cisco

Cisco Connect

Riyadh, Saudi Arabia

April 29-30, 2014

TOMORROW starts here.

Next Generation IPS and Advance Malware Protection

Mahmoud Rabi

Consulting Systems Engineer - Security

Threat Landscape and Attack Continuum

Today's Real World: Threats are evolving and evading traditional defense

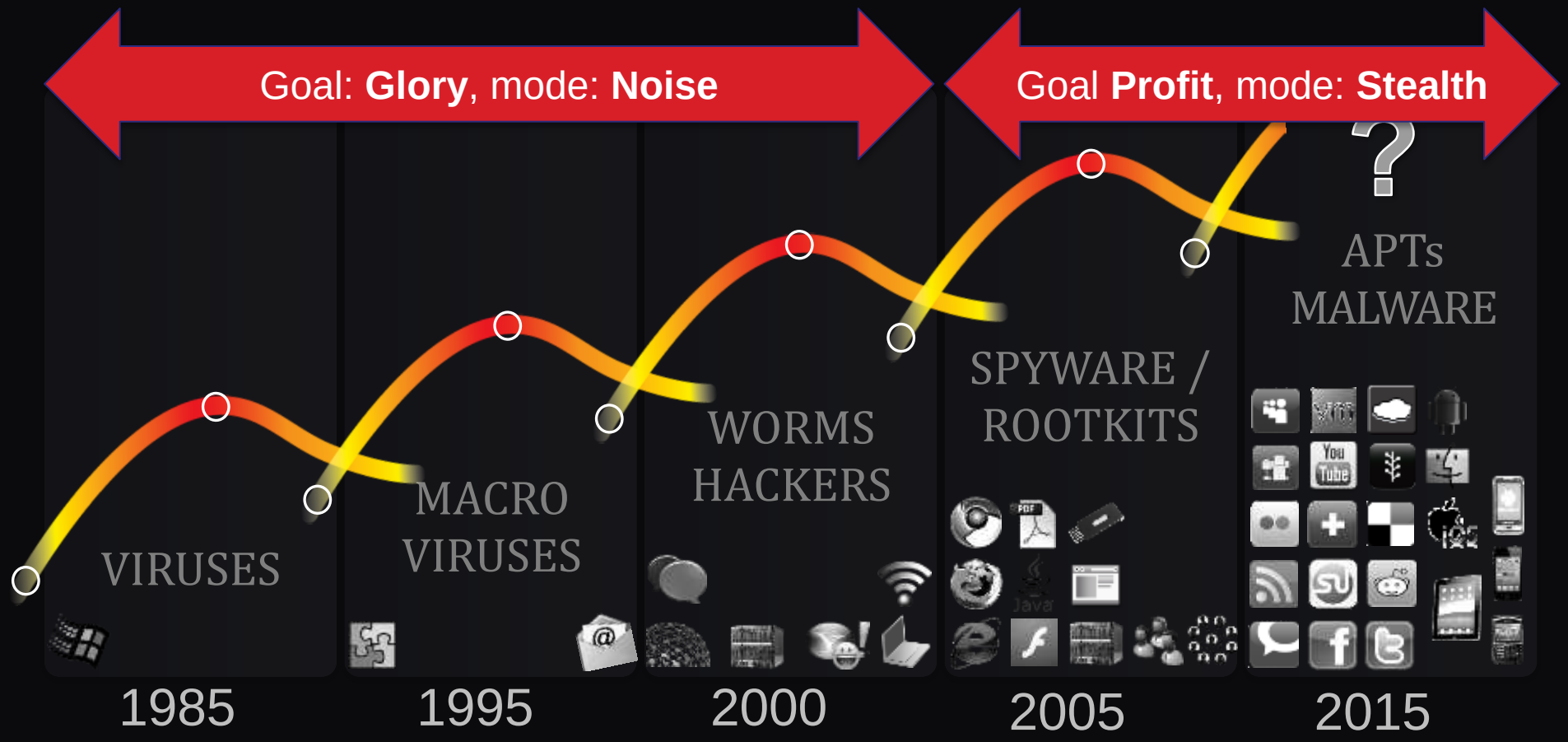
All were smart. All had security.
All were seriously compromised.

Today's Real World: Threats are evolving and evading traditional defense

So what's changed?

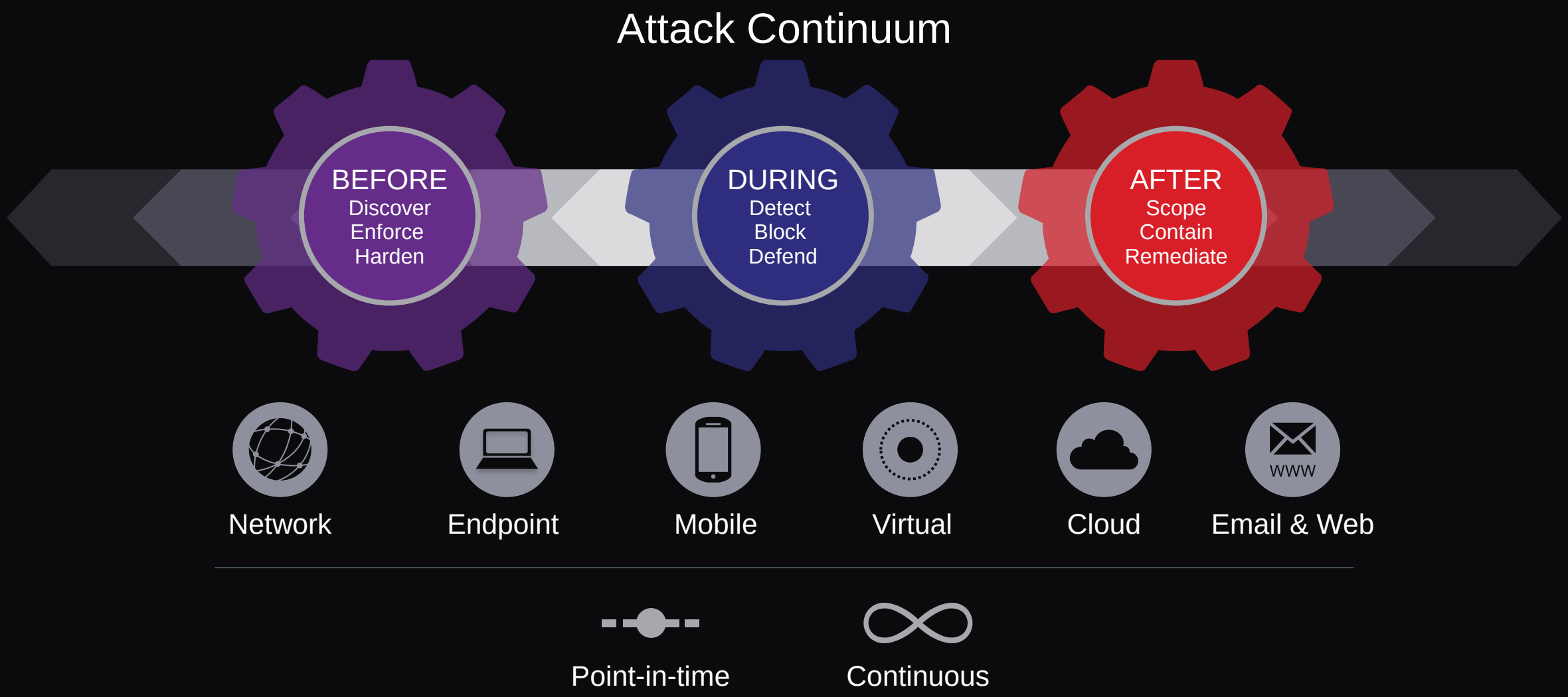
Hacking has!

Industrialization of Hacking



Attackers and defenders drive each other to innovate…
…resulting in distinct threat cycles

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



You should know the Estate of Your Network

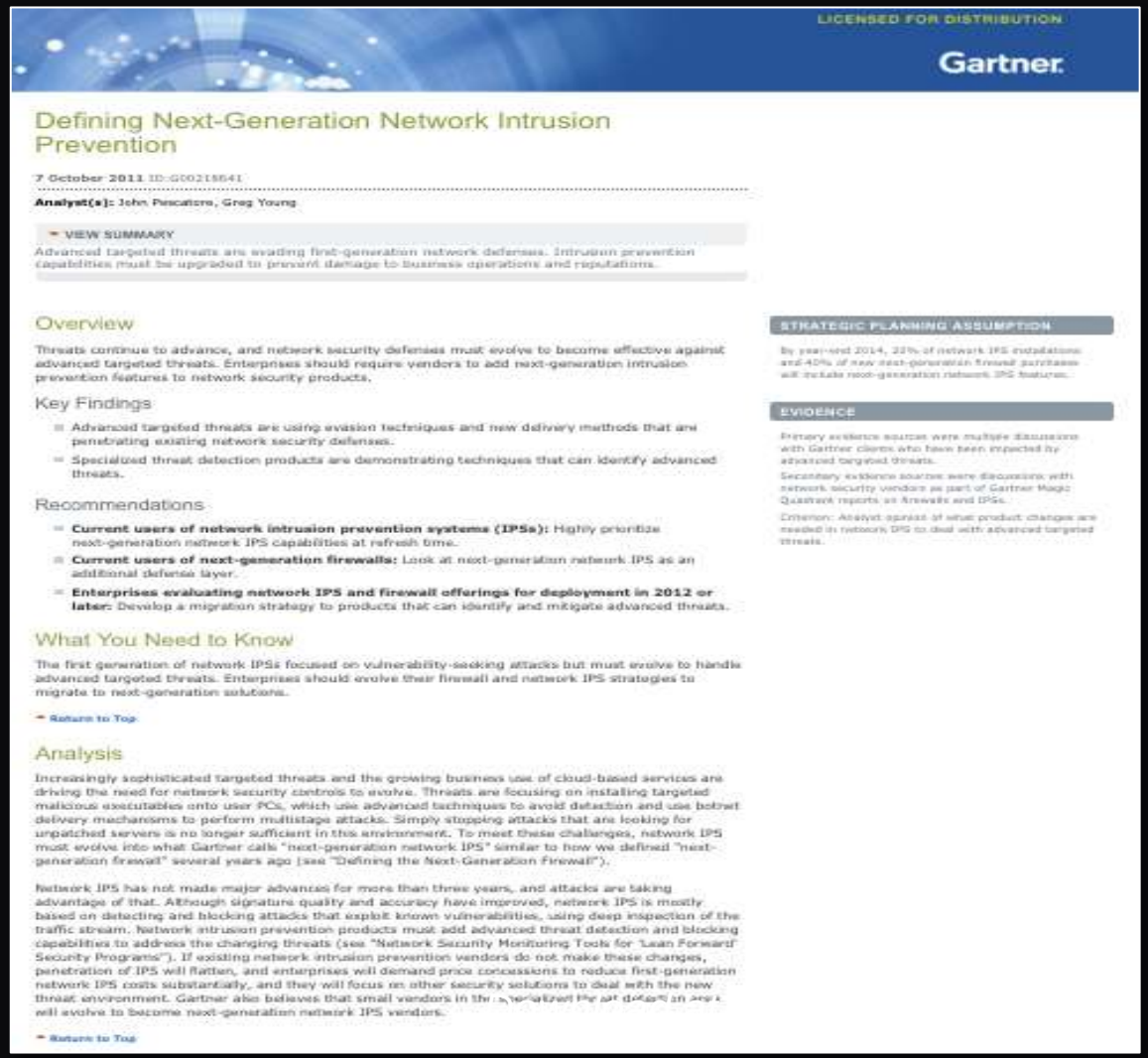
You can not protect what you can not see


Next Generation IPS

Gartner Defines Next-Generation IPS

NGIPS Definition

- Standard First-Gen IPS
- Context Awareness
- Application Awareness and full-stack visibility
- Content Awareness
- Adaptive Engine



LICENSED FOR DISTRIBUTION

Gartner

Defining Next-Generation Network Intrusion Prevention

7 October 2011 ID:G00218641

Analyst(s): John Pescatore, Greg Young

VIEW SUMMARY

Advanced targeted threats are evading first-generation network defenses. Intrusion prevention capabilities must be upgraded to prevent damage to business operations and reputations.

Overview

Threats continue to advance, and network security defenses must evolve to become effective against advanced targeted threats. Enterprises should require vendors to add next-generation intrusion prevention features to network security products.

Key Findings

- Advanced targeted threats are using evasion techniques and new delivery methods that are penetrating existing network security defenses.
- Specialized threat detection products are demonstrating techniques that can identify advanced threats.

Recommendations

- **Current users of network intrusion prevention systems (IPSs):** Highly prioritize next-generation network IPS capabilities at refresh time.
- **Current users of next-generation firewalls:** Look at next-generation network IPS as an additional defense layer.
- **Enterprises evaluating network IPS and firewall offerings for deployment in 2012 or later:** Develop a migration strategy to products that can identify and mitigate advanced threats.

What You Need to Know

The first generation of network IPSs focused on vulnerability-seeking attacks but must evolve to handle advanced targeted threats. Enterprises should evolve their firewall and network IPS strategies to migrate to next-generation solutions.

Return to Top

Analysis

Increasingly sophisticated targeted threats and the growing business use of cloud-based services are driving the need for network security controls to evolve. Threats are focusing on installing targeted malicious executables onto user PCs, which use advanced techniques to avoid detection and use botnet delivery mechanisms to perform multistage attacks. Simply stopping attacks that are looking for unpatched servers is no longer sufficient in this environment. To meet these challenges, network IPS must evolve into what Gartner calls "next-generation network IPS" similar to how we defined "next-generation firewall" several years ago [see "Defining the Next-Generation Firewall").

Network IPS has not made major advances for more than three years, and attacks are taking advantage of that. Although signature quality and accuracy have improved, network IPS is mostly based on detecting and blocking attacks that exploit known vulnerabilities, using deep inspection of the traffic stream. Network intrusion prevention products must add advanced threat detection and blocking capabilities to address the changing threats (see "Network Security Monitoring Tools for 'Lean Forward' Security Programs"). If existing network intrusion prevention vendors do not make these changes, penetration of IPS will flatten, and enterprises will demand price concessions to reduce first-generation network IPS costs substantially, and they will focus on other security solutions to deal with the new threat environment. Gartner also believes that small vendors in the specialized IPS [illegible] will evolve to become next-generation network IPS vendors.

Return to Top

STRATEGIC PLANNING ASSUMPTION

By year-end 2014, 20% of network IPS installations and 40% of new next-generation firewall purchases will include next-generation network IPS features.

EVIDENCE

Primary evidence sources were multiple discussions with Gartner clients who have been impacted by advanced targeted threats.

Secondary evidence sources were discussions with network security vendors as part of Gartner Magic Quadrant reports on firewalls and IPSs.

Criterion: Analyst opinion of what product changes are needed in network IPS to deal with advanced targeted threats.

Source: "Defining Next-Generation Network Intrusion Prevention" Gartner, October 7, 2011

What do we mean by Context Awareness

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

Typical Intrusion Event

Event:	Attempted Privilege Gain
Target:	96.16.242.135

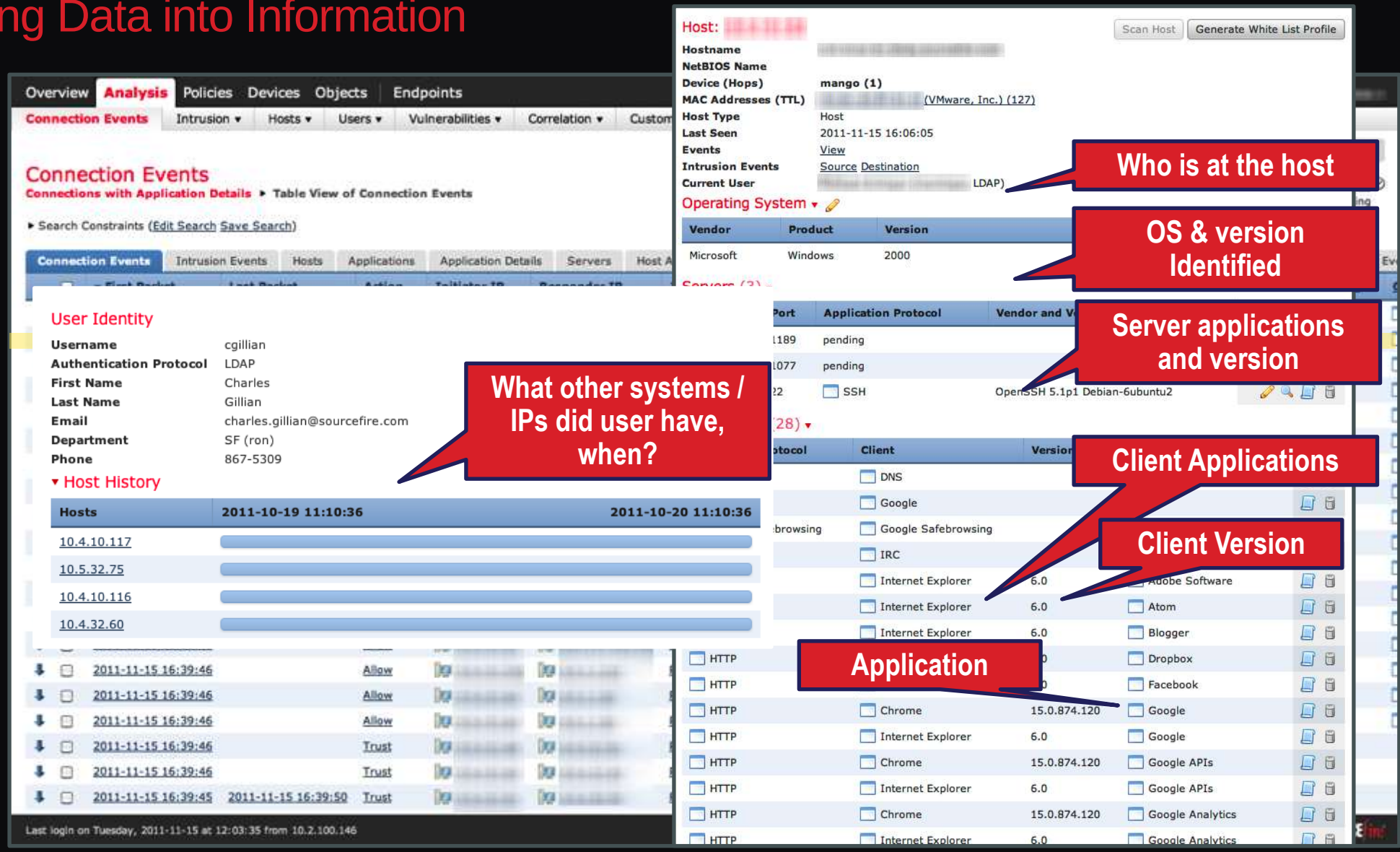
FireSIGHT™ Full Stack Visibility

CATEGORIES	EXAMPLES	Cisco Sourcefire FireSIGHT	TYPICAL IPS	TYPICAL NGFW
Threats	Attacks, Anomalies	✔	✔	✔
Users	AD, LDAP, POP3	✔	✗	✔
Web Applications	Facebook Chat, Ebay	✔	✗	✔
Application Protocols	HTTP, SMTP, SSH	✔	✗	✔
File Transfers	PDF, Office, EXE, JAR	✔	✗	✔
Malware	Conficker, Flame	✔	✗	✗
Command & Control Servers	C&C Security Intelligence	✔	✗	✗
Client Applications	Firefox, IE6, BitTorrent	✔	✗	✗
Network Servers	Apache 2.3.1, IIS4	✔	✗	✗
Operating Systems	Windows, Linux	✔	✗	✗
Routers & Switches	Cisco, Nortel, Wireless	✔	✗	✗
Mobile Devices	iPhone, Android, Jail	✔	✗	✗
Printers	HP, Xerox, Canon	✔	✗	✗
VoIP Phones	Avaya, Polycom	✔	✗	✗
Virtual Machines	VMware, Xen, RHEV	✔	✗	✗

Information Superiority → Contextual Awareness

Building Host Profiles

Converting Data into Information



Indicators of Compromise Within Host Profile

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

May have connected an Exploit Kit

+

Has connected to a host that SI tells us could be a CnC server

+

Has triggered an IPS event for traffic that looks like CnC

Indications of Compromise (3) = 3

Edit Rule States | Mark All Resolved

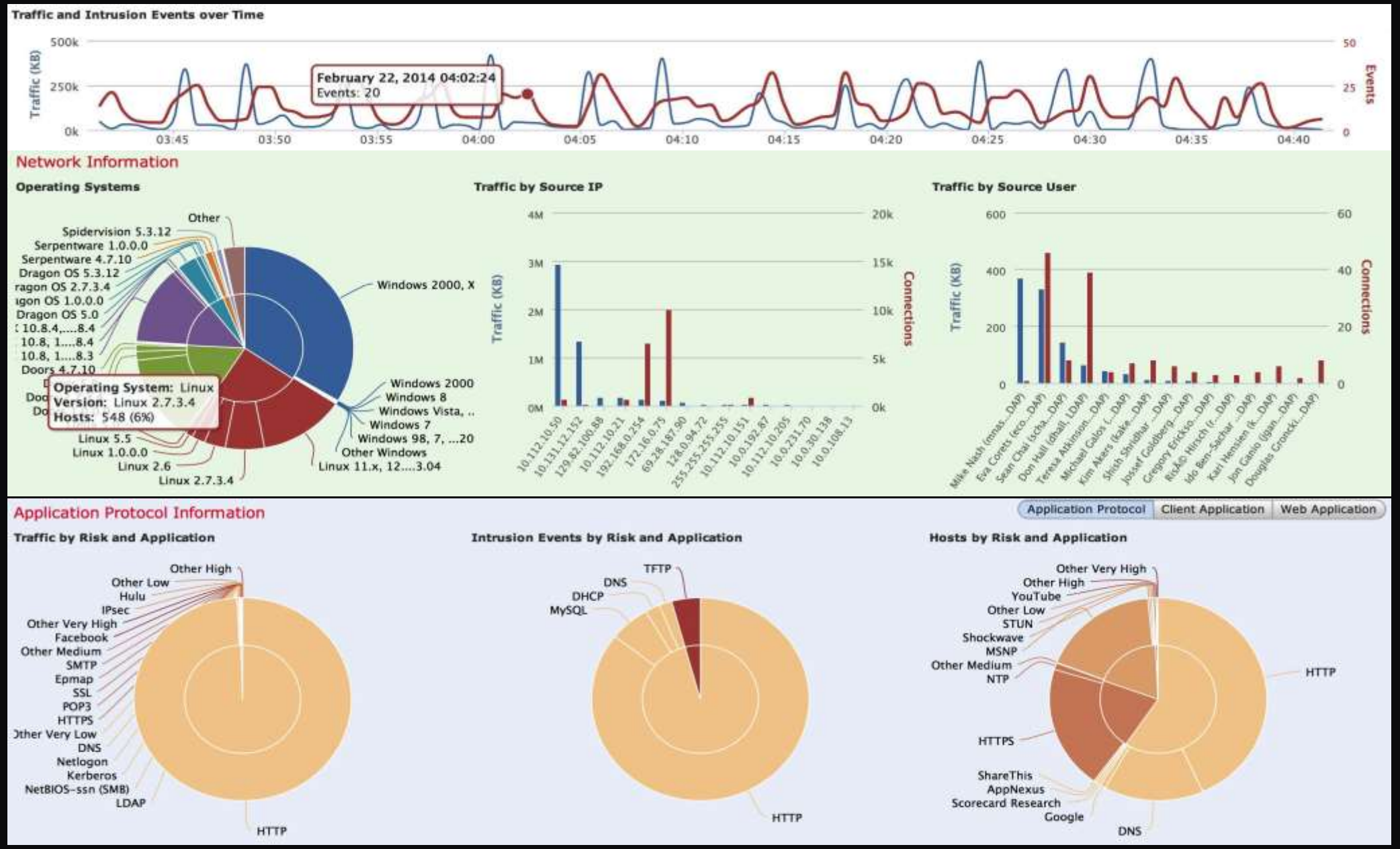
Category	Event Type	Description	First Seen	Last Seen
Exploit Kit	Intrusion Event - exploit-kit	The host may have encountered an exploit kit	2013-09-17 16:46:28	2013-09-20 06:35:31
CnC Connected	Security Intelligence Event - CnC	The host may be under remote control	2013-09-17 16:52:11	2013-09-20 03:55:45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

FireSIGHT™ Context Explorer



FireSIGHT™ Fuels NGIPS

IT Insight
Spot rogue hosts, anomalies, policy violations, and more

Impact Assessment
Threat correlation reduces actionable events by up to 99%

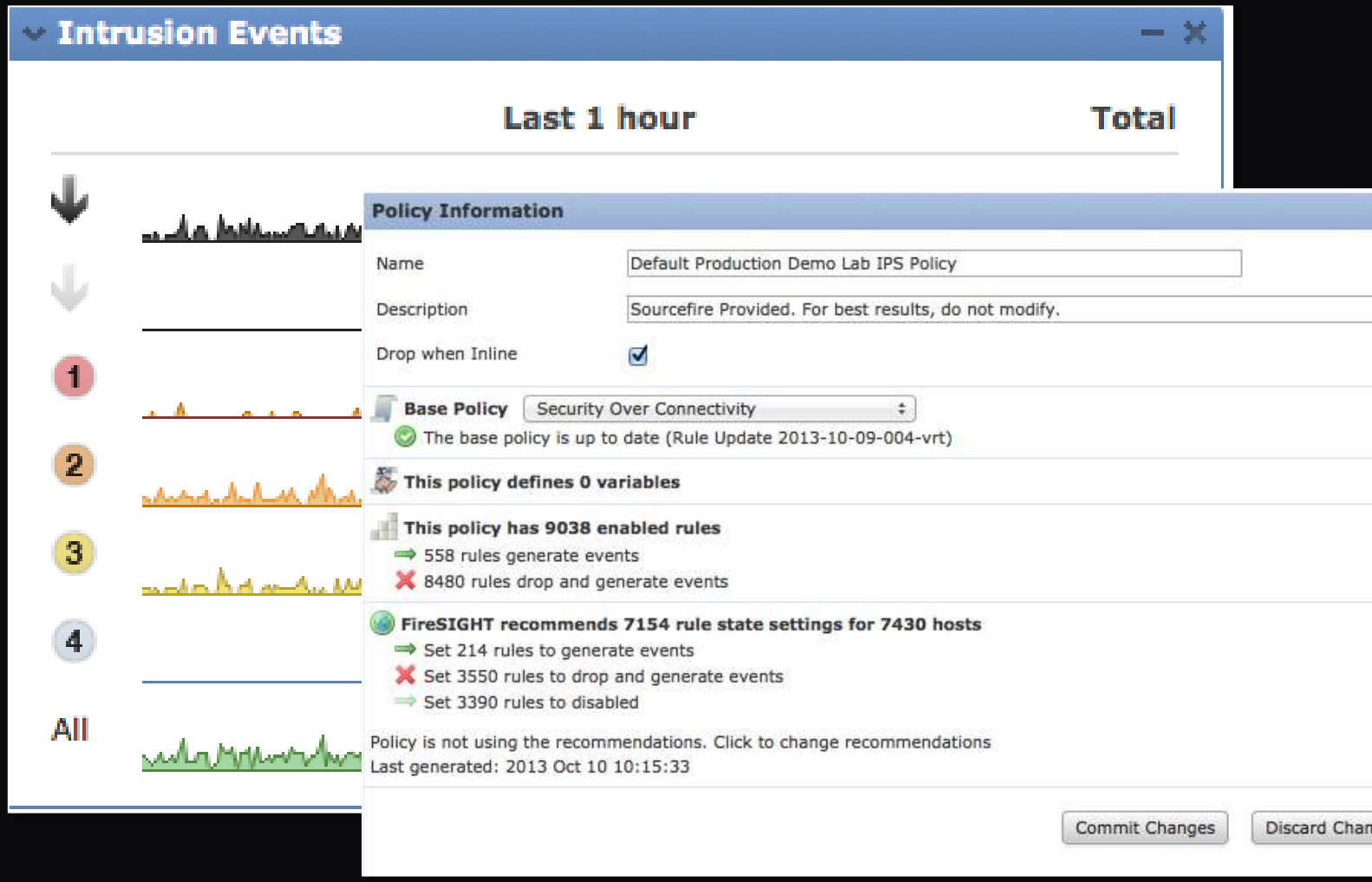
Automated Tuning
Adjust IPS policies automatically based on network change

User Identification
Associate users with security and compliance events

FireSIGHT™ Streamlines Operations

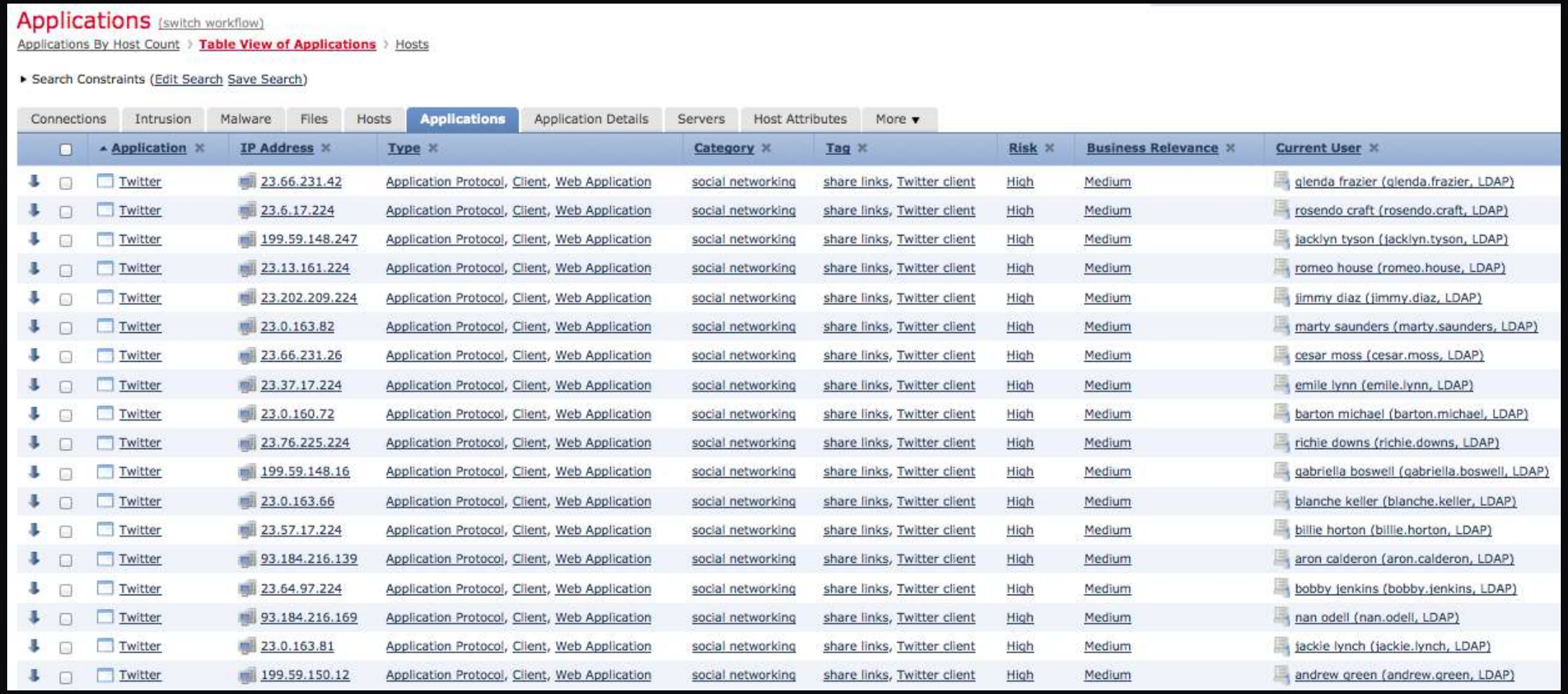
Impact Assessment and Generate Rules Recommendations (**Adaption**)

- Impact Assessment for all intrusion events (Linux based attack to Windows machine)
- Enable the IPS rules that should be enabled based on profiled network
- Easy access to all assessed intrusion events



FireSIGHT™ Reduces Response Time

Associate Users with Intrusion and Compliance Events



Applications (switch workflow)

Applications By Host Count › **Table View of Applications** › Hosts

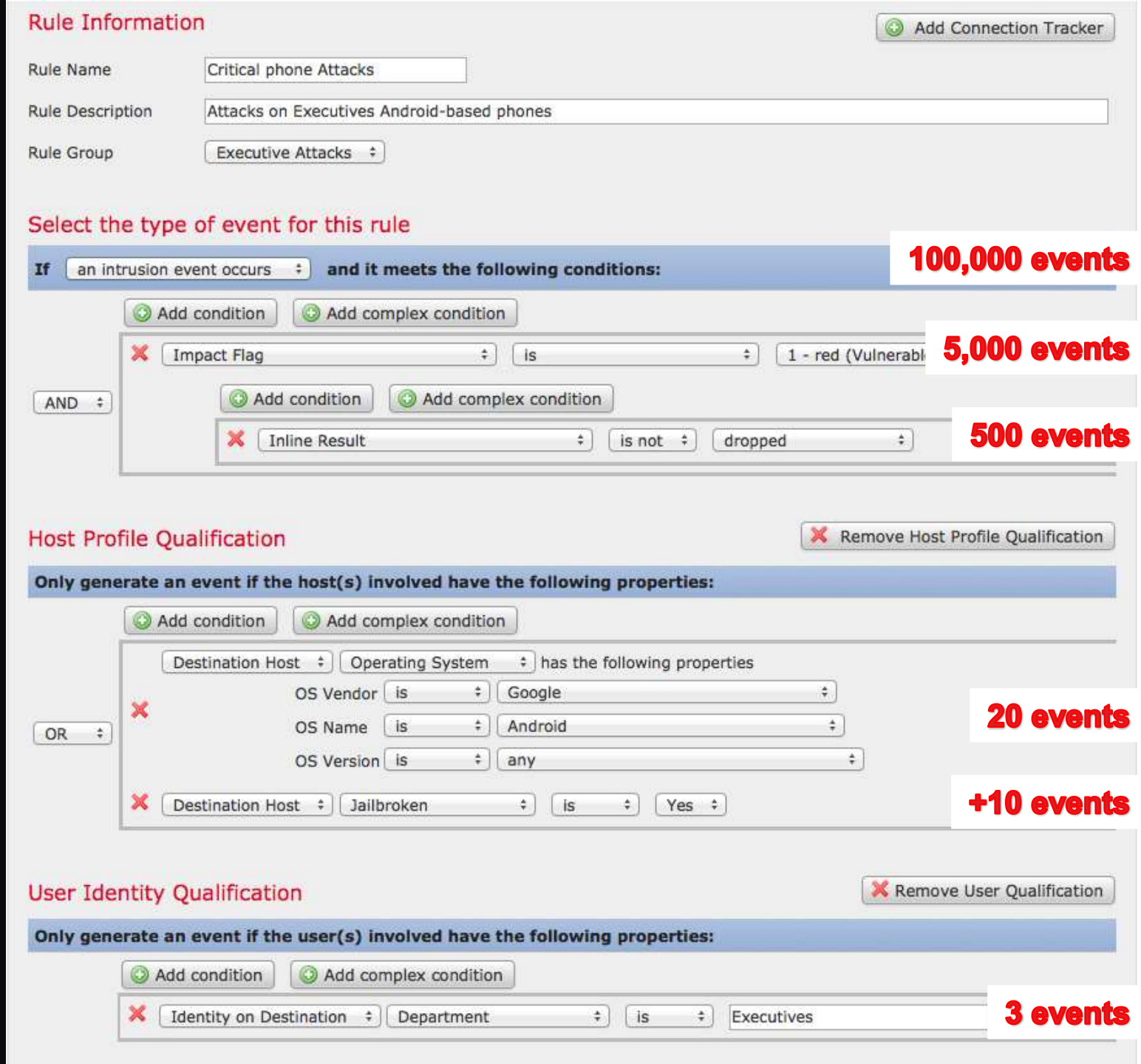
▸ Search Constraints (Edit Search Save Search)

Connections | Intrusion | Malware | Files | Hosts | **Applications** | Application Details | Servers | Host Attributes | More ▾

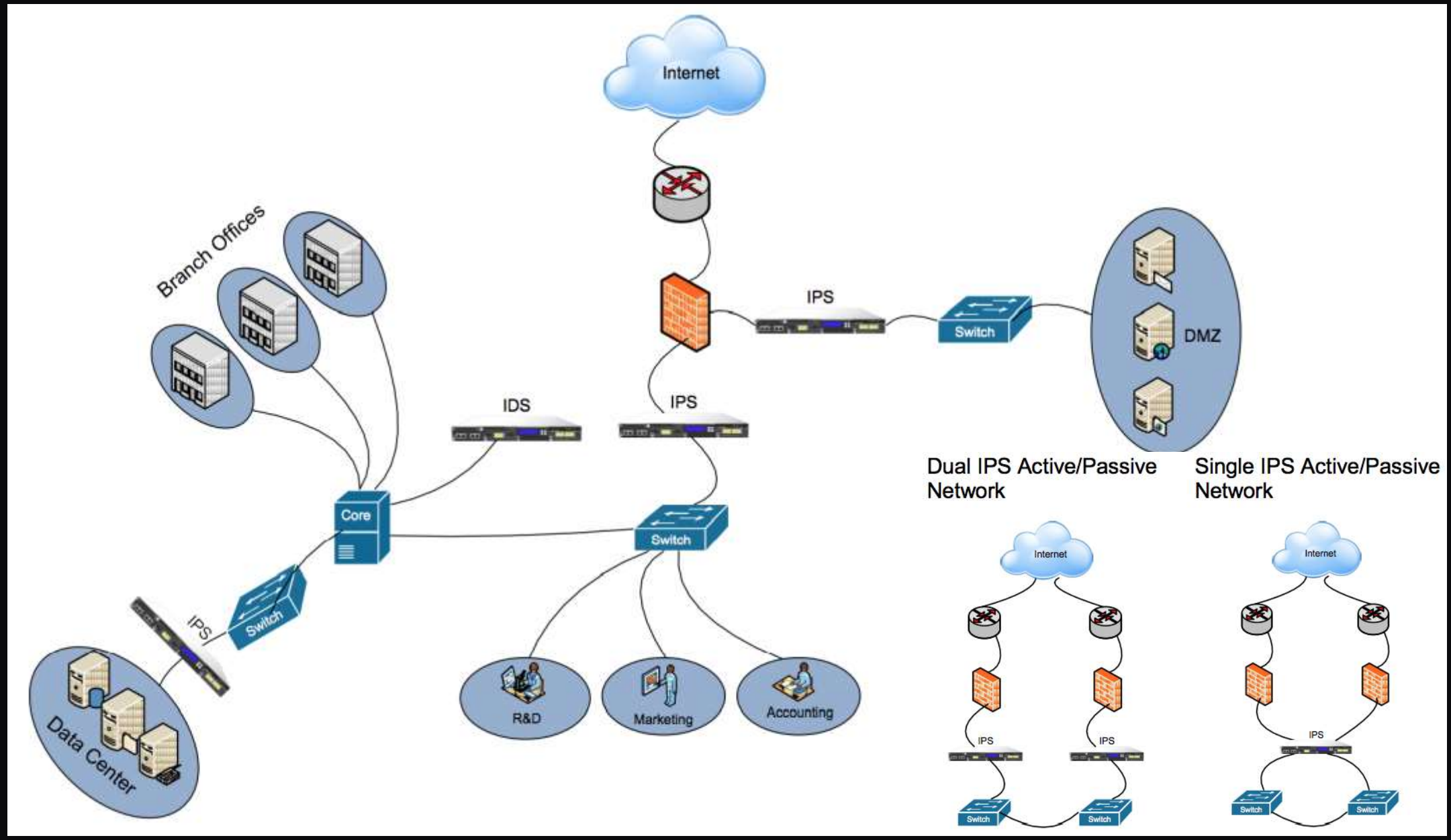
Application	IP Address	Type	Category	Tag	Risk	Business Relevance	Current User
Twitter	23.66.231.42	Application Protocol, Client, Web Application	social networking	share links, Twitter client	High	Medium	glenda frazier (glenda.frazier, LDAP)
Twitter	23.6.17.224	Application Protocol, Client, Web Application	social networking	share links, Twitter client	High	Medium	rosendo craft (rosendo.craft, LDAP)
Twitter	199.59.148.247	Application Protocol, Client, Web Application	social networking	share links, Twitter client	High	Medium	jacklyn tyson (jacklyn.tyson, LDAP)
Twitter	23.13.161.224	Application Protocol, Client, Web Application	social networking	share links, Twitter client	High	Medium	romeo house (romeo.house, LDAP)
Twitter	23.202.209.224	Application Protocol, Client, Web Application	social networking	share links, Twitter client	High	Medium	jimmy diaz (jimmy.diaz, LDAP)
Twitter	23.0.163.82	Application Protocol, Client, Web Application	social networking	share links, Twitter client	High	Medium	marty saunders (marty.saunders, LDAP)
Twitter	23.66.231.26	Application Protocol, Client, Web Application	social networking	share links, Twitter client	High	Medium	cesar moss (cesar.moss, LDAP)
Twitter	23.37.17.224	Application Protocol, Client, Web Application	social networking	share links, Twitter client	High	Medium	emile lynn (emile.lynn, LDAP)
Twitter	23.0.160.72	Application Protocol, Client, Web Application	social networking	share links, Twitter client	High	Medium	barton michael (barton.michael, LDAP)
Twitter	23.76.225.224	Application Protocol, Client, Web Application	social networking	share links, Twitter client	High	Medium	richie downs (richie.downs, LDAP)
Twitter	199.59.148.16	Application Protocol, Client, Web Application	social networking	share links, Twitter client	High	Medium	gabriella boswell (gabriella.boswell, LDAP)
Twitter	23.0.163.66	Application Protocol, Client, Web Application	social networking	share links, Twitter client	High	Medium	blanche keller (blanche.keller, LDAP)
Twitter	23.57.17.224	Application Protocol, Client, Web Application	social networking	share links, Twitter client	High	Medium	billie horton (billie.horton, LDAP)
Twitter	93.184.216.139	Application Protocol, Client, Web Application	social networking	share links, Twitter client	High	Medium	aron calderon (aron.calderon, LDAP)
Twitter	23.64.97.224	Application Protocol, Client, Web Application	social networking	share links, Twitter client	High	Medium	bobby jenkins (bobby.jenkins, LDAP)
Twitter	93.184.216.169	Application Protocol, Client, Web Application	social networking	share links, Twitter client	High	Medium	nan odell (nan.odell, LDAP)
Twitter	23.0.163.81	Application Protocol, Client, Web Application	social networking	share links, Twitter client	High	Medium	jackie lynch (jackie.lynch, LDAP)
Twitter	199.59.150.12	Application Protocol, Client, Web Application	social networking	share links, Twitter client	High	Medium	andrew green (andrew.green, LDAP)

Real Time Correlation

- Leverage Real Time Visibility
- Find the needle in the Haystack
- Correlation based on a Real Time traffic
- Receive alerts for specific scenarios
- Alert me for something specific
- Drop from 100K events to 3 specific events



Deployment Scenarios



Gartner Leadership

The Path “Up and Right”

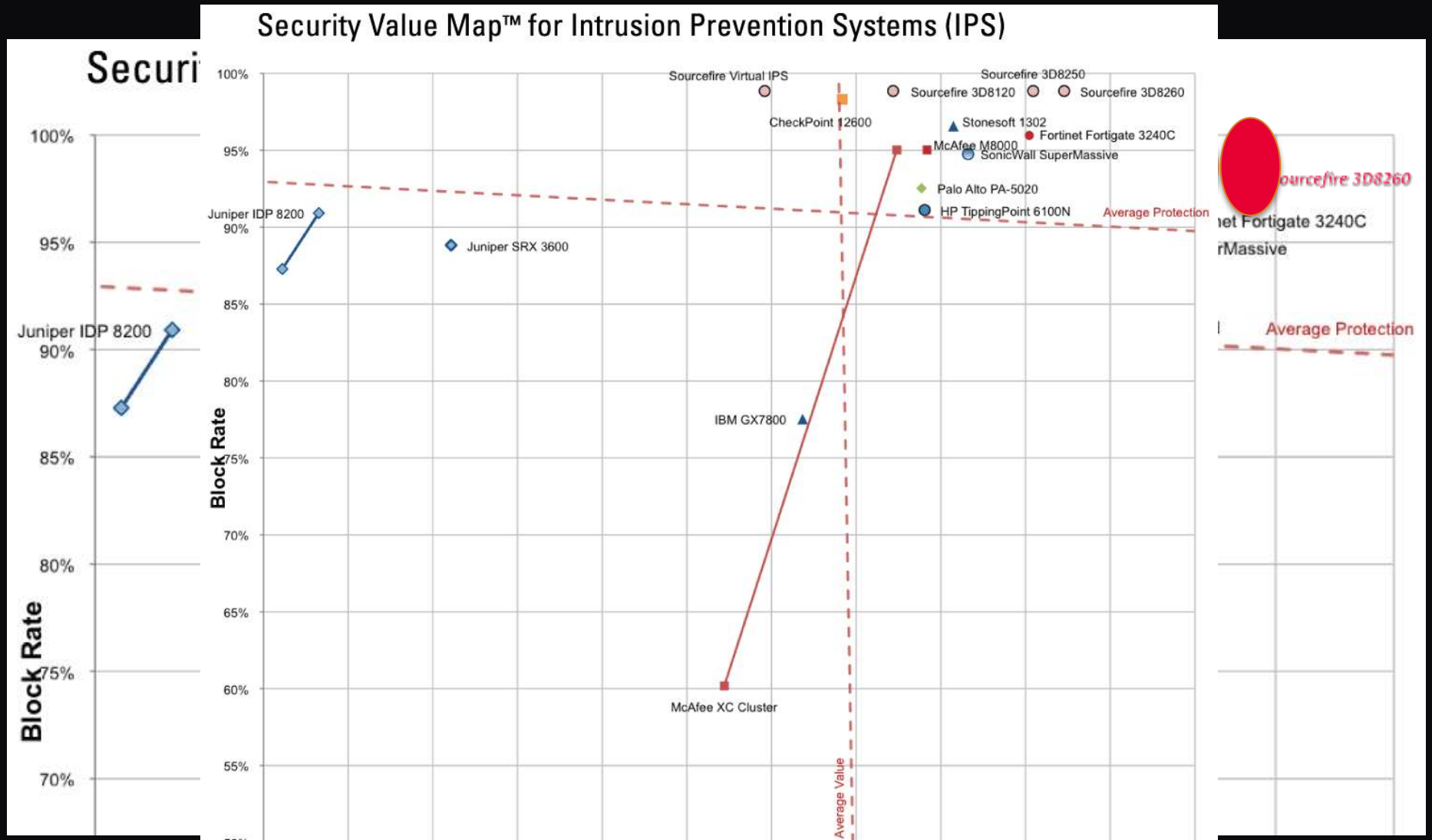
Gartner

Sourcefire has been a leader in the Gartner Magic Quadrant for IPS since 2006.

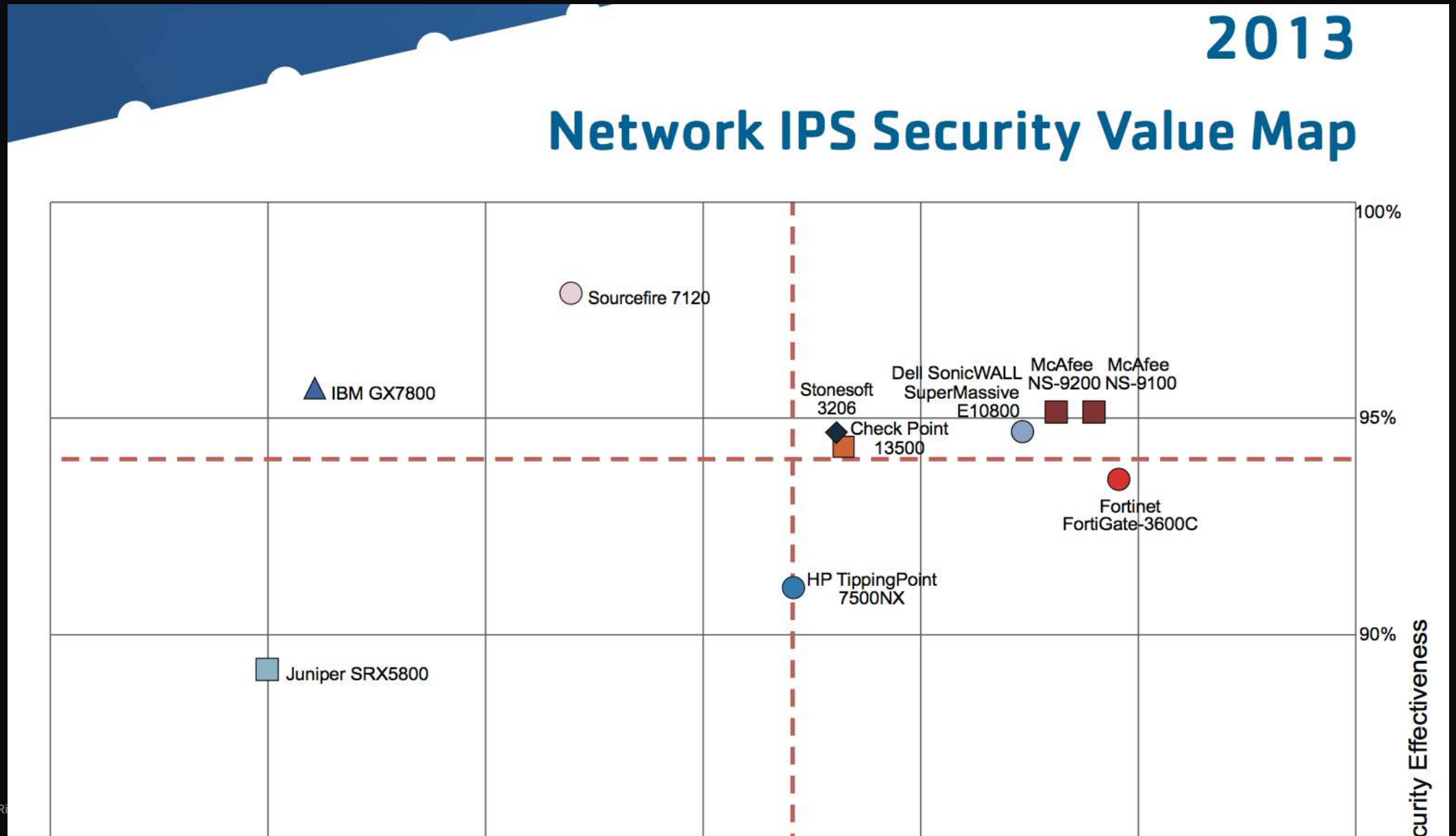
As of December 2013

Source: Gartner (December 2013)

2012 NSS Labs SVM for IPS

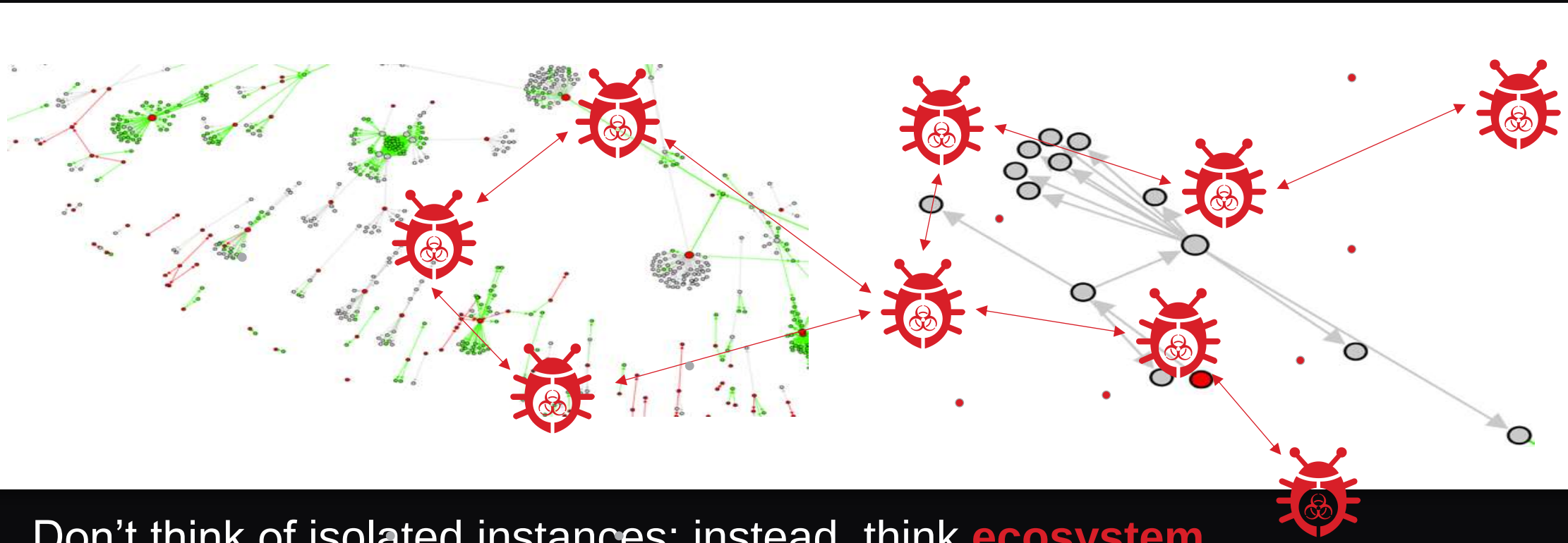


2013 NSS Labs SVM for IPS




Advanced Malware Protection

Malware Ecosystem: Droppers



- Don’t think of isolated instances; instead, think **ecosystem**
- Address ecosystem, otherwise re-infections occur

Cisco Sourcefire Advanced Malware Protection

Complete solution suite to protect the extended network

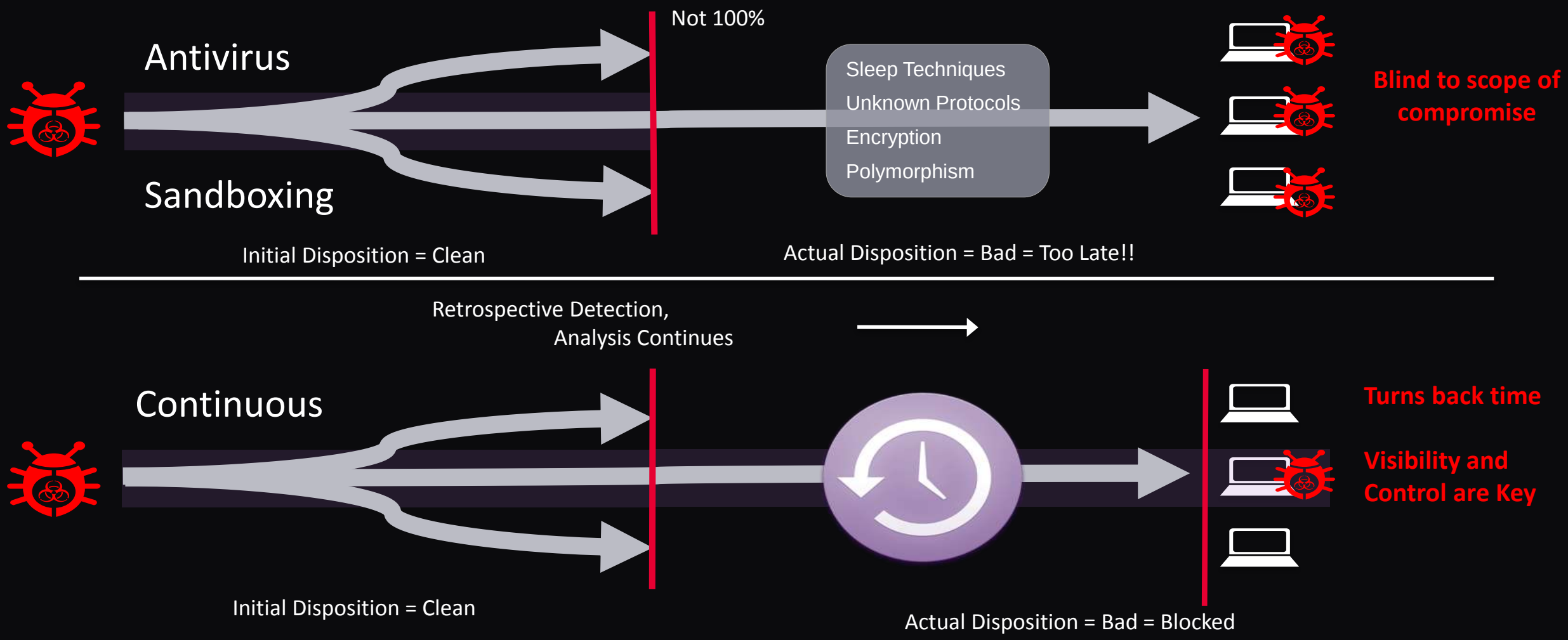
Dedicated Advanced Malware Protection (AMP) Appliances (FirePOWER & WSA/ESA

Advanced Malware Protection for FirePOWER (NGIPS)

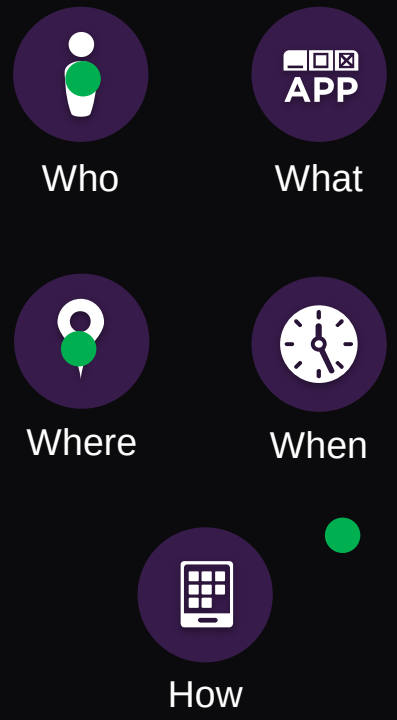
FireAMP for hosts (MS Windows & Mac), virtual and mobile devices

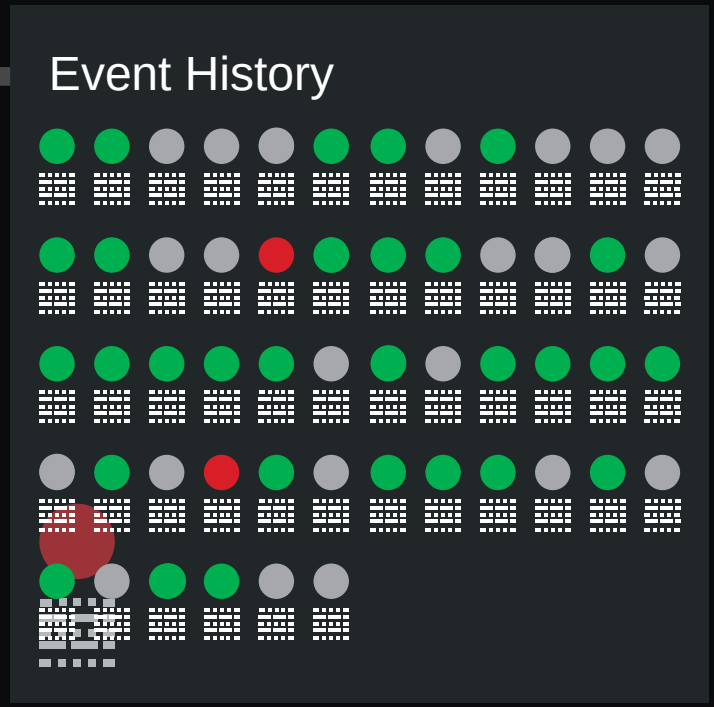
Beyond the Event Horizon

Addresses limitations of point-in-time detection



And the tools in place to rapidly isolate and remediate





Context

Enforcement

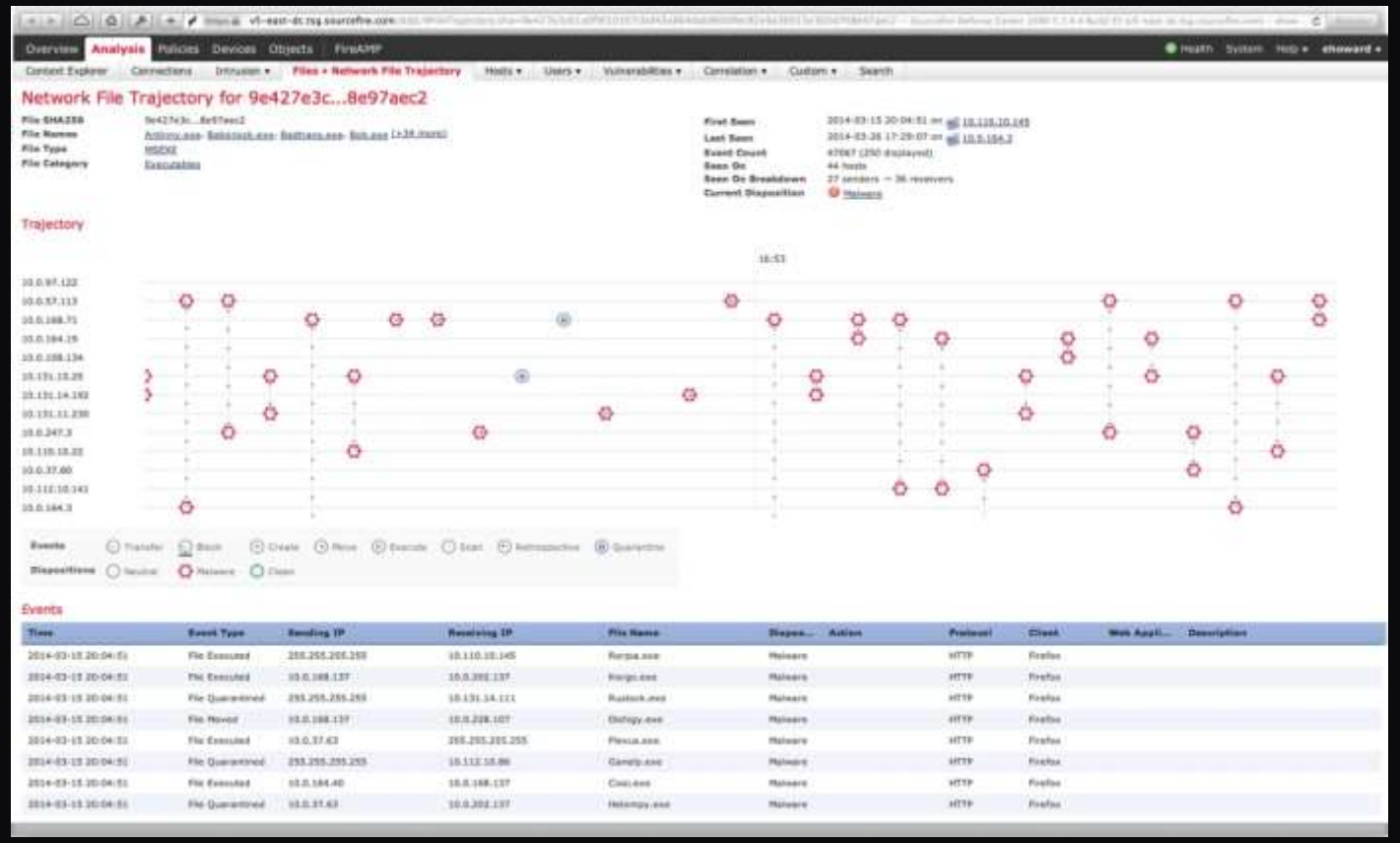
Continuous Analysis

File Trajectory

- Lets you determine scope by tracking malware in motion and activity
- Visibility across organization, centering on a given file

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 transfer protocols were used?

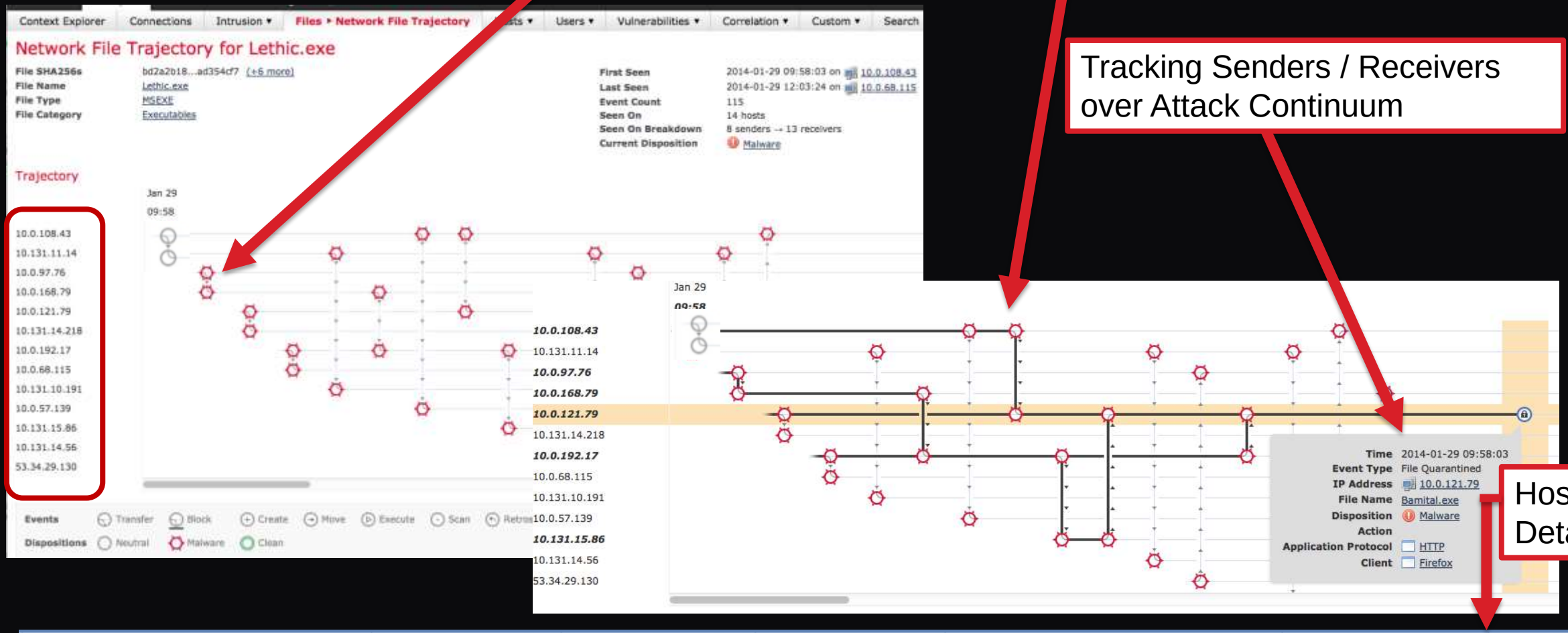


Network File Trajectory – Tracking

File Disposition Change to MALWARE

History of the File as it spreads

Tracking Senders / Receivers over Attack Continuum



Host Details

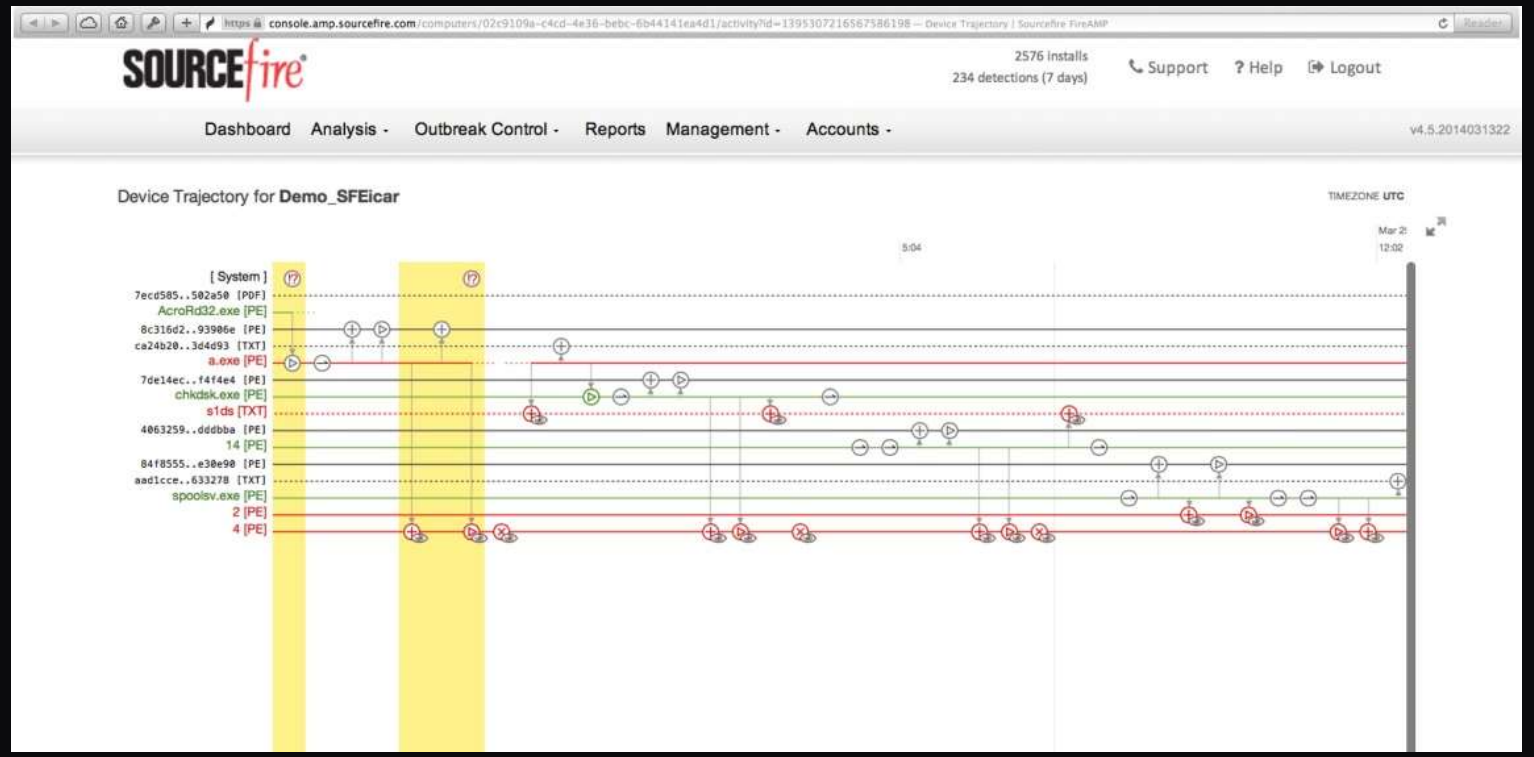
User	Current IP	First Name	Last Name	E-Mail	Department	Phone
Sunil Koduri (skoduri, LDAP)	10.0.108.43	Sunil	Koduri	SKoduri@demo.sourcefire.com	Finance	425-707-9530

Device Trajectory - FireAMP

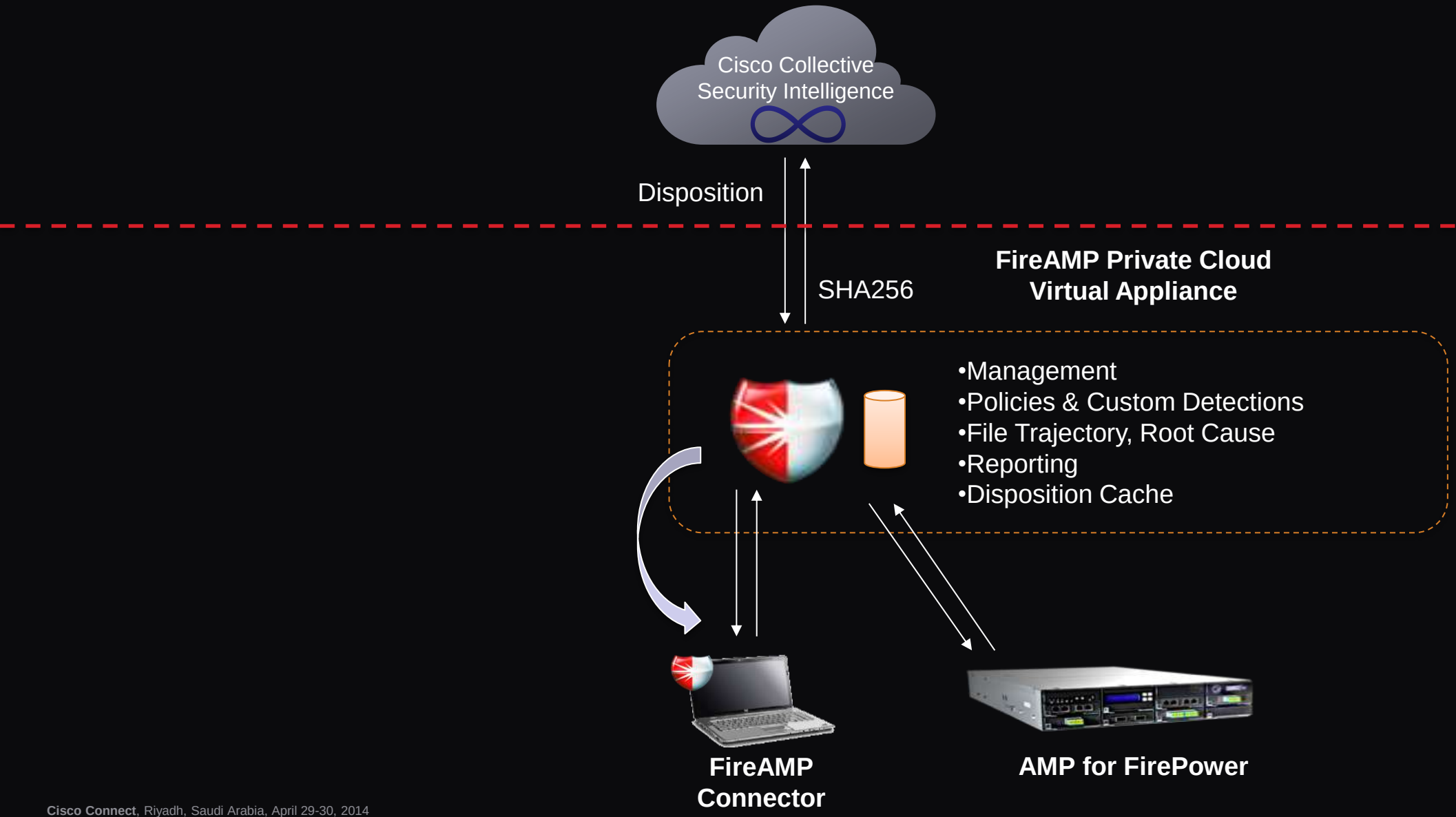
- Gives you deep visibility into file activity on a single device/endpoint

Looks DEEP into a device and helps answer:

- How did the threat get onto the system?
- How bad is my infection on a given device?
- What communications were made?
- What don't I know?
- What is the chain of events?



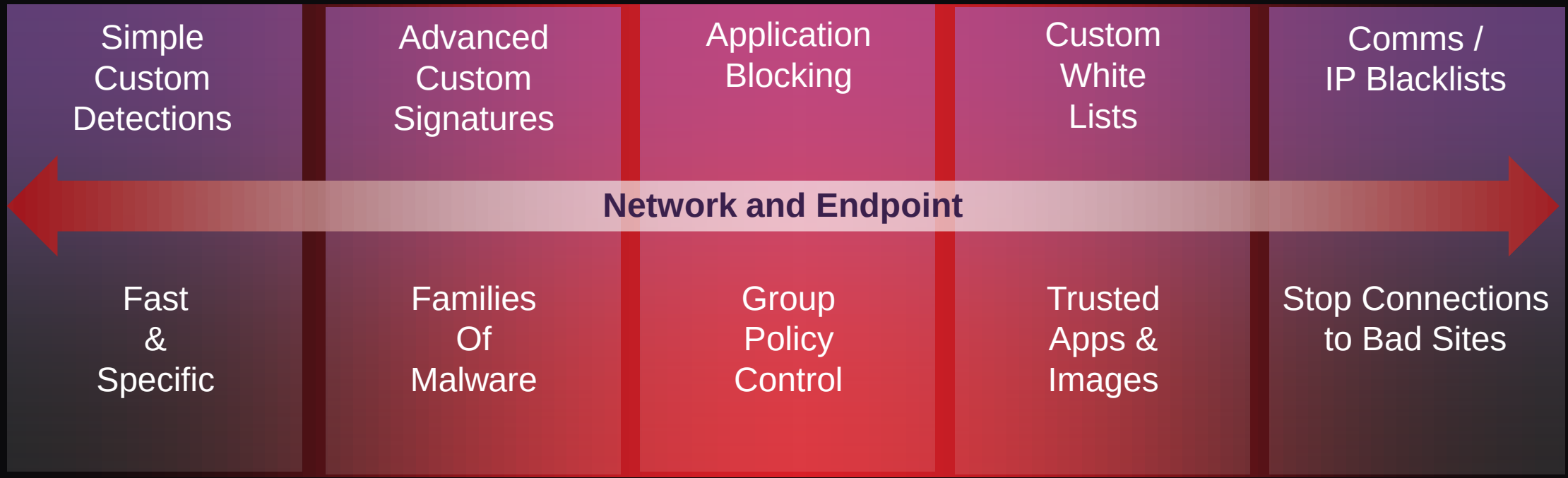
FireAMP Private Cloud: Maintains Customers' Privacy



Outbreak Control – Stop Malware Spread

No more waiting - stop threats and eliminate root causes

- Simple and specific controls
- Context rich signatures for broader control



2014 NSS Labs SVM for Breach Detection Systems

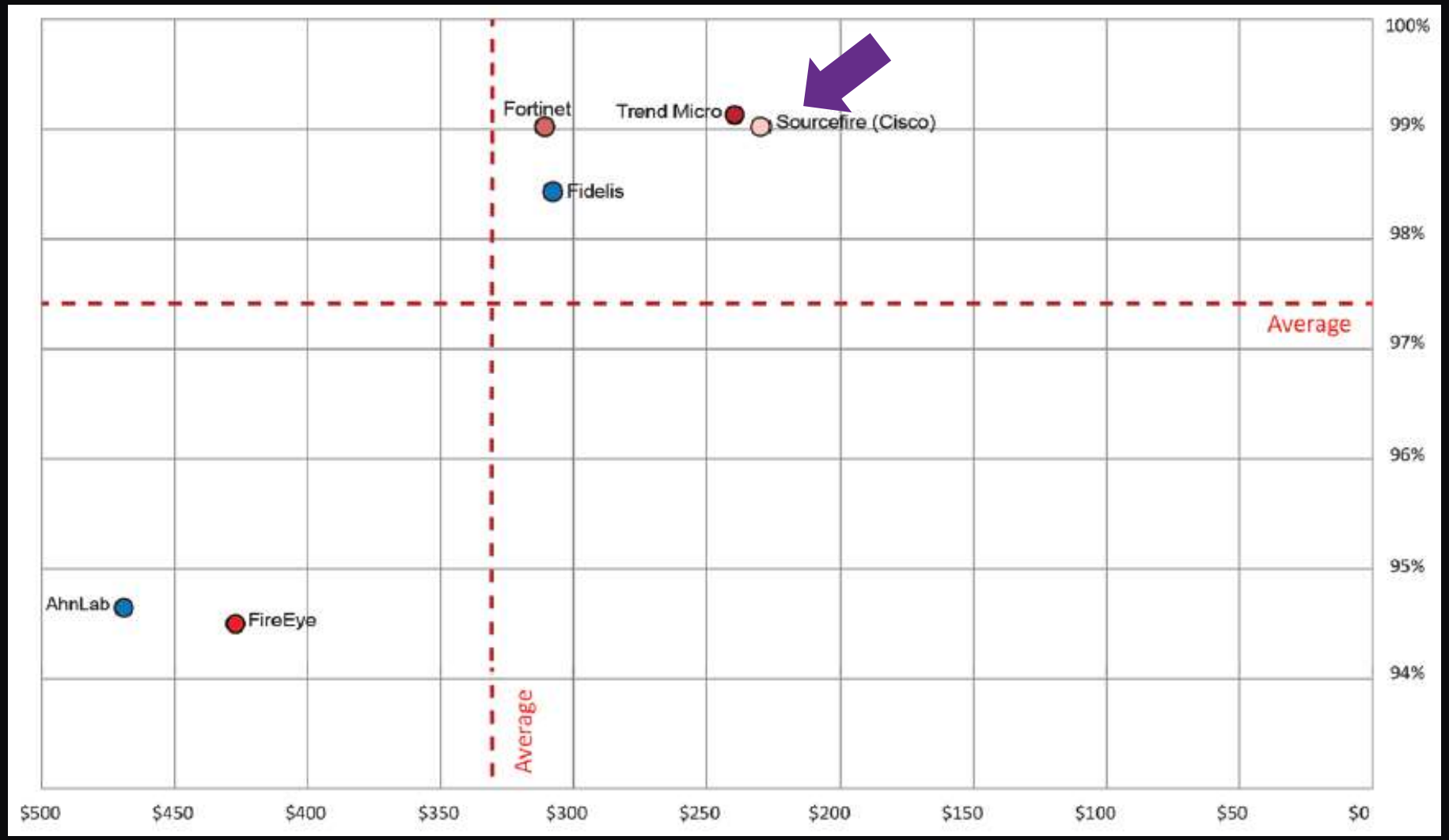
Cisco Advanced Malware Protection

Best Protection Value

99.0% Breach Detection Rating

Lowest TCO per Protected-Mbps

NSS Labs Security Value Map (SVM) for Breach Detection Systems




FirePOWER Platforms

Platforms and Places in the Network

From 50Mbps to 60Gbps
Modularity in 8000 Series
Fixed Connectivity in 7000 Series
Mixed SFPs in 7100 Series
Configuration Fail-Open & Fail-Close across all
Scalable 8000 Series
Runs NGIPS, AMP and App Control in the same chassis

IPS Performance and Scalability

FirePOWER 7000 Series
50 Mbps – 250 Mbps

FirePOWER 7100 Series
500 Mbps – 1 Gbps

FirePOWER 7120/7125/8120
1 Gbps - 2 Gbps

FirePOWER 8100/8200
2 Gbps - 10 Gbps

FirePOWER 8200 Series
10 Gbps – 40 Gbps

SOHO | **Branch Office** | **Internet Edge** | **Campus** | **Data Center**

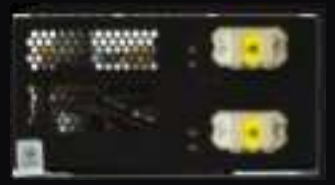
8000 Series Network Modules: Configurable-Bypass

Cluster Module

Used to connect an 3D8140, 3D8250, 8260, 8270, and 8290 to one or more stacking kits. Included in stacking kits.

40G Switch Module

Switch module for 8250/8260 that supports the 40G Fiber network module. Comes standard on 8270/8290.



1G Copper	1G Fiber	10G Fiber	40G Fiber
1 slot	1 slot	1 slot	2 slots
4 Port 1Gbps Copper	4 Port 1Gbps SX Fiber	2 Port SR or LR Fiber	2 Port 40GBASE-SR4

All interfaces are programmable bypass/fail-open and field replaceable.

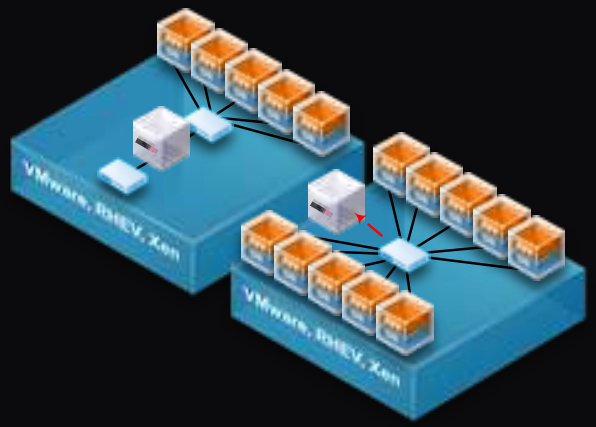
Defense Center Models

Centralized Command & Control

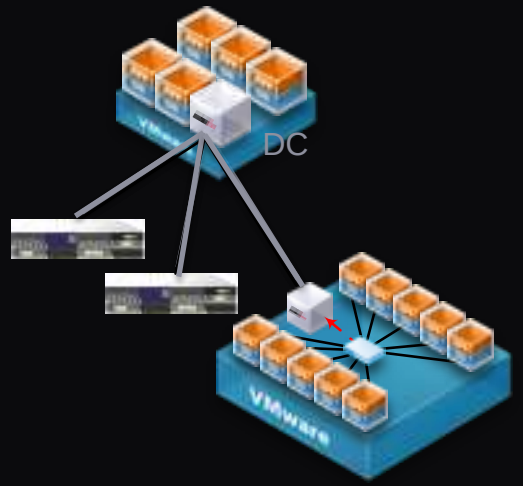
	DC750	DC1500	DC3500
Max. Devices Managed*	10	35	150
Max. IPS Events	20M	30M	150M
Event Storage	100 GB	125 GB	400 GB
Max. Network Map (hosts | users)	2k | 2k	50k | 50k	300k | 300k
Max. Flow Rate (flows/second)	2000 fps	6000 fps	10000 fps
High Availability Features	Lights-out Management (LOM)	RAID 1, LOM, High Availability pairing (HA)	RAID 5, LOM, HA, Redundant AC Power

* Max number of devices is dependent upon sensor type and event rate

Network Virtual Appliances



- Virtual 3D Device
  - Inline or passive deployment
  - Full NGIPS Capabilities
  - Deployed as virtual appliance
  - Use Cases
    - SNORT Conversion
    - Small / Remote Sites
    - Virtual Environment Protection

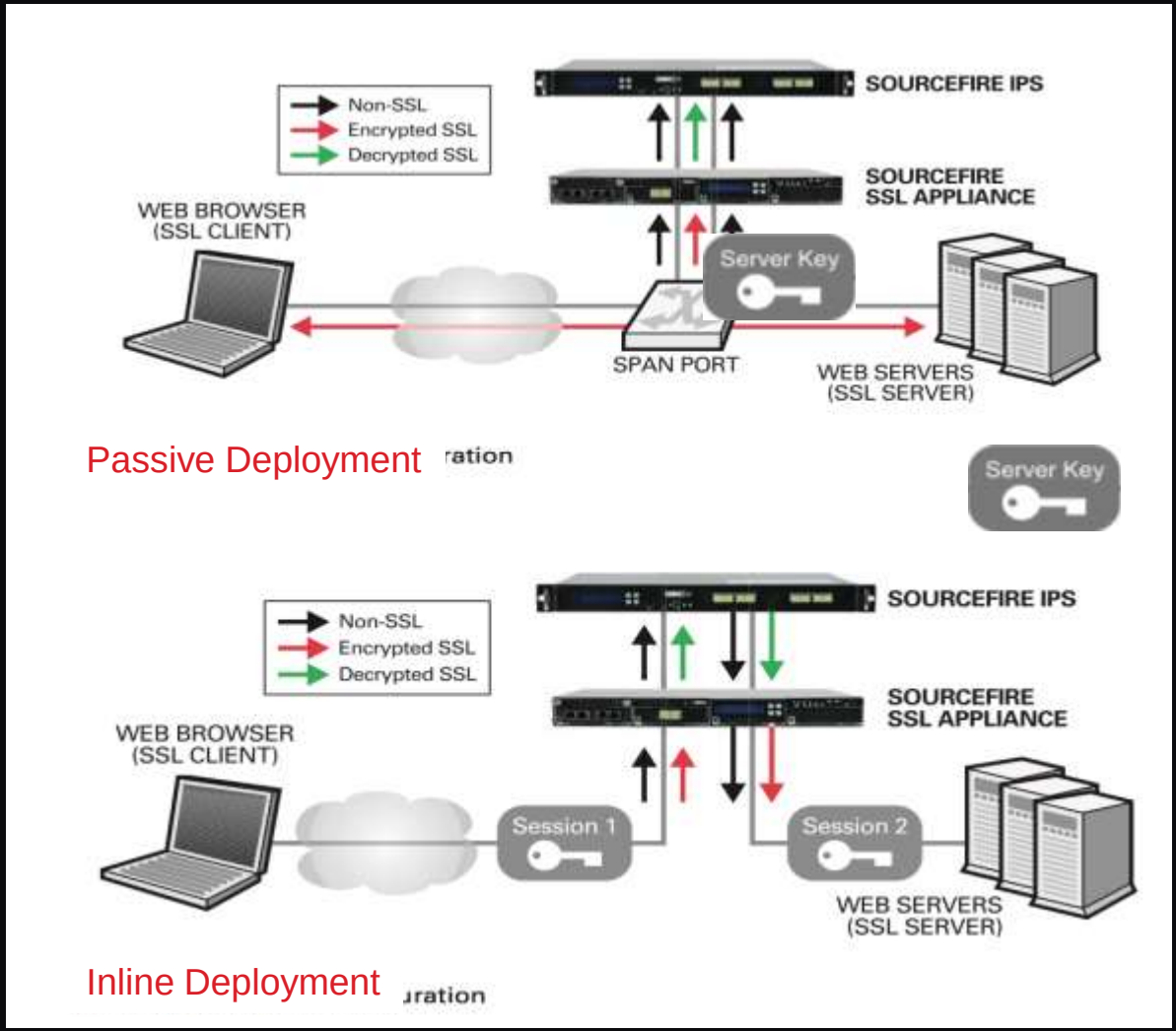


- Virtual Defense Center
  - Manages up to 25 sensors
    - physical and virtual
    - single pane-of-glass
  - Use Cases
    - Rapid Evaluation
    - Pre-production Testing
    - Service Providers

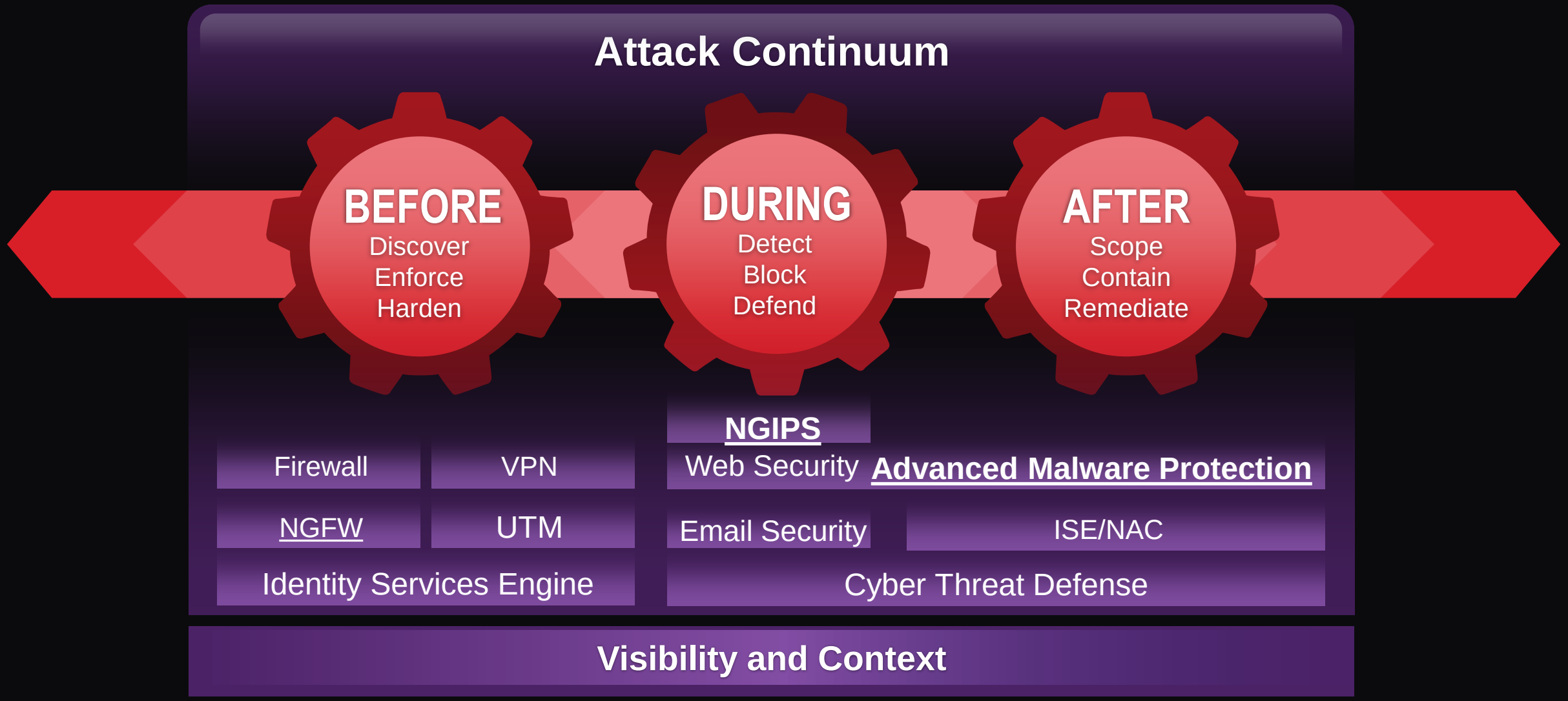
NOTE: Supports ESX(i) 4.x and 5.x on Sourcefire 5.x platforms

SSL Appliance for SSL Inspection

- "Known-server key" for SSL
  - Requires access to the server key
  - Decrypts inbound SSL communication
- "Certificate resign" for SSL
  - Requires Intermediate certificate in browsers
  - Decrypts outbound SSL communication
- Only Physical Appliance
- Cut-through non-SSL traffic



Cisco Sourcefire System in the Attack Continuum




CISCO
TM