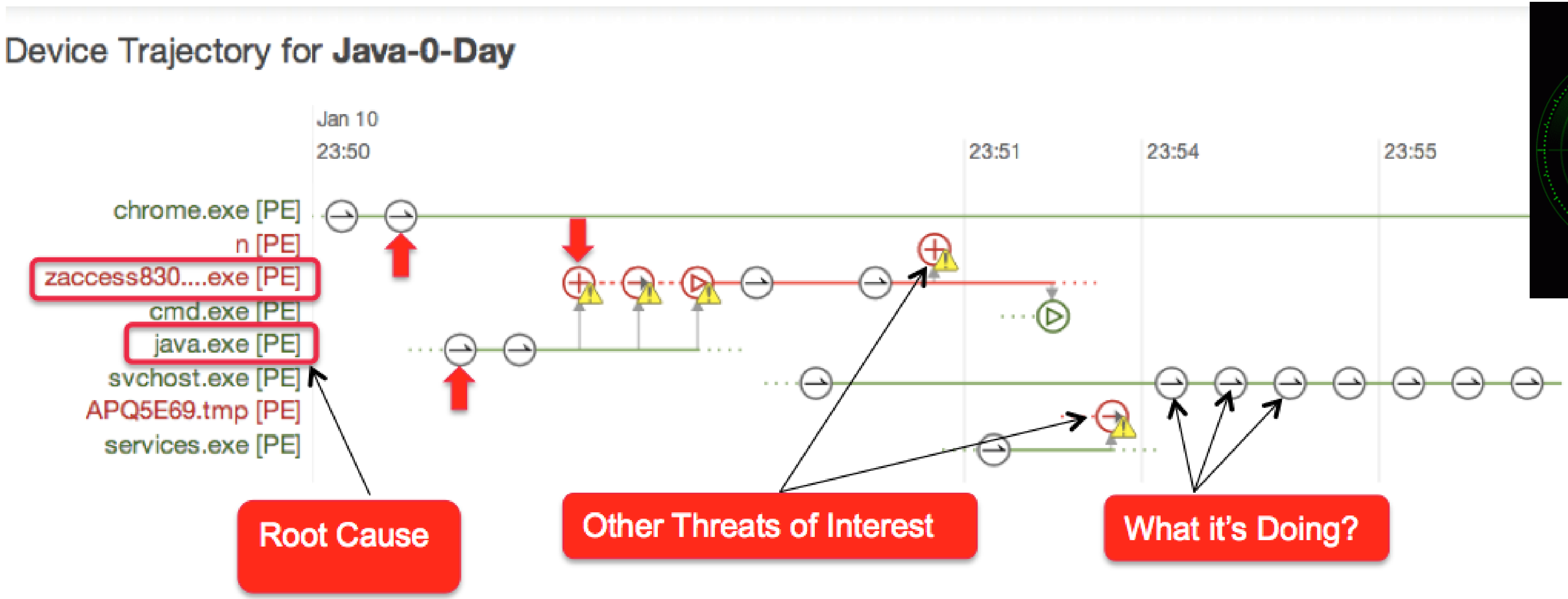
Advanced Malware Protection

- Malware detection of files across the wire
- In-line **Retrospective Security** for continuous analysis and detection including retrospective alerts
- Security Intelligence for outbound / C&C

Control: FireAMP Connectors (Client/Mobile/Virtual) Provide:

- Enhanced Intelligence
- Cleanup Capabilities

AMP – Device trajectory



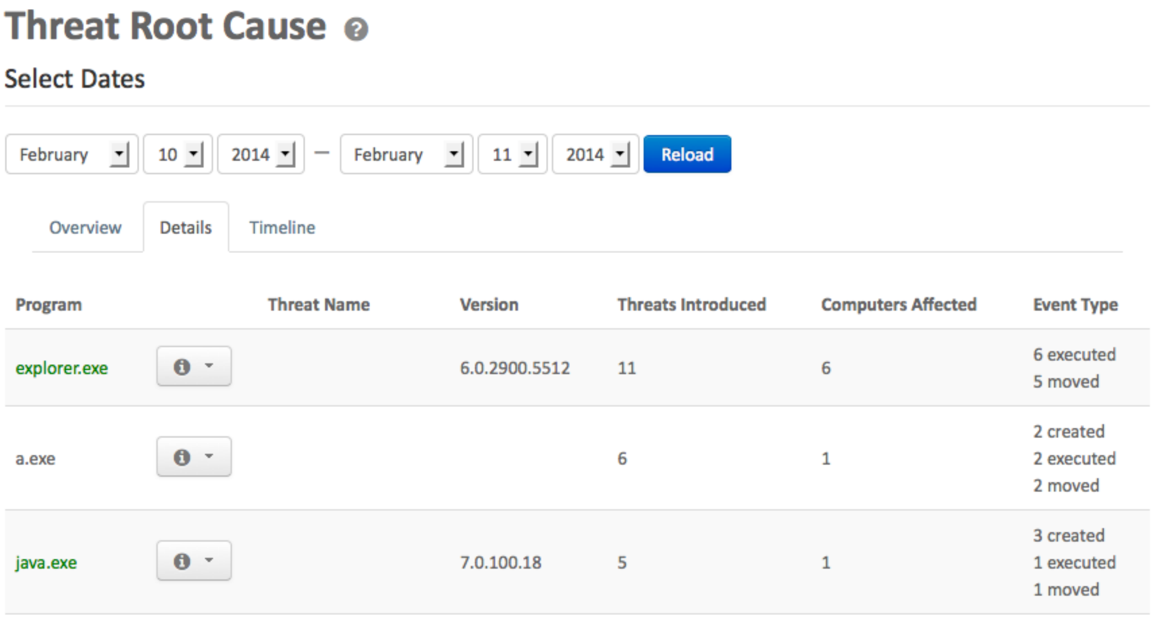
Device Trajectory for **Java-0-Day**

Root Cause

Other Threats of Interest

What it's Doing?

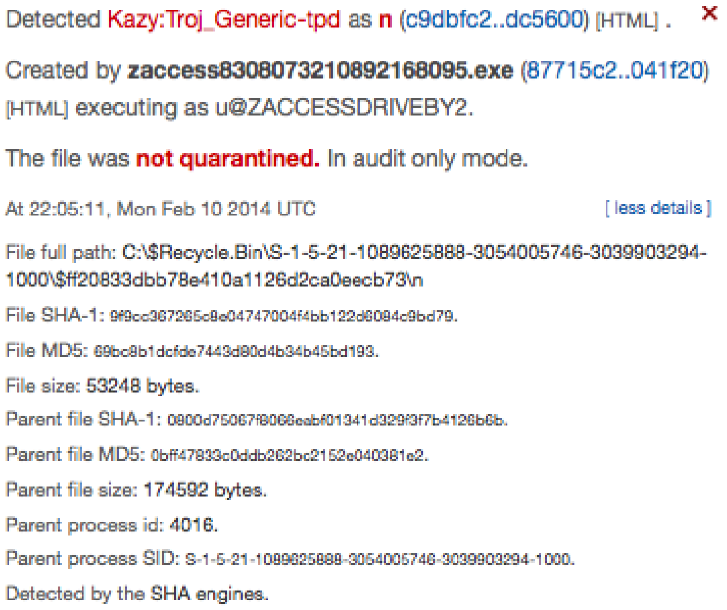
AMP Context – Threat Root Cause



Threat Root Cause

Select Dates

Program		Threat Name	Version	Threats Introduced	Computers Affected	Event Type
explorer.exe			6.0.2900.5512	11	6	6 executed 5 moved
a.exe				6	1	2 created 2 executed 2 moved
java.exe			7.0.100.18	5	1	3 created 1 executed 1 moved



Detected Kazy:Troj_Generic-tpd as n (c9dbfc2..dc5600) [HTML] .

Created by **zaccess8308073210892168095.exe** (87715c2..041f20) [HTML] executing as u@ZACCESSDRIVEBY2.

The file was **not quarantined.** In audit only mode.

At 22:05:11, Mon Feb 10 2014 UTC

File full path: C:\$Recycle.Bin\S-1-5-21-1089625888-3054005746-3039903294-1000\$ff20833dbb78e410a1126d2ca0eecb73\n

File SHA-1: 9f9cc367265c8e04747004f4bb122d6094c9bd79.

File MD5: 69bc8b1dcfde7443d80d4b34b45bd193.

File size: 53248 bytes.

Parent file SHA-1: 0900d75067f8066eabf01341d329f3f7b4126b6b.

Parent file MD5: 0bff47833c0ddb262bc2152e040381e2.

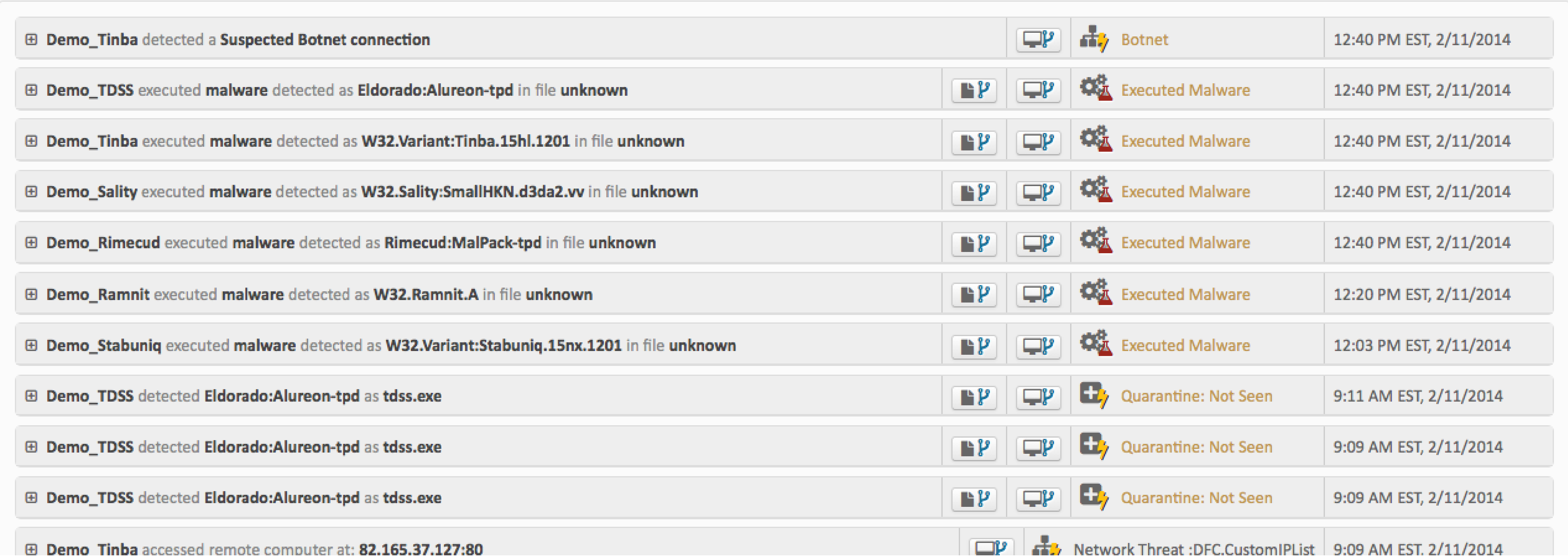
Parent file size: 174592 bytes.

Parent process id: 4016.

Parent process SID: S-1-5-21-1089625888-3054005746-3039903294-1000.

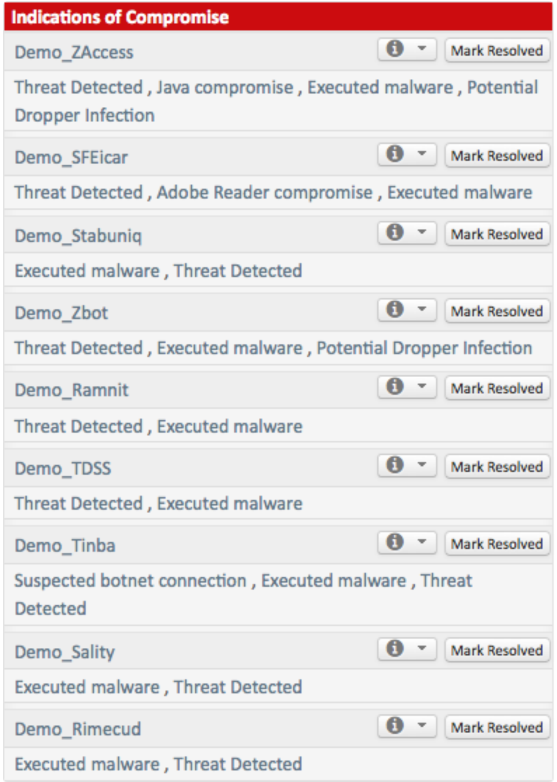
Detected by the SHA engines.

AMP Context – Explorer Details



⊞ **Demo_Tinba** detected a **Suspected Botnet connection**	Botnet	12:40 PM EST, 2/11/2014
⊞ **Demo_TDSS** executed **malware** detected as **Eldorado:Alureon-tpd** in file **unknown**	Executed Malware	12:40 PM EST, 2/11/2014
⊞ **Demo_Tinba** executed **malware** detected as **W32.Variant:Tinba.15hl.1201** in file **unknown**	Executed Malware	12:40 PM EST, 2/11/2014
⊞ **Demo_Sality** executed **malware** detected as **W32.Sality:SmallHKN.d3da2.vv** in file **unknown**	Executed Malware	12:40 PM EST, 2/11/2014
⊞ **Demo_Rimecud** executed **malware** detected as **Rimecud:MalPack-tpd** in file **unknown**	Executed Malware	12:40 PM EST, 2/11/2014
⊞ **Demo_Ramnit** executed **malware** detected as **W32.Ramnit.A** in file **unknown**	Executed Malware	12:20 PM EST, 2/11/2014
⊞ **Demo_Stabuniq** executed **malware** detected as **W32.Variant:Stabuniq.15nx.1201** in file **unknown**	Executed Malware	12:03 PM EST, 2/11/2014
⊞ **Demo_TDSS** detected **Eldorado:Alureon-tpd** as **tdss.exe**	Quarantine: Not Seen	9:11 AM EST, 2/11/2014
⊞ **Demo_TDSS** detected **Eldorado:Alureon-tpd** as **tdss.exe**	Quarantine: Not Seen	9:09 AM EST, 2/11/2014
⊞ **Demo_TDSS** detected **Eldorado:Alureon-tpd** as **tdss.exe**	Quarantine: Not Seen	9:09 AM EST, 2/11/2014
⊞ **Demo_Tinba** accessed remote computer at: **82.165.37.127:80**	Network Threat :DFC.CustomIPList	9:09 AM EST, 2/11/2014

AMP Context – IOC's



Indications of Compromise

Demo_ZAccess

Threat Detected , Java compromise , Executed malware , Potential Dropper Infection

Demo_SFEicar

Threat Detected , Adobe Reader compromise , Executed malware

Demo_Stabuniq

Executed malware , Threat Detected

Demo_Zbot

Threat Detected , Executed malware , Potential Dropper Infection

Demo_Ramnit

Threat Detected , Executed malware

Demo_TDSS

Threat Detected , Executed malware

Demo_Tinba

Suspected botnet connection , Executed malware , Threat Detected

Demo_Sality

Executed malware , Threat Detected

Demo_Rimecud

Executed malware , Threat Detected

- Indicators of Compromise
  - Monitor and Analyse files potential Malware traits
  - Monitors the now & retrospectively convicts files
  - Filters and sorts the most important events
  - Tells the analyst what is happening to reduce TCO
  - Quick links to trajectory
  - Search for SHA's (fingerprints, list all computers that have the file

BEFORE

See it,
Control it

DURING

Intelligent &
Context Aware

AFTER

Retrospective
Security

Vulnerability Management

tenable network security · RAPID7 · QUALYS · Critical Watch (Visibility. Measurability. Control) · Greenbone

Custom Detection

onapsis · WhiteHat Security · NTO (NT Objectives, Inc.)

Network Access/Data Capture

IXIA · Net Optics · Network Critical (The Window to your Network™) · VSS monitoring · Gigamon (The Smart Route To Visibility™) · GARLAND Technology

Full Packet Capture

nPulse Technologies · NETSCOUT · SOLERA Networks

NAC

Bradford Networks (the smart edge) · PacketFence · extreme networks · CITRIX

Incident Response

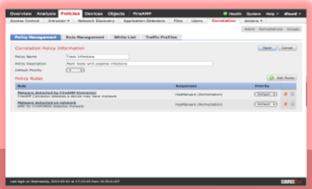
Guidance Software

Visualisation

realstatus (IT insight)

SIEM

BlackStratus · Tier-3 · Trustwave (Information Security & Compliance) · ArcSight · loglogic · splunk> · Q1 Labs (An IBM Company) · LogRhythm



Correlation Policy Information

Policy Name: Track Infections

Policy Description: Mark hosts with possible infections

Default Priority

Policy Rules

Rule	Responses	Priority
Malware detected by FireAMP Connector FireAMP Connector detects a device may have malware	HasMalware (Remediation)	Default
Malware detected on network AMP for FirePOWER detects malware	HasMalware (Remediation)	Default

Last login on Wednesday, [illegible]

FireSIGHT Management Centre

Sourcefire STP Program – API Framework

Cisco live!

Deployment Scenarios / Considerations

Deployment Scenarios / Usage – NGIPS / NGFW

- Data Centre GW
- Partner Networks / OGO's
- Branch Office Links
- ISP feeds
- DMZs
- Segregated PCI LAN
- Out of band management LAN
- VLAN's
- Internal (Core) LAN
- Critical Infrastructure LAN

- Traditional IDS / IPS
- Malware Detection
- Data Exfiltration (insider threat)
- Bandwidth Hogs
- Improper use of Corporate systems
  - (Websites / BitTorrent)
- Compliance PII / PCI data breaches
- Application usage / control and adherence to policies
- BYOD
- Due Diligence

Deployment Scenarios / Usage – Virtual

- Partner Networks / OGO's
- Branch Office Links
- DMZs
- Segregated PCI LAN
- Out of band management LAN
- VLAN's
- Internal (Core) LAN
- Critical Infrastructure LAN
- Deployed Infrastructure (Defence)
- Cloud Services

- Traditional IDS / IPS
- Malware Detection
- Data Exfiltration (insider threat)
- Bandwidth Hogs
- Improper use of Corporate systems
  - (Websites / BitTorrent)
- Compliance PII / PCI data breaches
- Application usage / control and adherence to policies
- BYOD
- Due Diligence
- Resilience!

Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2014 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 21 March 12:00pm - 2:00pm

Learn online with Cisco Live!

Visit us online after the conference for full access to session videos and presentations. www.CiscoLiveAPAC.com cisco TM