
TOMORROW
starts here.
CISCO
Cisco live!

Introduction to the Cisco Sourcefire NGIPS

BRKSEC-1030

Gary Spiteri

Consulting Security Engineer

#clmel

Cisco live!

Are you a laugher or a liar?

Problems with Traditional IPS Technology

- Overwhelms you with irrelevant events
- Doesn't give you much information to go on
- Requires you to spend months tuning
- "Black box" – difficult to determine whether it works
- False sense of Security – that an IPS is your "Silver Bullet"

- Result:
  - IPS is minimally effective or isn't used
  - Massive amounts of time and resources spent making IPS work
  - Organisations exploited

Getting Effectiveness out of an IPS

- Identifying the “needle in the haystack” – the attacks and hosts that really matter
- Giving you contextual information about the **who, what, where, why, and when** of a critical attack
- Giving you confidence that attacks are fully covered

- Session Result:
  - Gain an understanding of how Cisco’s Sourcefire products apply to these problems
  - Get an overview about how the Sourcefire NGIPS works

Agenda

- The Problems with Traditional IPS
- What's a New Generation IPS?
- The Sourcefire and Snort Legacy
- The FirePOWER Next Generation IPS
- Going beyond Next Generation with Cisco

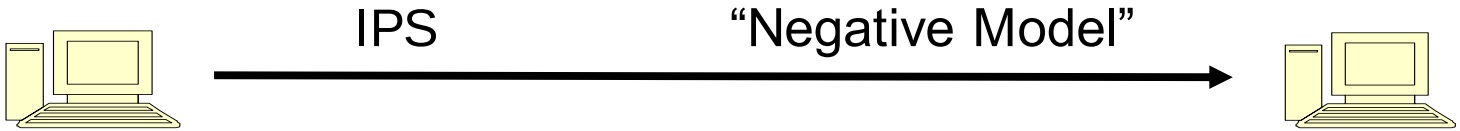
IPS Overview and Background

What is an IPS?

- Intrusion Prevention System
  - Monitors networks for malicious or suspicious behaviour
  - Blocks attacks and/or sends alerts in real time
- Evolved from:
  - Intrusion Detection System (IDS) – Can monitor but not block attacks
- Today, we use “IPS” generically
  - Inline blocking mode = IPS
  - Passive detecting mode = IDS

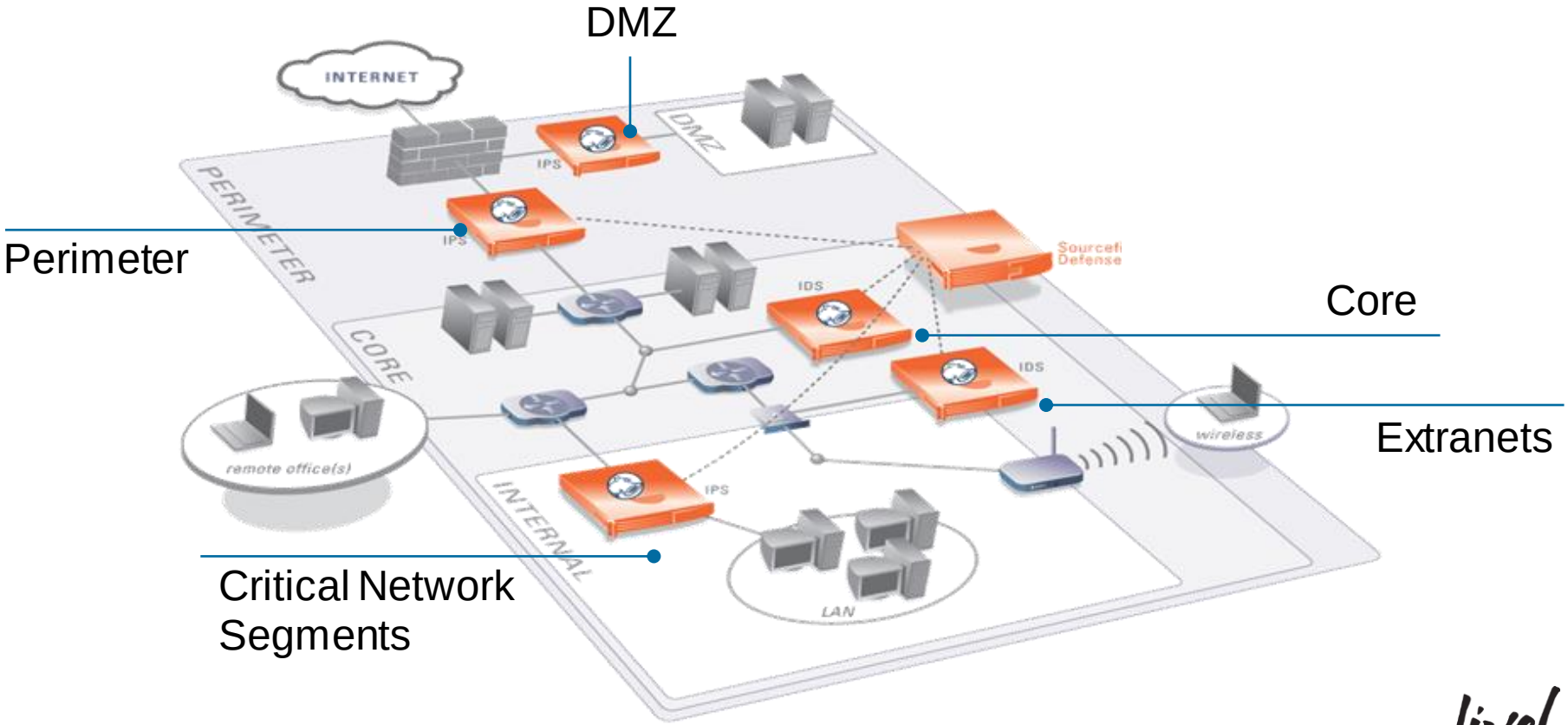
Traditional IPS and Firewall Models

Controls what traffic types/paths are permitted.



Detects/blocks malicious traffic within allowed paths.

Deployment Locations for an IPS



Typical IPS Deployment Locations

- Perimeter
  - Blocks/monitors attacks incoming from external machines
  - Behind or integrated with a firewall
- DMZ
  - Demilitarised zone – partly trusted area where web servers live
  - Risk of compromising web and/or database servers
- Core
  - Detects attacks from inside the organisation
  - Good for worms and insider attacks
- Extranets
  - Extranets provide connectivity to partners, suppliers, customers
  - Often have carry risks of access to sensitive info
- Critical Network Segments
  - Highly sensitive network segments
  - Example: eCommerce systems affected by PCI regulation

Ways to Deploy an IPS

- **Inline** – blocking and/or monitoring
  - Between two devices
    - Switch and firewall
    - Router and a switch
  - Uses 2 ports on the IPS – an inline pair
  - Appliances may provide fail-open and fail-over capabilities for situations when:
    - Sensor loses power
    - Sensor suffers software failure
    - Sensor intentionally shut down

- **Passive** – monitoring only
  - Off a switch's SPAN port
    - Special switch port that can mirror traffic from one or more ports
  - Off a network tap
    - Device that allows you to monitor a single segment without interrupting traffic flow
  - Uses 1 port on the IPS

Vulnerabilities vs. Exploits

- **Vulnerability**: Weakness in a system that allows an attacker to exploit it
  - Example: Microsoft Tuesday – On the second Tuesday of every month, Microsoft announces vulnerabilities and releases patches for them.
  - We are a member of MAPP – Microsoft Active Protections Program
- **Exploit**: Specific attack against a vulnerability
- There are many potential exploits for each vulnerability
- Traditional IPS signatures often look for exploits rather than the full triggering conditions of vulnerabilities

Problems with Traditional IPS Technology

- Overwhelms you with irrelevant events
- Doesn't give you much information to go on
- Requires you to spend months tuning
- "Black box" – difficult to determine whether it works

- Result:
  - IPS is minimally effective or isn't used
  - Massive amounts of time and resources spent making IPS work
  - Organisations exploited

About Sourcefire and Snort

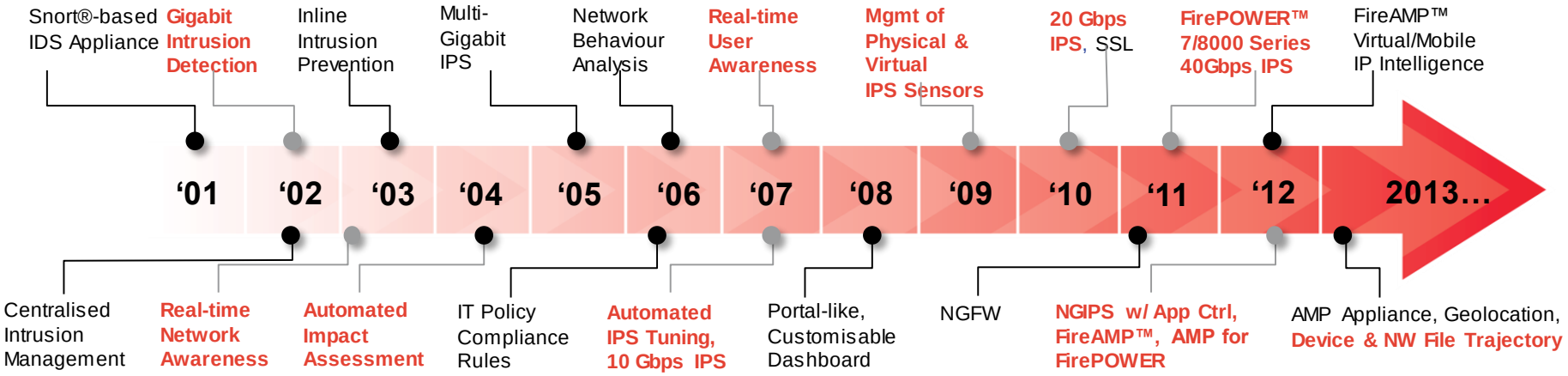
About Sourcefire

- Founded in 2001, acquired by Cisco in 2013
- Security from Cloud to Core
  - Market leader in (NG)IPS
  - New entrant to NGFW space with strong offering
  - Groundbreaking Advanced Malware Protection solution
- Pioneer in IPS, context-driven security, advanced malware
- World-class research capability
- Owner of major Open Source security projects
  - Snort, ClamAV, Razorback

Sourcefire

Culture of Innovation

Major innovations indicated in red



52 Patents Awarded or Pending

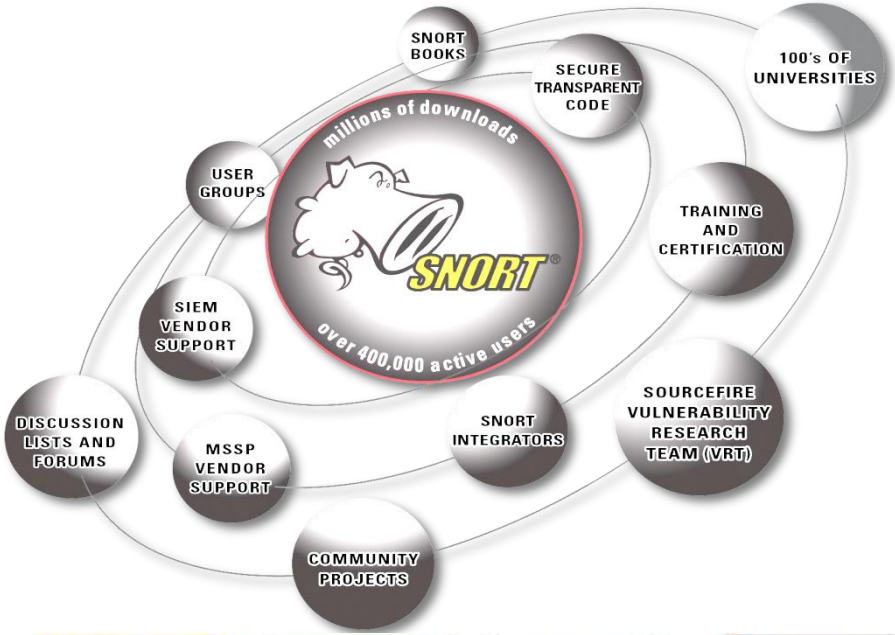
World-Class Vulnerability Research Team (VRT)

“Sourcefire is the best in the business. Having Sourcefire NGIPS on the network is like having the mind of Martin Roesch in the building and that's a good thing.”

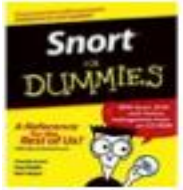
Chief Security Officer

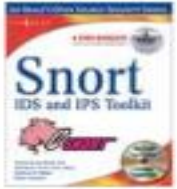
Fortune 100

Open Source Snort®



- First created by Martin Roesch in 1998
- Global standard for Intrusion Detection and Prevention
- World's largest threat response community
- Interoperable with other security products
- Owned and controlled by Sourcefire/Cisco
- www.snort.org



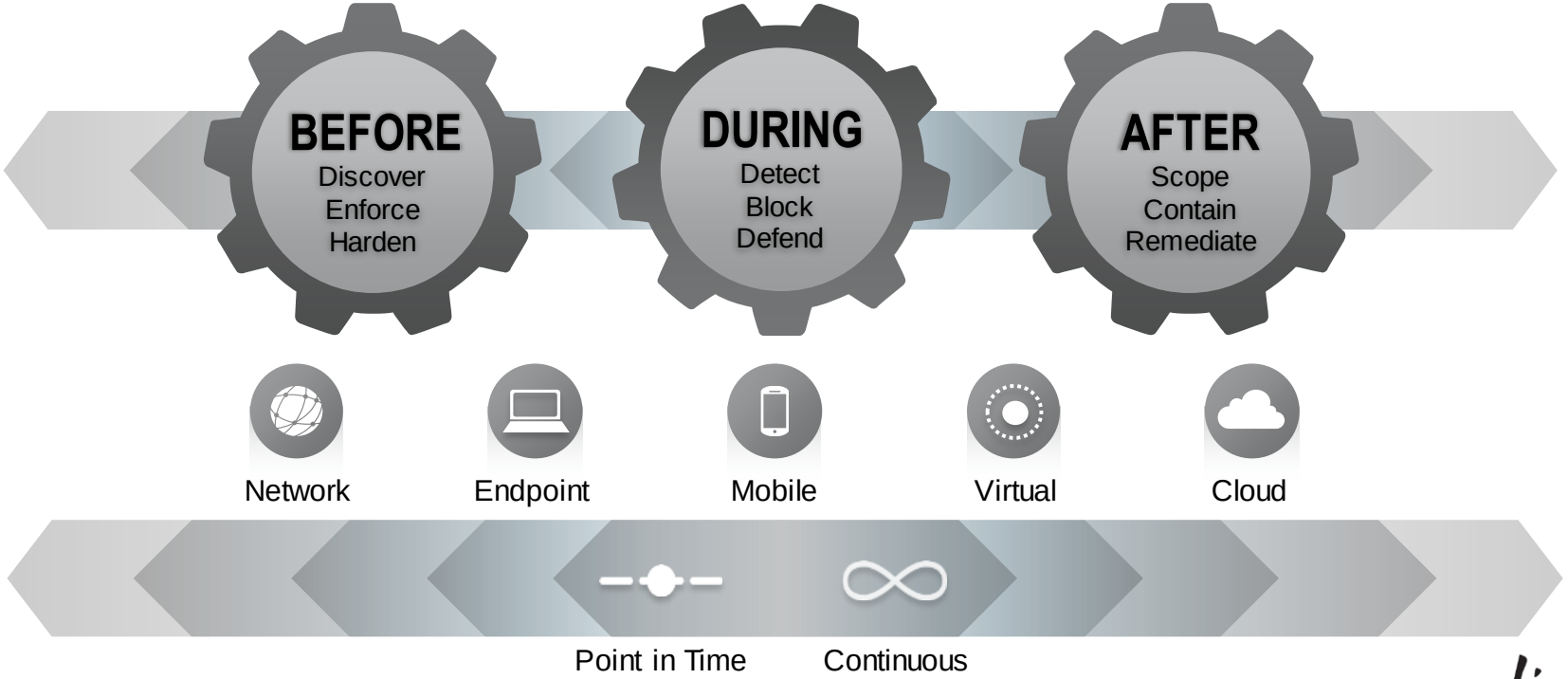


Open Source Philosophy and Benefits

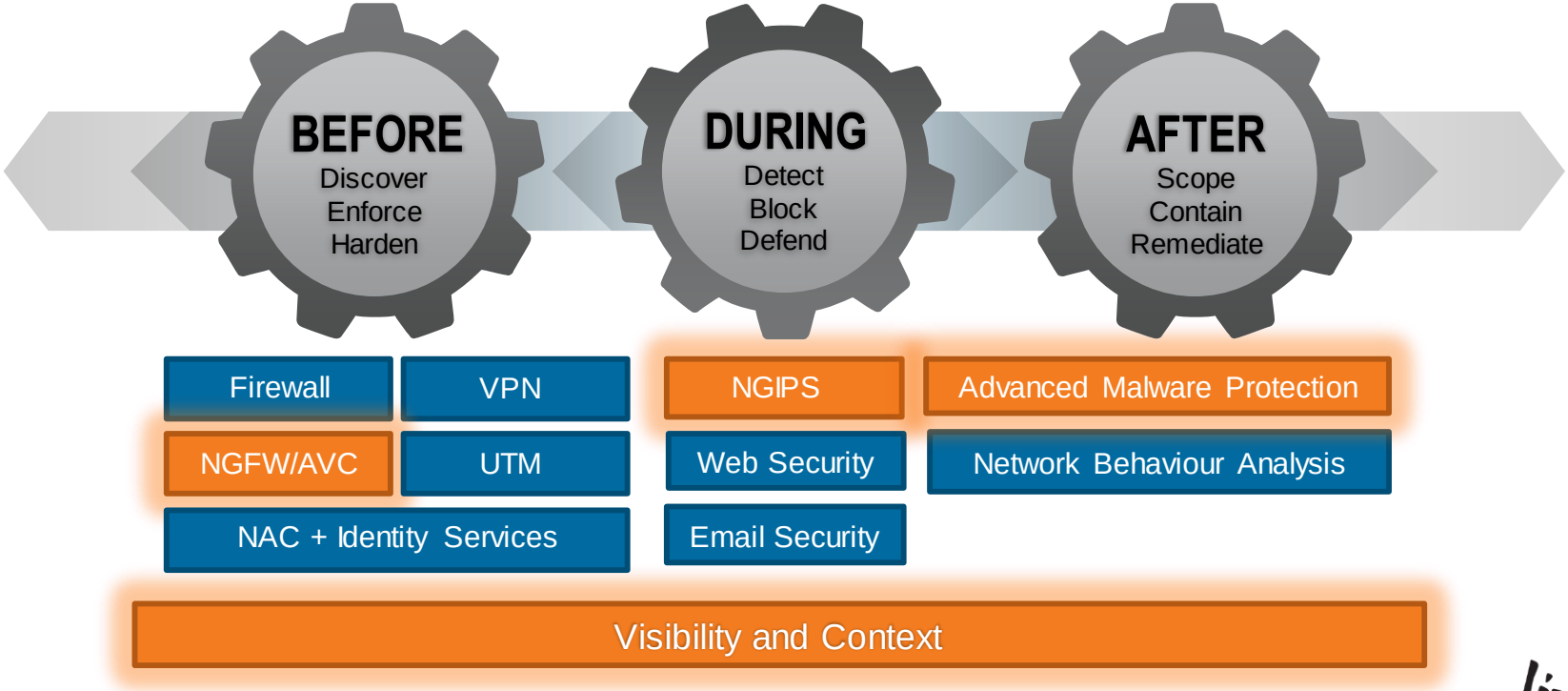
- About Building Great Software
  - In a Collaborative Manner
  - With the User Community
- About Building Trust
  - Legacy of Success (Linux, Apache, Snort)
  - Robustness of Community
  - No 'Black Box' Functionality
  - Weaknesses Exposed and Corrected

Community	Collaboration	Trust
Engage with users and developers to strengthen their solutions	Build with the community to solve complex security problems	Demonstrate technical excellence, trustworthiness and thought leadership

The Attack Continuum



Mapping Technologies to the Attack Continuum



The Cisco/Sourcefire Offering

Cisco/Sourcefire Security Solutions

FireSIGHT™ Management Centre

APPLIANCES | VIRTUAL

NEXT-GENERATION INTRUSION PREVENTION

APPLICATION CONTROL

ADVANCED MALWARE PROTECTION

COLLECTIVE SECURITY INTELLIGENCE

FireAMP™

HOSTS | VIRTUAL
MOBILE

CONTEXTUAL AWARENESS

FirePOWER™ Appliances

APPLIANCES | VIRTUAL

FirePOWER™ Appliances

- Industry-best
  Intrusion Prevention
- Real-time
  Contextual Awareness
- Full Stack Visibility
- Intelligent Security Automation with FireSIGHT™
- Unparalleled Performance and Scalability
- Easily add Application Control, URL Filtering and Advanced Malware Protection with optional subscription licenses

FirePOWER™ Appliances

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

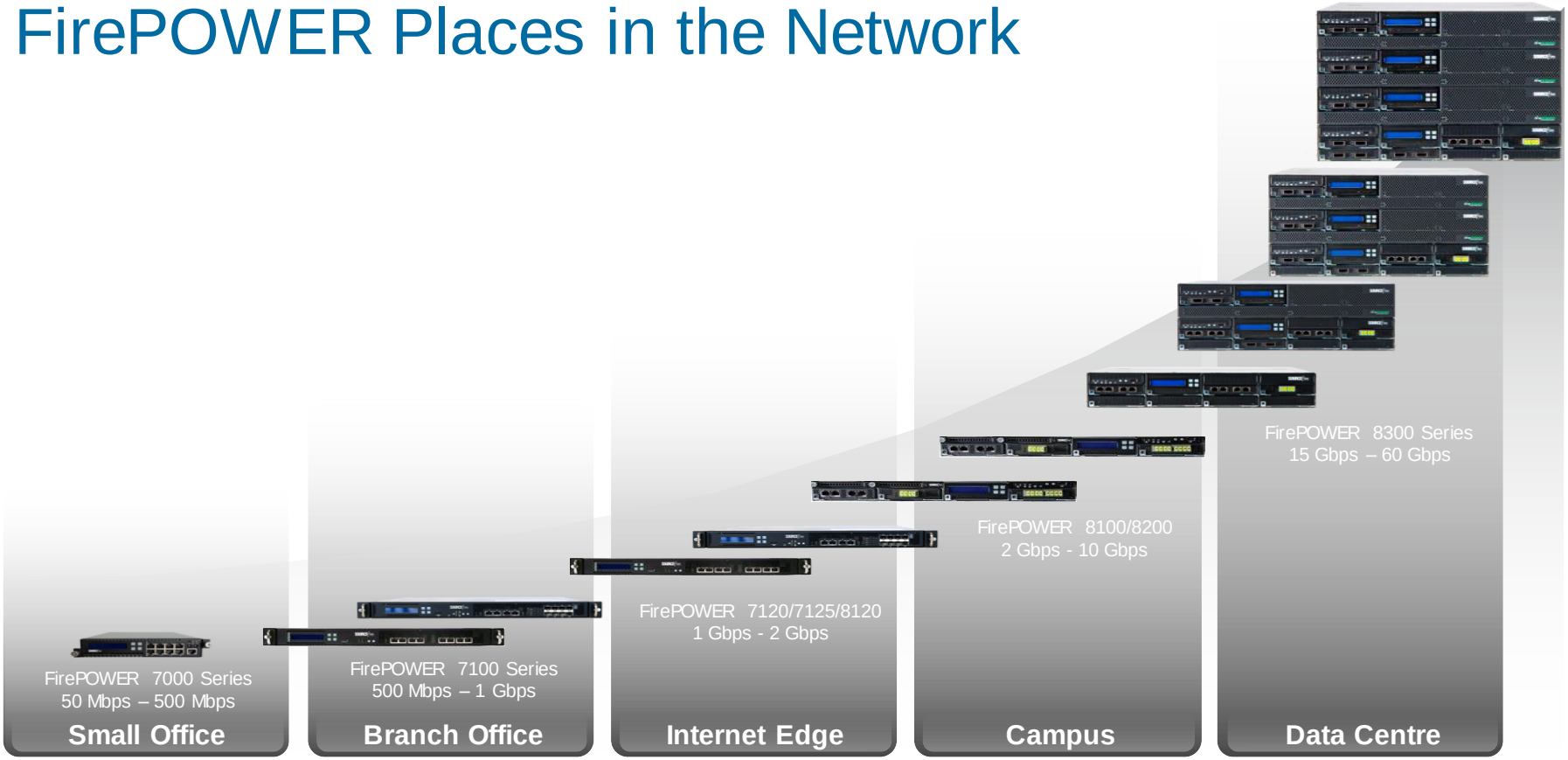
Hardware Acceleration
For best in class throughput, security, Rack size/Mbps, and price/Mbps

Lights Out Management
For minimal operational impact

Solid State Drive
For increased reliability

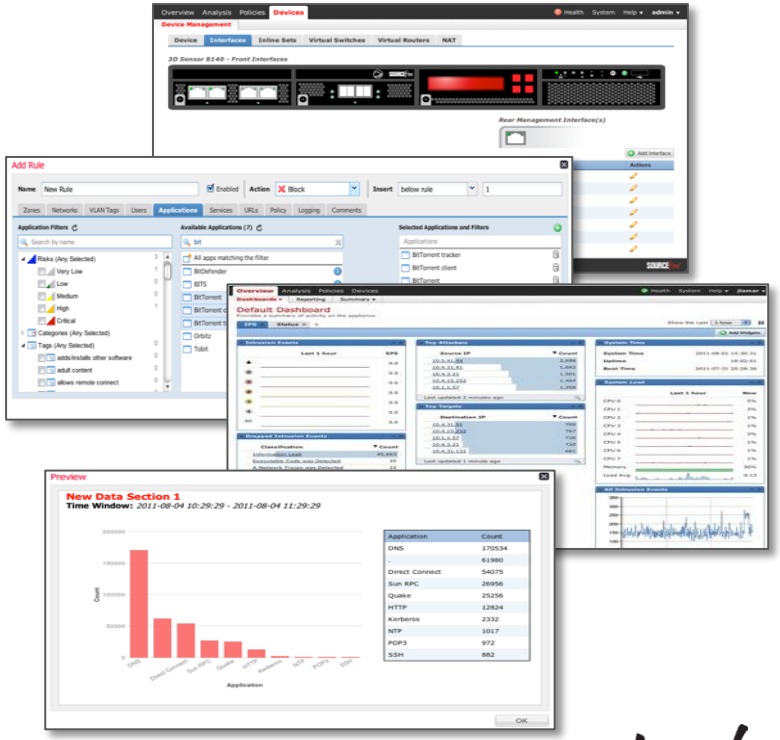
FirePOWER Places in the Network

IPS Performance and Scalability



FireSIGHT Management Centre

Single console for event, policy, and configuration management



- Centralised analysis and management
- Customisable dashboard
- Comprehensive reports & alerts
- Centralised policy administration
- High availability
- Integrates with existing security

FireSIGHT™ Management Centre: Dashboard

Overview | Analysis | Policies | Devices | Objects | FireAMP | Health | System | Help | jolaughlin

Dashboards | Reporting | Summary | Report Designer

Security Awareness Dashboard (JRS)

Detailed Dashboard (Javed)

Malware | Files | Threat Summary | Flows | Applications | Traffic | GeoDB | Intrusions | User Activity | URL Activity | Firesight | Show the Last 1 hour | Add Widgets

Intrusion Events

	Last 1 hour	Total
		662
1		23
2		227
3		405
All		662

Security Events by Destination IP

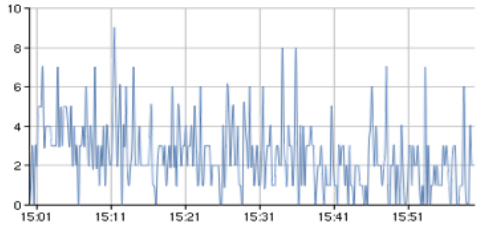
	Destination IP	Count
	10.131.11.127	7
+3	10.131.12.13	6
	131.75.28.98	6
	172.16.0.107	4
	10.131.10.254	3

Last updated 9 minutes ago

Impact Level 1 Events by Application

	Username	Impact Level 1 Events
+1	abdul.joyner (abdul.joyner, LDAP)	1
+1	marianna.lyon (marianna.lyon, LDAP)	1
+1	mayra.atkinson (mayra.atkinson, LDAP)	1
+1	meagan.velez (meagan.velez, LDAP)	1
	mittie.jarrett (mittie.jarrett, LDAP)	1

All Intrusion Events



Last updated 9 minutes ago

Impact Level 1 Events by Application

Application	Impact Level 1 Events
HTTP	22
Web browser	22
generic audio/video	8
MySQL	1
MySQL client	1

Last updated 9 minutes ago

Total Events by User

	Username	Total Events
	lucio.david (lucio.david, LDAP)	12
-1	adelaida.blount (adelaida.blount, LDAP)	10
+2	liliana.reilly (liliana.reilly, LDAP)	10

All Intrusion Events (Not Dropped)

	Message	Count
	INDICATOR-SHELLCODE x86 OS agnostic fnstenv geteip dword xor	33
	PROTOCOL-TFTP GET filename overflow attempt (1:1941)	31
	SERVER-OTHER Wireshark LWRES Dissector getaddrsbyname buffer	22
	SERVER-MAIL Microsoft Windows Exchange MODPROPS denial of service	21
	PROTOCOL-IMAP CRAM-MD5 authentication method buffer overflow	19
	PROTOCOL-IMAP CRAM-MD5 authentication method buffer overflow	19
+4	WEB-CLIENT obfuscated header in PDF (3:16343)	19
+2	FILE-MULTIMEDIA VideoLAN VLC Media Player TY processing buffer	18
+2	SERVER-WEBAPP OpenView Network Node Manager cookie buffer	17
+2	SERVER-WEBAPP HP OpenView Network Node Manager OvOSLocale	17
+2	OS-WINDOWS DCERPC Messenger Service buffer overflow attempt	14
-4	INDICATOR-SHELLCODE x86 fldz get eip shellcode (1:14986)	13
-3	EXPLOIT dhclient subnet mask option buffer overflow attempt	13
-2	SERVER-OTHER McAfee ePolicy Orchestrator Framework Services log	13
-3	INDICATOR-SHELLCODE x86 OS agnostic alpha numeric upper case	12
	BROWSER-IE Microsoft Internet Explorer marquee object handling	11
	FILE-OFFICE Microsoft Office Outlook SMB attach by reference code	11
	BROWSER-IE Microsoft Internet Explorer oversize recordset object	11
-7	SERVER-OTHER ISC BIND RRSIG query denial of service attempt	11
	SERVER-WEBAPP HP OpenView Performance Insight Server backdoor	10

Last updated 5 minutes ago

Total Events by Application

Application	Total Events
HTTP	678
Web browser	626

FireSIGHT™ Management Centre: Policies

Overview | Analysis | **Policies** | Devices | Health | System | Help ▾ | jlamar ▾

Intrusion ▾ | **Access Control** | Network Discovery | Custom Applications | Users | Correlation ▾ | Actions ▾

Interesting Use Cases

Enter a description

Save | Cancel | Save and Apply | Add Category | Add Rule | Search Rules

Device Targets: 0 devices

#	Name	Source Zones	Dest Zones	Sou... Net...	Dest Net...	VLA...	U...	Applications	Services	URLs	Action			
Administrator Rules														
This category is empty.														
Standard Rules														
1	Mobile Security 1	Intern	any	any	Ten	any	any	Android browser Blackberry browser Mobile Safari	any	any	Block		1	
2	Read Only Facebook	Intern	Extern	any	any	any	any	Facebook Status Update Facebook Send Email Facebook Comment Facebook Chat Tags: Facebook game; Fil	any	any	Block		0	
3	Web Block List	Intern	Extern	any	any	any	any	any	any	Adult and Pornography (Any Reputation) Bot Nets (Any Reputation) Confirmed SPAM Sources (Any Reputati Gambling (Any Reputation) (13 more...)	Block		0	
4	Block All P2P	Intern	Extern	any	any	any	any	Categories: peer to peer	any	any	Block		0	
5	Inbound Email	Extern	Intern	any	any	any	any	SMTP	SMTP	any	Allow		0	
6	Outbound Web Browsing	Extern	Intern	any	any	any	any	HTTP	any	any	Allow		0	
Root Rules														
This category is empty.														

Default Action Access Control: Block All Traffic

1 Row Selected | Displaying 1 - 6 of 6 rules | Page 1 of 1

SOURCEfire

FireSIGHT™ Management Centre: Devices

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

Device Management | NAT | VPN

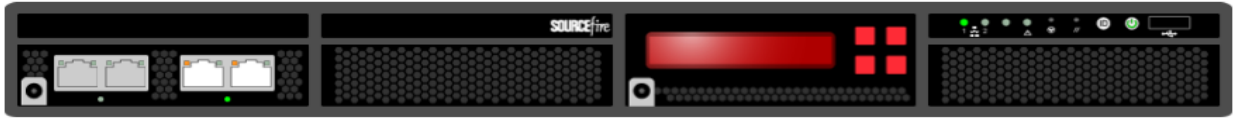
v5-east-3d.tsg.sourcefire.com

3D8140

You have unapplied changes | Apply Changes

Device | Interfaces | Inline Sets | Virtual Switches | Virtual Routers

Add Interface



eth0 (Management)

Link	Name	Type	Security Zone	Used By	MAC Address	IP Addresses	
	eth0	Management			00:1e:67:1f:82:9c		
	s1p1						
	s1p2						
	s1p3	Inline	External	Default Inline Set			
	s1p4	Inline	Internal	Default Inline Set			

FireSIGHT™ Management Centre: Administrators

Overview Analysis Policies Devices Objects FireAMP Health System Help ▾ jolaughlin ▾

Local ▸ User Management Updates Licenses Monitoring ▾ Tools ▾

Users User Roles Login Authentication

Configure Permission Escalation Create User Role

User Role	Enabled	Actions
Access Admin Sourcefire-provided	✓	
Administrator Sourcefire-provided	✓	
Discovery Admin Sourcefire-provided	✓	
External Database User Sourcefire-provided	✓	
Intrusion Admin Sourcefire-provided	✓	
Maintenance User Sourcefire-provided	✓	
Network Admin Sourcefire-provided	✓	
Security Analyst Sourcefire-provided		
Security Analyst (Read Only) Sourcefire-provided		
Security Approver Sourcefire-provided		
Locked Down SE User Role Sourcefire-provided		

Menu-Based Permissions

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

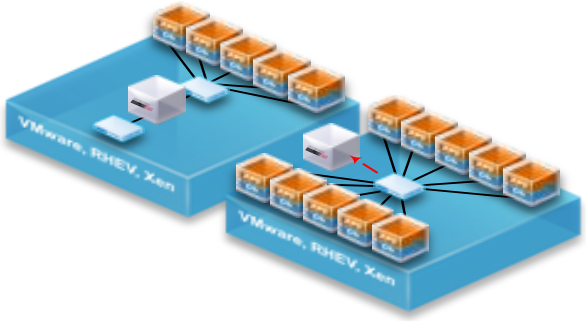
FireSIGHT Management Centre Appliances



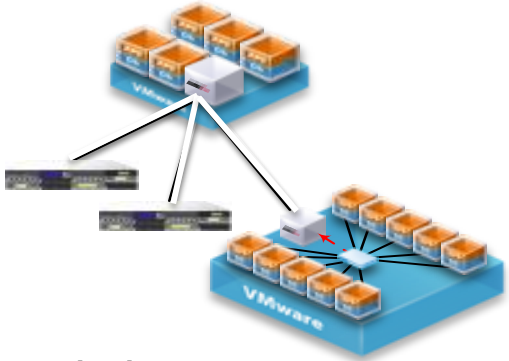
	750	1500	3500
Max. Devices Managed*	10	35	150
Max. IPS Events	20M	30M	150M
Event Storage	100 GB	125 GB	400 GB
Max. Network Map (hosts / users)	2K/2K	50K/50K	300K/300K
Max. Flow Rate	2000 fps	6000 fps	10000 fps

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

Network Virtual Appliances



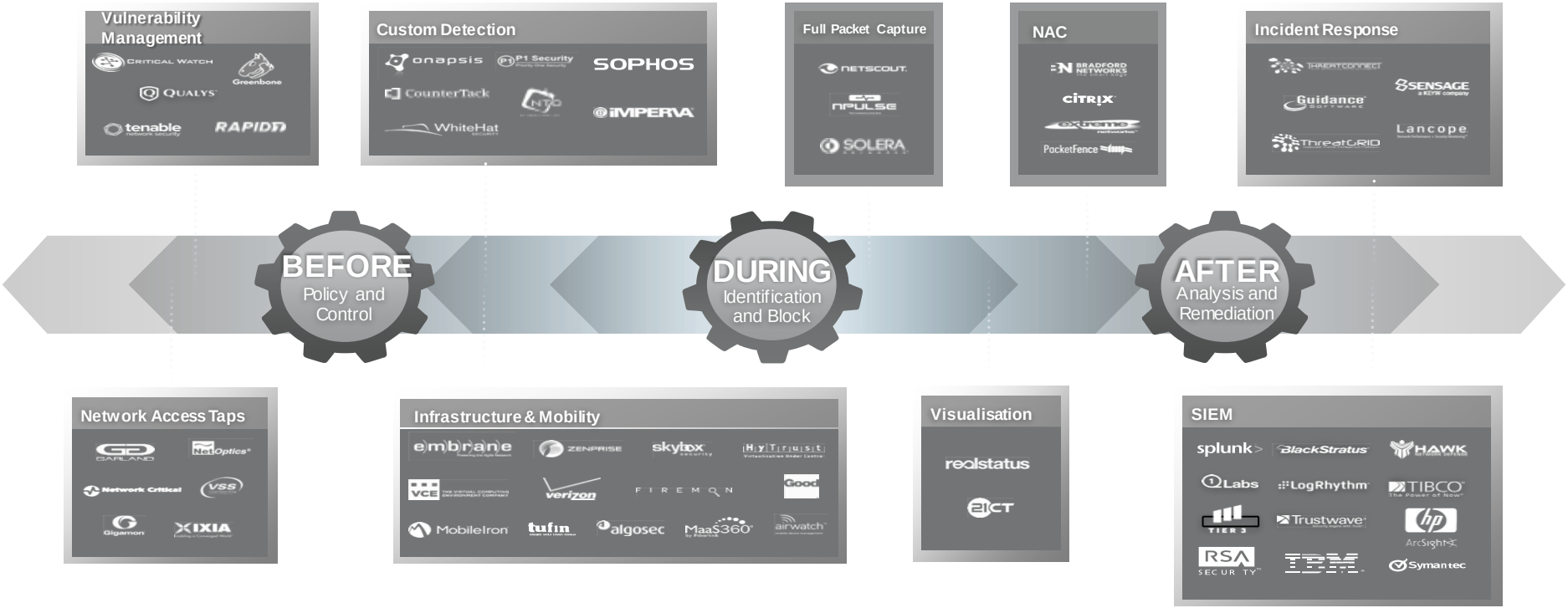
- NGIPSv
  - Inline or passive deployment
  - Full NGIPS Capabilities
  - Deployed as virtual appliance
  - Use Cases
    - SNORT Conversion
    - Small / Remote Sites
    - Virtualised workloads (PCI)



- Virtual FireSIGHT Management Centre
  - 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.

Robust Partner Ecosystem

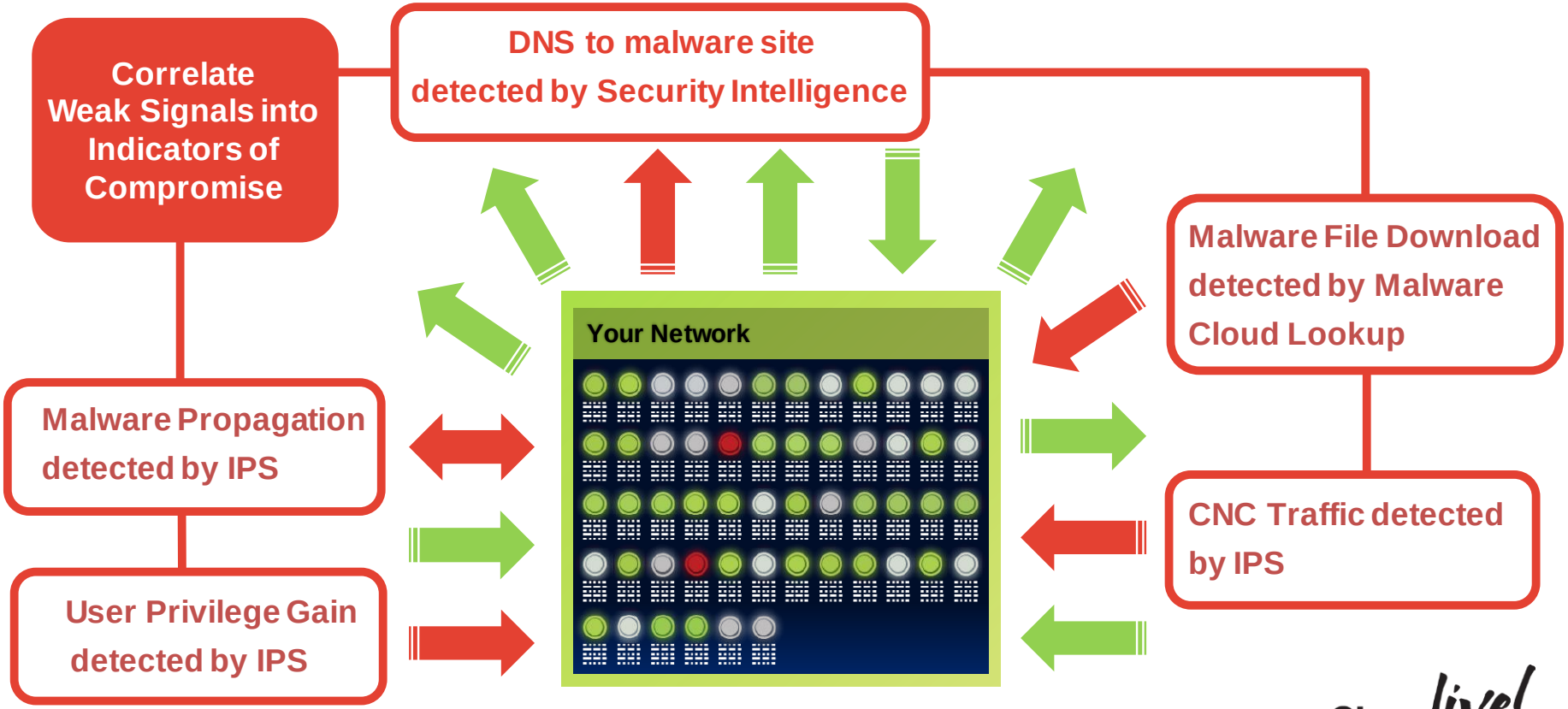


Combined API Framework

FirePOWER Next Generation IPS

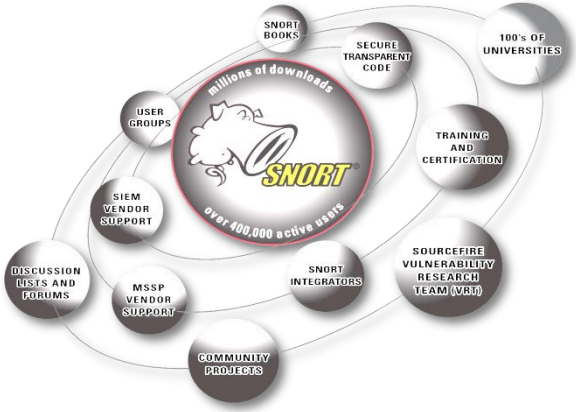
Cisco live!

Correlating Indicators of Compromise

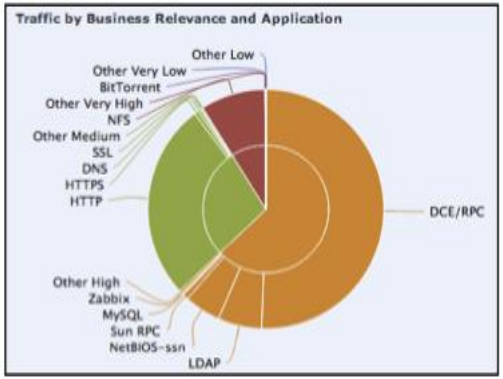


Three Key Sourcefire NGIPS Differentiators

- Trusted Security Engine and Security Intelligence



- Network Awareness and Visibility

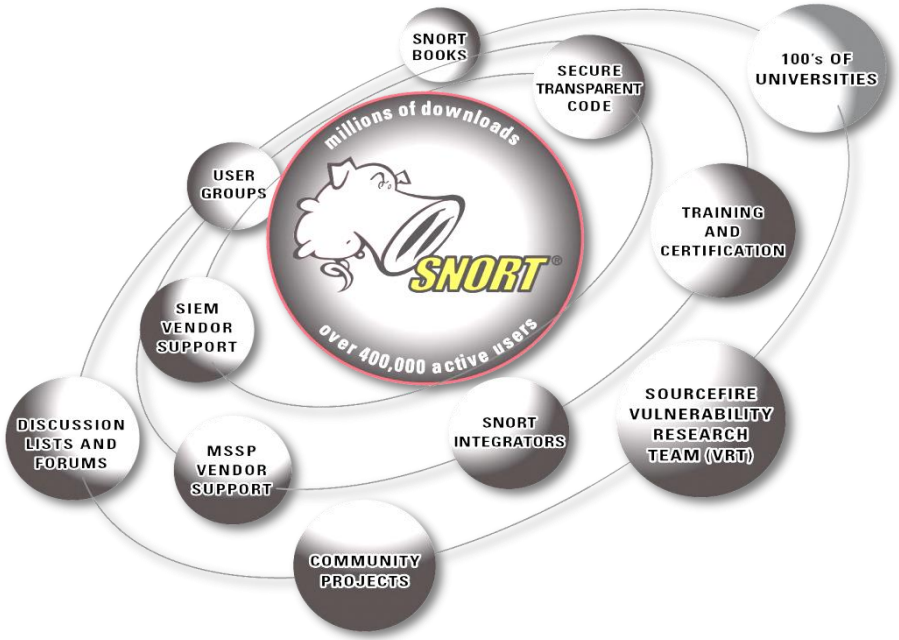


- Security Automation

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

Sourcefire NGIPS Engine

- Engine is Snort, created and developed by Sourcefire/Cisco
- Rules developed by Sourcefire/Cisco Vulnerability Research Team
- Built on collective security intelligence from a variety of sources
- Extremely broad platform and threat coverage
- Rules are open and inspectable
- All packets are logged
- Import and use third-party rules in the industry standard format



Protecting Your Network

Annual Output

2 SEU/SRUs,
1 VDB updates per week

>10 CVEs covered per day

4,310 new IPS rules

>180,000 malware submissions per day

Protecting Your Network

Annual Output

2 SEU/SRUs
1 VDB updates
week

>10 CVEs
vered per day

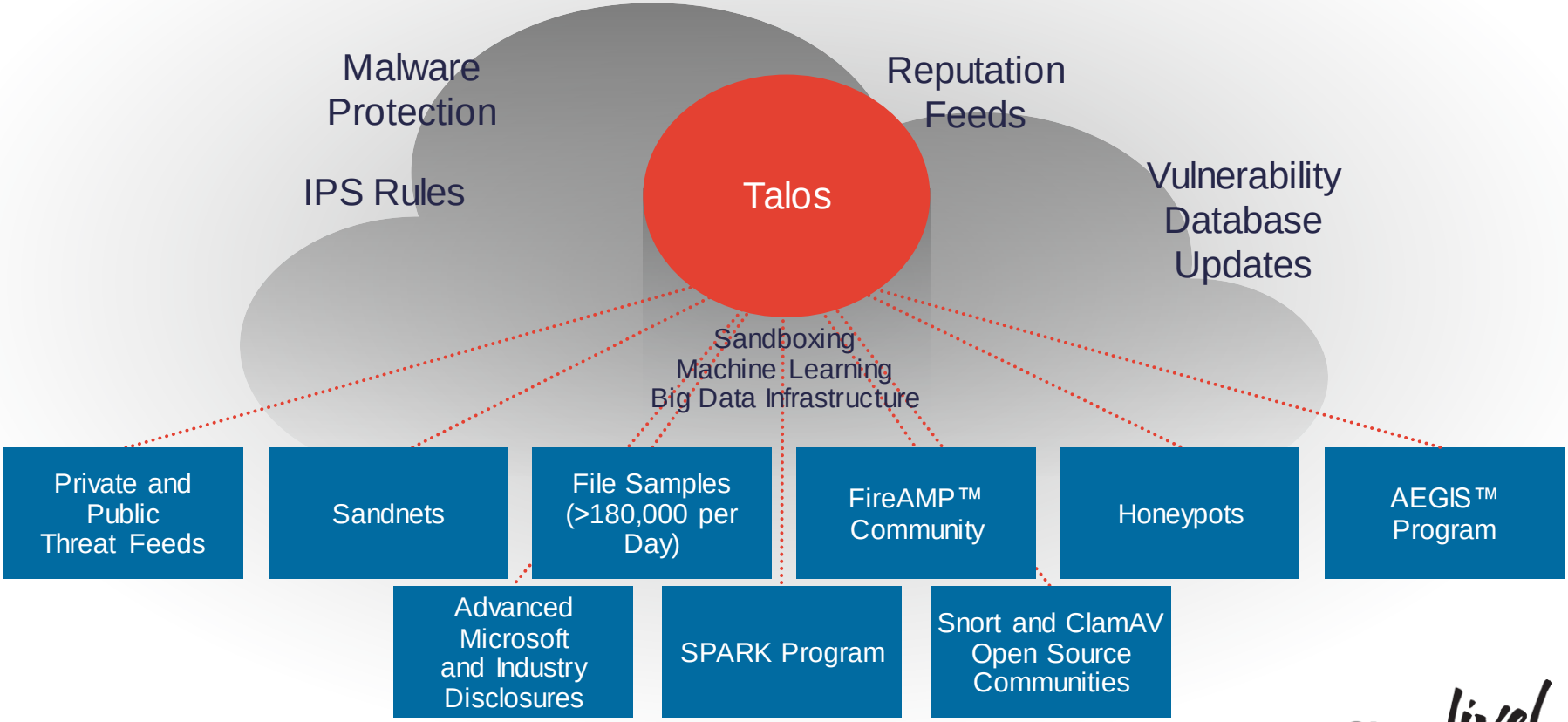
98.9%
Vulnerability
coverage per NSS Labs IPS group test

100%
Same-day
protection for Microsoft vulnerabilities

4,310 new IP
rules

0,000 malware
nissions per day

Collective Security Intelligence



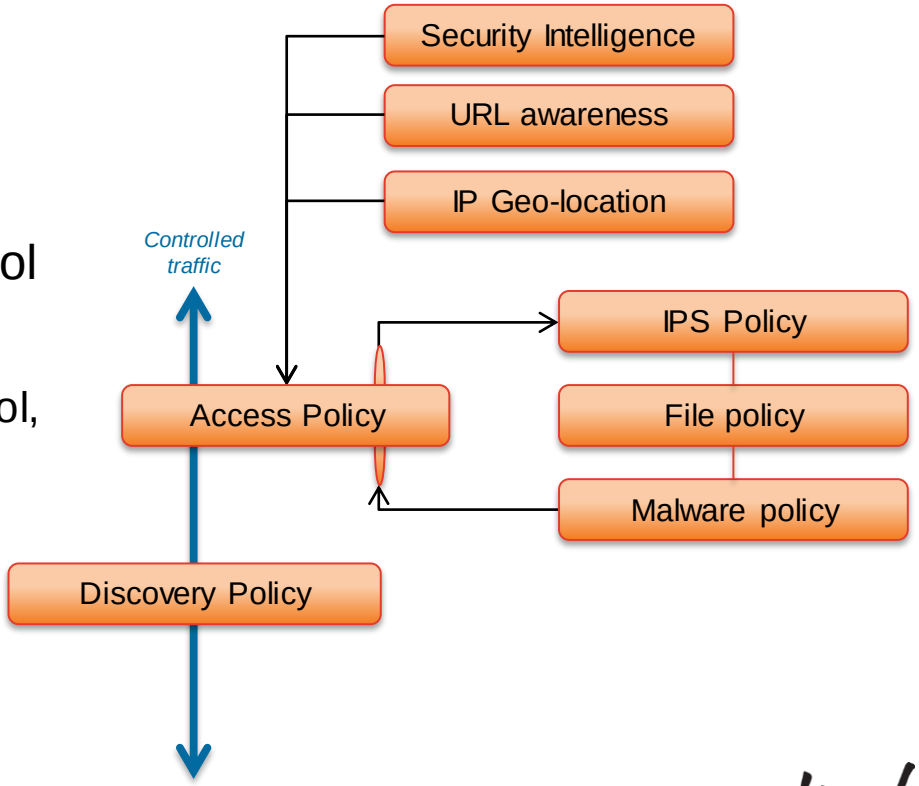
Detection Capabilities

Talos 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 control
- **Comprehensive access control**
  - By network zone, VLAN, IP, port, protocol, 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, AMP Endpoint events
- **Network File Trajectories** – Tracking of Files as they traverse the network

Network Awareness and Full Stack Visibility

CATEGORIES	EXAMPLES	Cisco/Sourcefire NGIPS	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 → **Network Awareness**

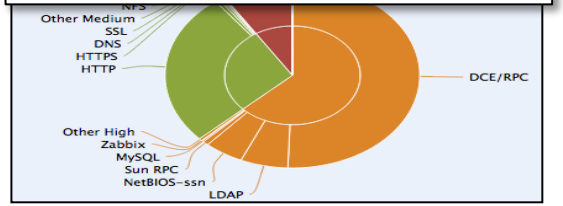
Context Through FireSIGHT

- 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

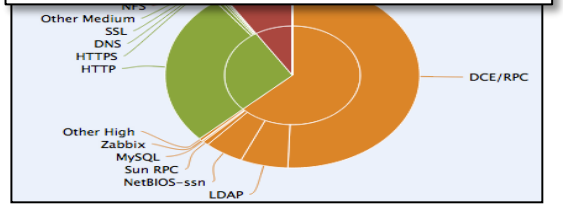
FireSIGHT™ Context Explorer

View all application traffic…

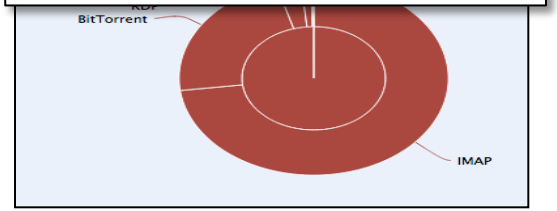


FireSIGHT™ Context Explorer

View all application traffic…

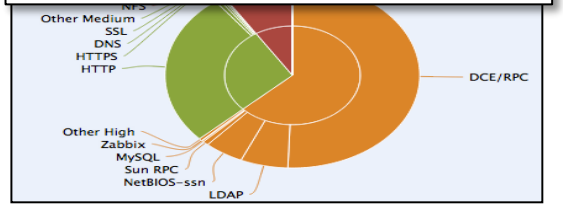


Look for risky applications…

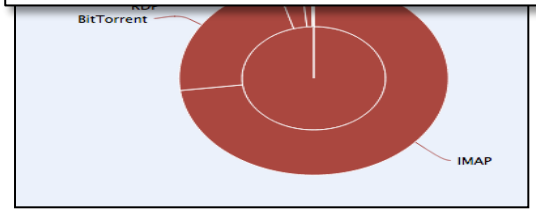


FireSIGHT™ Context Explorer

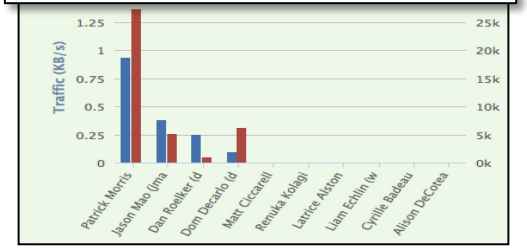
View all application traffic…



Look for risky applications…

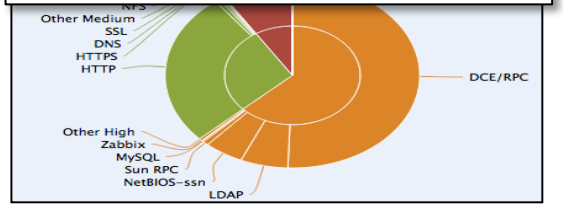


Who is using them?

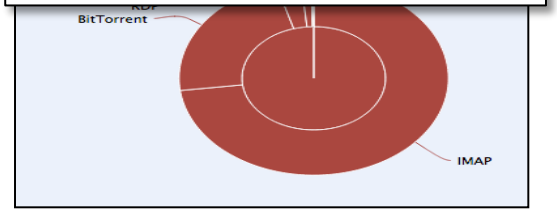


FireSIGHT™ Context Explorer

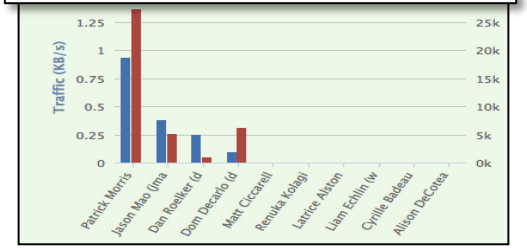
View all application traffic…



Look for risky applications…



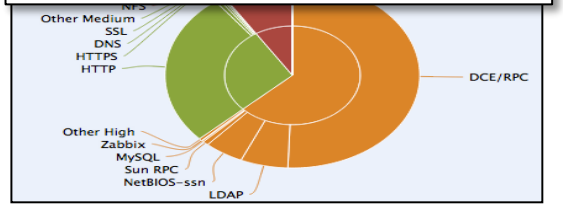
Who is using them?



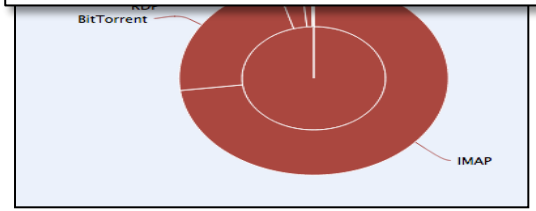
On what operating systems?

FireSIGHT™ Context Explorer

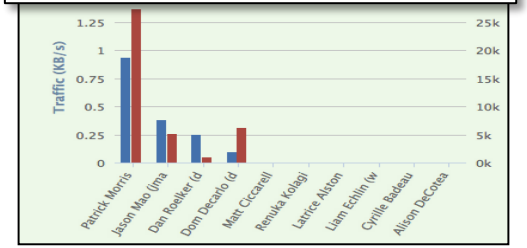
View all application traffic…



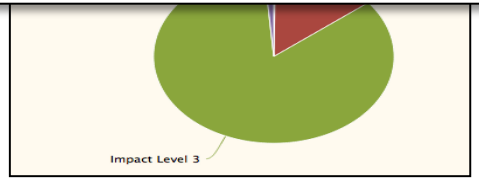
Look for risky applications…



Who is using them?



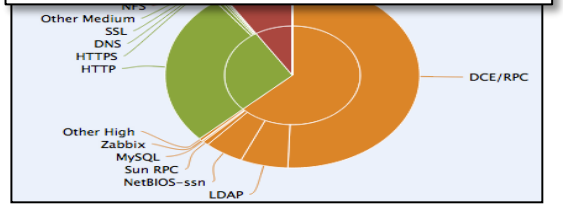
What else have these users been up to?



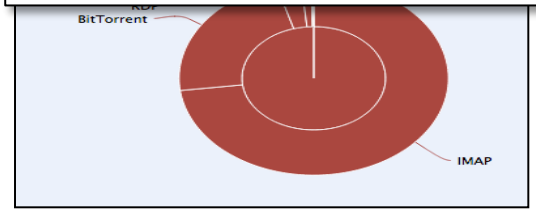
On what operating systems?

FireSIGHT™ Context Explorer

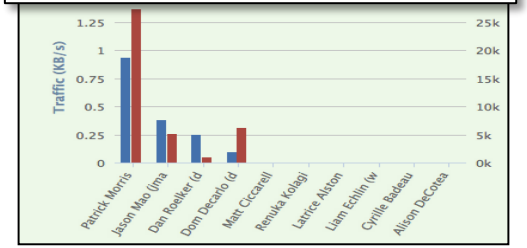
View all application traffic…



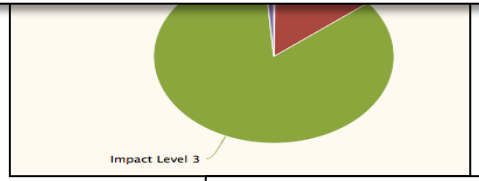
Look for risky applications…



Who is using them?

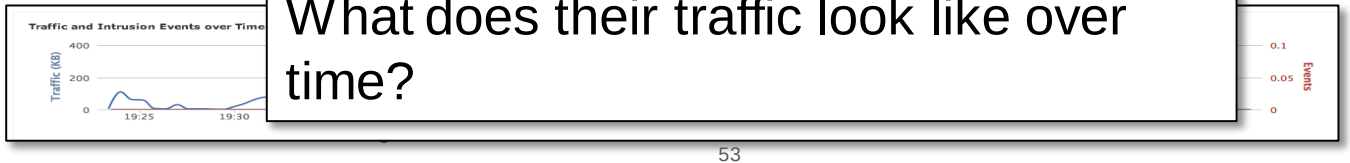


What else have these users been up to?



On what operating systems?

What does their traffic look like over time?



Network Awareness

Overview | Analysis | Policies | Devices | Objects | Endpoints | Health | System | Help

Connection Events | Intrusion | Hosts | Users | Vulnerabilities | Correlation | Custom | Search

Bookmark This Page | Report Designer | Workflows | View Bookmarks | Search

Connection Events

Connections with Application Details ▸ Table View of Connection Events

2011-11-15 15:37:56 - 2011-11-15 16:39:53
Expanding

▸ Search Constraints (Edit Search Save Search)

Connection Events | Intrusion Events | Hosts | Applications | Application Details | Servers | Host Attributes | Discovery Events | Users | Vulnerabilities | Third-Party Vulnerabilities | Correlation Events | White List Ev

First Packet	Last Packet	Action	Initiator IP	Responder IP	Ingress Security Zone	Egress Security Zone	Initiator Port	Responder Port	Application Protocol
2011-11-15 16:39:47		Allow			Passive		1040/tcp	80 (http)/tcp	HTTP
2011-11-15 16:39:47		Allow			Passive		42812/udp	53 (domain)/udp	DNS
2011-11-15 16:39:47		Allow			Passive		1041/tcp	80 (http)/tcp	HTTP
2011-11-15 16:39:47		Allow			Passive		41197/udp	53 (domain)/udp	DNS
2011-11-15 16:39:47		Allow			Passive		51495/udp	53 (domain)/udp	DNS
2011-11-15 16:39:47		Allow			Passive		35986/udp	53 (domain)/udp	DNS
2011-11-15 16:39:46	2011-11-15 16:39:46	Allow			Passive		54602/tcp	389 (ldap)/tcp	LDAP
2011-11-15 16:39:46		Allow			Passive		45206/udp	53 (domain)/udp	DNS
2011-11-15 16:39:46		Allow			Passive		49703/tcp	389 (ldap)/tcp	LDAP
2011-11-15 16:39:46		Allow			Passive		50607/udp	53 (domain)/udp	DNS
2011-11-15 16:39:46		Allow			Passive		58095/tcp	389 (ldap)/tcp	LDAP
2011-11-15 16:39:46		Allow			Passive		49383/udp	53 (domain)/udp	DNS
2011-11-15 16:39:46		Allow			Passive		1038/tcp	80 (http)/tcp	HTTP
2011-11-15 16:39:46		Allow			Passive		1037/tcp	80 (http)/tcp	HTTP
2011-11-15 16:39:46		Allow			Passive		54602/tcp	389 (ldap)/tcp	LDAP
2011-11-15 16:39:46		Allow			Passive		55131/udp	53 (domain)/udp	DNS
2011-11-15 16:39:46		Allow			Passive		1036/udp	53 (domain)/udp	DNS
2011-11-15 16:39:46		Trust			Passive		871/udp	846/udp	
2011-11-15 16:39:46		Trust			Passive		22 (ssh)/tcp	38398/tcp	
2011-11-15 16:39:45	2011-11-15 16:39:50	Trust			Passive		846/udp	51012/udp	

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

SOURCEfire

Network Awareness

Overview | Analysis | Policies | Devices | Objects | Endpoints

Connection Events | Intrusion | Hosts | Users | Vulnerabilities | Correlation | Custom

Connection Events

Connections with Application Details ▸ Table View of Connection Events

▸ Search Constraints (Edit Search Save Search)

Connection Events | Intrusion Events | Hosts | Applications | Application Details | Servers | Host A

First Packet	Last Packet	Action	Initiator IP	Responder IP
2011-11-15 16:39:47		Allow		
2011-11-15 16:39:47		Allow		
2011-11-15 16:39:47		Allow		
2011-11-15 16:39:47		Allow		
2011-11-15 16:39:47		Allow		
2011-11-15 16:39:47		Allow		
2011-11-15 16:39:46	2011-11-15 16:39:46	Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Trust		
2011-11-15 16:39:46		Trust		
2011-11-15 16:39:45	2011-11-15 16:39:50	Trust		

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

Host: [redacted]

Scan Host | Generate White List Profile

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)

Operating System

Vendor	Product	Versi		Source	Confidence
Microsoft	Windows	2000,		FireSIGHT	66

Servers (3)

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

Applications (28)

Application Protocol	Client	Version	Web Application
DNS	DNS		
Google	Google		
Google Safebrowsing	Google Safebrowsing		
IRC	IRC		
HTTP	Internet Explorer	6.0	Adobe Software
HTTP	Internet Explorer	6.0	Atom
HTTP	Internet Explorer	6.0	Blogger
HTTP	Internet Explorer	6.0	Dropbox
HTTP	Internet Explorer	6.0	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

Network Awareness

Overview | Analysis | Policies | Devices | Objects | Endpoints

Connection Events | Intrusion | Hosts | Users | Vulnerabilities | Correlation | Custom

Connection Events

Connections with Application Details ▸ Table View of Connection Events

▸ Search Constraints (Edit Search Save Search)

Connection Events | Intrusion Events | Hosts | Applications | Application Details | Servers | Host A

First Packet	Last Packet	Action	Initiator IP	Responder IP
2011-11-15 16:39:47		Allow		
2011-11-15 16:39:47		Allow		
2011-11-15 16:39:47		Allow		
2011-11-15 16:39:47		Allow		
2011-11-15 16:39:47		Allow		
2011-11-15 16:39:47		Allow		
2011-11-15 16:39:46	2011-11-15 16:39:46	Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Trust		
2011-11-15 16:39:46		Trust		
2011-11-15 16:39:45	2011-11-15 16:39:50	Trust		

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

Host: [redacted]

Scan Host | Generate White List Profile

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

Who is at the host

Operating System

Vendor	Product	Versi		Source	Confidence
Microsoft	Windows	2000,		FireSIGHT	66

Servers (3)

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

Applications (28)

Application Protocol	Client	Version	Web Application
DNS	DNS		
Google	Google		
Google Safebrowsing	Google Safebrowsing		
IRC	IRC		
HTTP	Internet Explorer	6.0	Adobe Software
HTTP	Internet Explorer	6.0	Atom
HTTP	Internet Explorer	6.0	Blogger
HTTP	Internet Explorer	6.0	Dropbox
HTTP	Internet Explorer	6.0	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

Network Awareness

Overview | Analysis | Policies | Devices | Objects | Endpoints

Connection Events | Intrusion | Hosts | Users | Vulnerabilities | Correlation | Custom

Connection Events

Connections with Application Details ▸ Table View of Connection Events

▸ Search Constraints (Edit Search Save Search)

Connection Events | Intrusion Events | Hosts | Applications | Application Details | Servers | Host A

First Packet	Last Packet	Action	Initiator IP	Responder IP
2011-11-15 16:39:47		Allow		
2011-11-15 16:39:47		Allow		
2011-11-15 16:39:47		Allow		
2011-11-15 16:39:47		Allow		
2011-11-15 16:39:47		Allow		
2011-11-15 16:39:47		Allow		
2011-11-15 16:39:46	2011-11-15 16:39:46	Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Trust		
2011-11-15 16:39:46		Trust		
2011-11-15 16:39:45	2011-11-15 16:39:50	Trust		

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

Host: [redacted]

Scan Host | Generate White List Profile

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)

Operating System

Vendor	Product	Versi
Microsoft	Windows	2000,

Servers (3)

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

Applications (28)

Application Protocol	Client	Version	Web Application
DNS	DNS		
Google	Google		
Google Safebrowsing	Google Safebrowsing		
IRC	IRC		
HTTP	Internet Explorer	6.0	Adobe Software
HTTP	Internet Explorer	6.0	Atom
HTTP	Internet Explorer	6.0	Blogger
HTTP	Internet Explorer	6.0	Dropbox
HTTP	Internet Explorer	6.0	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

Who is at the host

OS & version Identified

Network Awareness

Overview | Analysis | Policies | Devices | Objects | Endpoints

Connection Events | Intrusion | Hosts | Users | Vulnerabilities | Correlation | Custom

Connection Events

Connections with Application Details ▸ Table View of Connection Events

▸ Search Constraints (Edit Search Save Search)

Connection Events | Intrusion Events | Hosts | Applications | Application Details | Servers | Host A

First Packet	Last Packet	Action	Initiator IP	Responder IP
2011-11-15 16:39:47		Allow		
2011-11-15 16:39:47		Allow		
2011-11-15 16:39:47		Allow		
2011-11-15 16:39:47		Allow		
2011-11-15 16:39:47		Allow		
2011-11-15 16:39:47		Allow		
2011-11-15 16:39:46	2011-11-15 16:39:46	Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Trust		
2011-11-15 16:39:46		Trust		
2011-11-15 16:39:45	2011-11-15 16:39:50	Trust		

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

Host: [redacted]

Scan Host | Generate White List Profile

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)

Operating System

Vendor	Product	Versi
Microsoft	Windows	2000,

Servers (3)

Protocol	Port	Application Protocol	Vendor and V
tcp	1189	pending	
tcp	1077	pending	
tcp	22	SSH	OpenSSH 5.1p1

Applications (28)

Application Protocol	Client	Version	Web Application
DNS	DNS		
Google	Google		
Google Safebrowsing	Google Safebrowsing		
IRC	IRC		
HTTP	Internet Explorer	6.0	Adobe Software
HTTP	Internet Explorer	6.0	Atom
HTTP	Internet Explorer	6.0	Blogger
HTTP	Internet Explorer	6.0	Dropbox
HTTP	Internet Explorer	6.0	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

Who is at the host

OS & version Identified

Server applications and versions

Network Awareness

Overview | Analysis | Policies | Devices | Objects | Endpoints

Connection Events | Intrusion | Hosts | Users | Vulnerabilities | Correlation | Custom

Connection Events

Connections with Application Details ▸ Table View of Connection Events

▸ Search Constraints (Edit Search Save Search)

Connection Events | Intrusion Events | Hosts | Applications | Application Details | Servers | Host A

First Packet	Last Packet	Action	Initiator IP	Responder IP
2011-11-15 16:39:47		Allow		
2011-11-15 16:39:47		Allow		
2011-11-15 16:39:47		Allow		
2011-11-15 16:39:47		Allow		
2011-11-15 16:39:47		Allow		
2011-11-15 16:39:47		Allow		
2011-11-15 16:39:46	2011-11-15 16:39:46	Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Allow		
2011-11-15 16:39:46		Trust		
2011-11-15 16:39:46		Trust		
2011-11-15 16:39:45	2011-11-15 16:39:50	Trust		

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

Host: [redacted]

Scan Host | Generate White List Profile

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)

Operating System

Vendor	Product	Versi
Microsoft	Windows	2000,

Servers (3)

Protocol	Port	Application Protocol	Vendor and V
tcp	1189	pending	
tcp	1077	pending	
tcp	22	SSH	OpenSSH 5.1p1

Applications (28)

Application Protocol	Client	Version	
DNS	DNS		
Google	Google		
Google Safebrowsing	Google Safebrowsing		
IRC	IRC		
HTTP	Internet Explorer	6.0	Adobe Software
HTTP	Internet Explorer		Atom
HTTP	Internet Explorer	6.0	Blogger
HTTP	Internet Explorer	6.0	Dropbox
HTTP	Internet Explorer	6.0	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

Who is at the host

OS & version Identified

Server applications and versions

Client Applications

Network Awareness

Who is at the host

OS & version Identified

Server applications and versions

Client Applications

Client Version

Network Awareness

Who is at the host

OS & version Identified

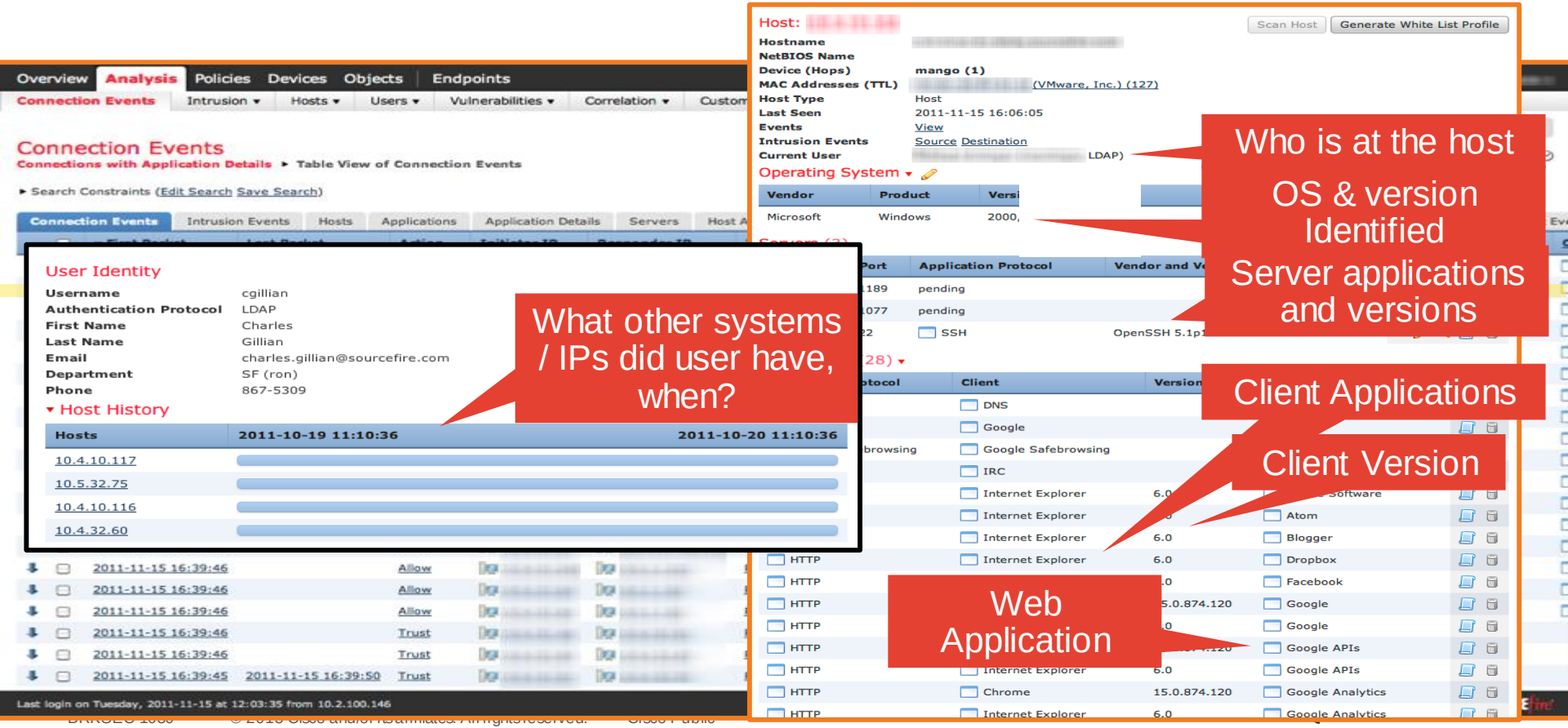
Server applications and versions

Client Applications

Client Version

Web Application

Network Awareness



Security Automation

IT Insight

Spot rogue hosts, anomalies, policy violations, and more

Automated Tuning

Adjust IPS policies automatically based on network change

Indications of Compromise

Identify the machines most likely to be owned

Impact Assessment

Reduce actionable events by up to 99% with correlation

User Identification

Associate users with security and compliance events

Security Automation: Streamlining Operations

Impact Assessment

- Discovers Host, Application and User information in real-time, continuously, passively
- Derives a Vulnerability Map of the monitored Network
- Correlates all Intrusion Events to an Impact of the attack against the target
- Focuses the analyst on events that really matter

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

Security Automation: Streamlining Operations

Impact Assessment

Security Automation: Streamlining Operations

Recommended Rules

Policy Information

Name: Default Production Demo Lab IPS Policy

Description: Sourcefire Provided. For best results, do not modify.

Drop when Inline: ☑

Base Policy Security Over Connectivity

The base policy is up to date (Rule Update 2013-10-09-004-vrt)

This policy defines 0 variables

This policy has 9038 enabled rules

- 558 rules generate events
- 8480 rules drop and generate events

FireSIGHT recommends 7154 rule state settings for 7430 hosts

- Set 214 rules to generate events
- Set 3550 rules to drop and generate events
- Set 3390 rules to disabled

Policy is not using the recommendations. Click to change recommendations

Last generated: 2013 Oct 10 10:15:33

Commit Changes | Discard Changes

Security Automation: Reducing Response Time

Associating Users with Security 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)

Security Automation: Identifying Compromises

Indications of Compromise

Security Automation: Identifying Compromises

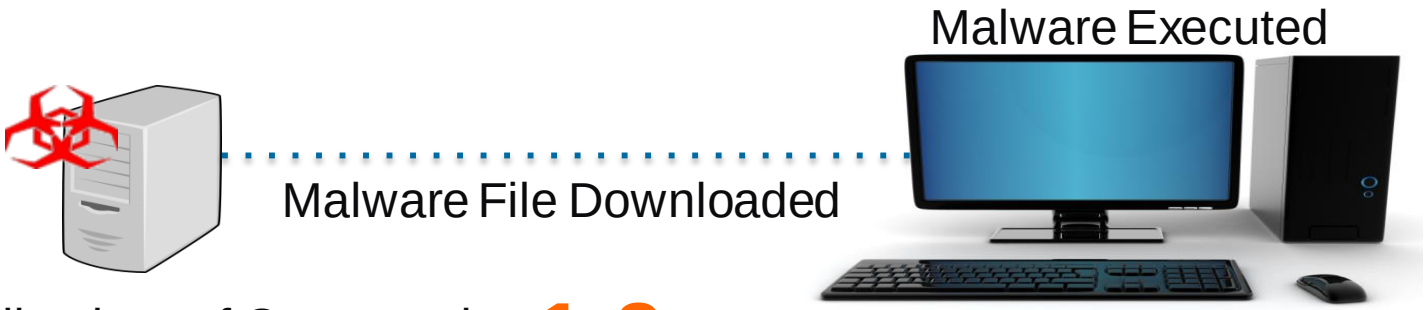
Indications of Compromise

Malware File Downloaded

Indications of Compromise: **1**

Security Automation: Identifying Compromises

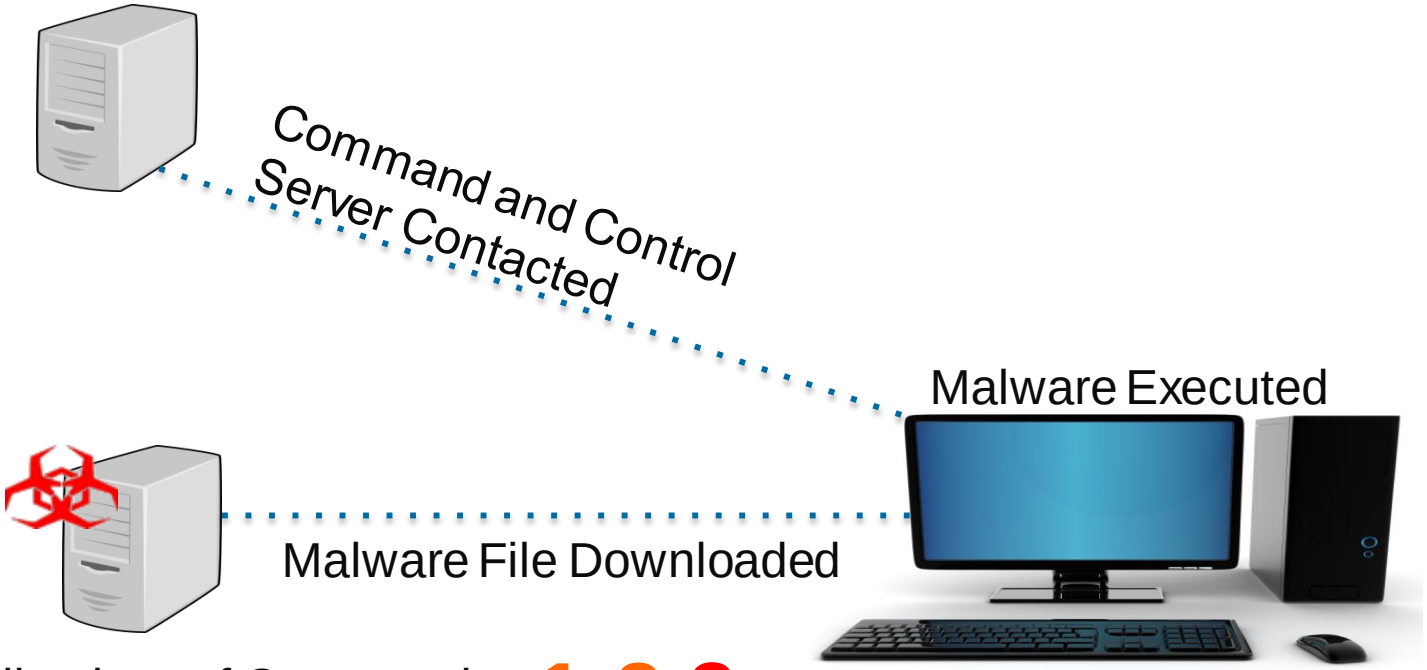
Indications of Compromise



Indications of Compromise: **1 2**

Security Automation: Identifying Compromises

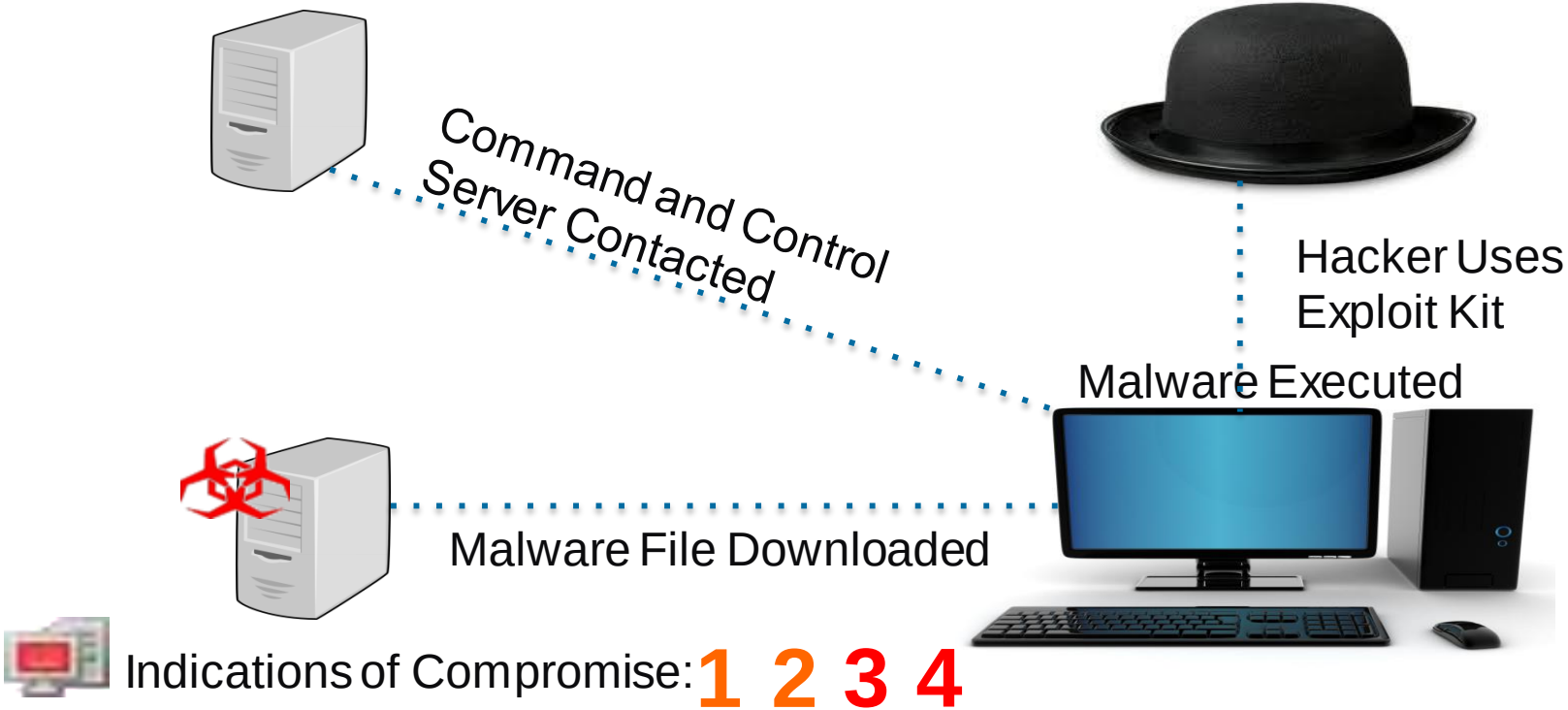
Indications of Compromise



Indications of Compromise: **1 2 3**

Security Automation: Identifying Compromises

Indications of Compromise



Security Automation: Identifying Compromises

Indications of Compromise

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)

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

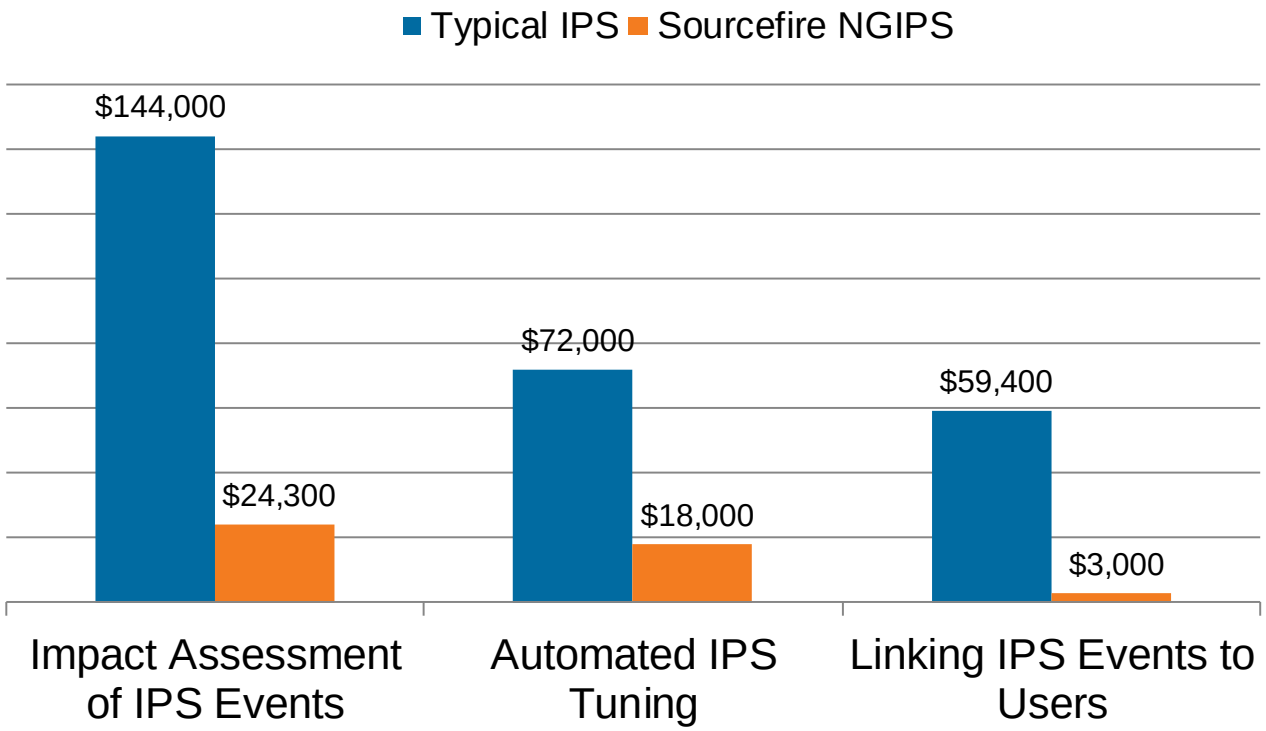
Security Automation: Costs of IPS Maintenance

One of the world's 3 largest credit reporting agencies:

- 20,000 nodes
- 7,500 employees

Generic Work Rate: $75/hour

Sourcefire NGIPS collectively saves this customer $230,100 per year.



Source: SANS "Calculating TCO on Intrusion Prevention Technology" whitepaper, December 2013

Gartner Report (2013)

“Next-Generation IPS Technology Disrupts the IPS Market”

- Sourcefire truly has NGIPS capabilities
  - Leading example in the market
  - Gartner attributes growth to innovation
- Disruption extends to NGFW
  - Sourcefire has forced other IPS vendors to develop contingency plans
  - Gartner writes, unlike Sourcefire: “Most NGFWs have limited threat detection capabilities”
- Advanced threats are part of the story
  - NGIPS should also address advanced threats, for example, with integrated advanced malware protection

“...security buyers seek more **application visibility**, more situational or **context awareness** of network interactions, and greater **control over the content** coming into and out of their organisations.” — **Gartner**


LICENSED FOR DISTRIBUTION

Gartner

Next-Generation IPS Technology Disrupts the IPS Market

26 March 2013 ID:G00247375

Analyst(s): Eric Ahrn

VIEW SUMMARY

The network IPS market has shown slow growth from 2011 to 2012 due in part to the economic decline, but also due to erosion of IPS sales to NGFW providers. We discuss the impact of NGFW on the network IPS market and how next-generation IPS is a disruptive force to both the IPS and NGFW market.

Overview

Impacts

- Next-generation firewalls (NGFWs) that offer intrusion prevention system (IPS) technologies combined with firewall, app control and user risk awareness features are capturing sales once won by IPS providers.
- Network IPS providers have released extended capabilities defined as next-generation IPS (NGIPS) technologies that show evidence of being a disruptive force in the network IPS market.
- Some network IPS providers leading with NGIPS technologies have released NGFW products as well, showing their desire to compete in the NGFW market.
- Advanced threat appliance providers could threaten the network IPS market in the future by capturing spending usually destined for the IPS market from security buyers.

Recommendations

- Product marketing managers at network IPS providers need to start incorporating NGIPS technologies to offset the competitive pressure from the NGFW market.
- Product developers at IPS providers should start working on their NGIPS product development and marketing plans to protect market share within the IPS market.
- Executive leaders at network IPS providers should build contingency plans to enter the enterprise firewall market. If Sourcefire can successfully enter the NGFW marketplace, it may become critical for other IPS providers to follow suit in order to continue competitive pressure.
- Competitive intelligence managers at network IPS providers need to prepare for the potential competitive threat of advanced targeted attack (ATA) appliance players, and develop plans to either compete in the advanced threat market or partner with ATA providers.

Analysis

Figure 1 describes the impacts and recommendations for next-generation IPS.

Learn how Gartner can help you succeed

Become a Client now >

DOWNLOAD ATTACHMENTS

impactapprai... (21KB)

FirePOWER Application Control

Reduce Risk Through Granular Application Control

- Control access for applications, users and devices
- “Employees may view Facebook, but only Marketing may post to it”
- “No one may use peer-to-peer file sharing apps”

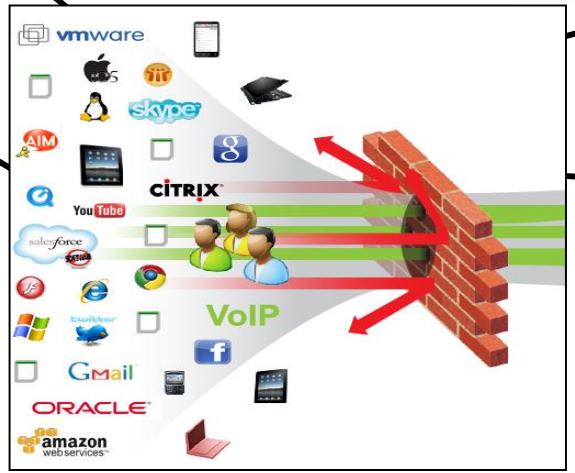
Over 2,200 apps, devices, and more!

Benefits of Application Control

Social:
Security and DLP

Security:
Reduce Attack Surface

Mobile:
Enforce BYOD Policy



Bandwidth:
Recover Lost Bandwidth

Application Visibility

Overview | Analysis | Policies | Devices | Objects | Endpoints | Health | System | Help

Dashboards | Reporting | Summary

Application Statistics

Provides traffic and intrusion event statistics by application

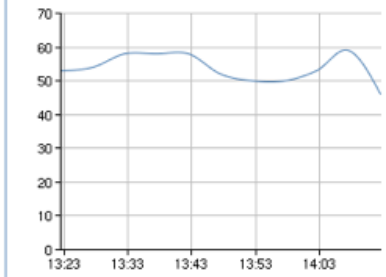
Connections | Intrusion Events

Allowed Connections by Application

Application	Allowed Connections
Sun RPC	191,962
Sun RPC client	191,962
DNS	177,792
HTTP	80,881
HTTPS	41,480
+1 Direct Connect	23,586
Direct Connect	23,586
+1 SNMP	20,094
+1 Dropbox	13,369
+1 SSL	9,756

Last updated less than a minute ago

Unique Applications over Time



Last updated less than a minute ago

Risky Applications

Application
BitTorrent
eDonkey
Ustream.tv
Facebook
+1 Yet ABC
Facebook A
QQ
MySpace
-1 Gnutella

Last updated 2 minu

Allowed Connections by Business

Business Relevance	Allowed Connections
High	410,375
Medium	331,579
Very High	53,575
Very Low	6,905
Low	28

Allowed Connections by Application Risk

Risk	Allowed Connections
High	584,664
Very Low	138,513
Medium	72,069
Very High	6,923
Low	293

Traffic by Applicat

Category	
remote adminis	
network	
security manag	
remote file stor	
download manager	1,354.04
remote desktop control	404.91

Risky Applications

Title: Risky Applications
Preset: None
Table: Application Statistics
Field: Application
Aggregate: Total Bytes (KB)
Filter: High Risk Applications with Low Bu
Show: Top
Results: 10
Show Movers: ☑
Color:

Application	Total Bytes (KB)
BitTorrent	41,077.00
eDonkey	320.16
Ustream.tv	81.63
Facebook	34.69
+1 Yet ABC	8.89
Facebook Apps	4.16
QQ	1.98
MySpace	0.70
-1 Gnutella	0.53

Last updated 4 minutes ago

Last login on Tuesday, 2011-11-15 at 10:23:56 from 10.2.100.129

SOURCEfire

Application Control Example

Prevent BitTorrent

Add Rule

Name: New Rule | Enabled | Action: Block | Insert: below rule | 1

Zones | Networks | VLAN Tags | Users | **Applications** | Services | URLs | Policy | Logging | Comments

Application Filters

Search by name

- Risks (Any Selected) 3
  - Very Low 1
  - Low 0
  - Medium 0
  - High 1
  - Critical
- Categories (Any Selected)
- Tags (Any Selected) 0
  - adds/installs other software 0
  - adult content 0
  - allows remote connect 0

Available Applications (7)

bit

- All apps matching the filter
- BitDefender
- BITS
- BitTorrent
- BitTorrent client
- BitTorrent tracker
- Orbitz
- Tobit

Add to Rule

Selected Applications and Filters

Applications

- BitTorrent tracker
- BitTorrent client
- BitTorrent

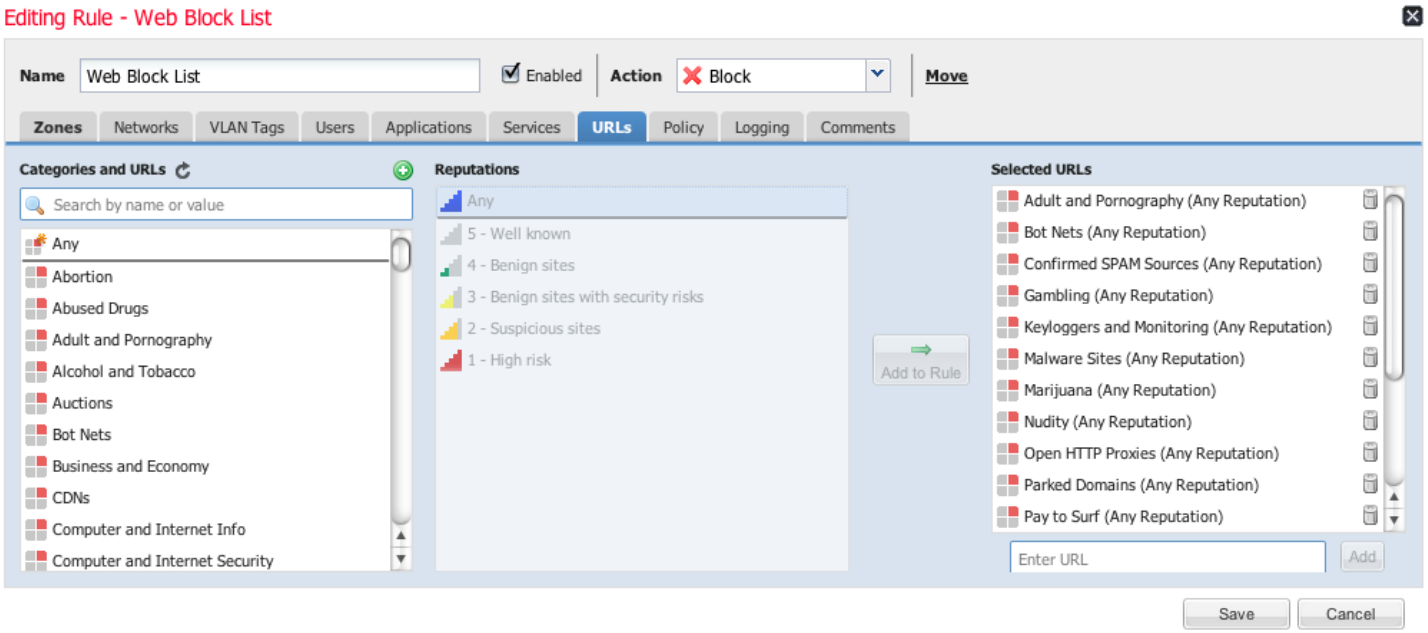
Save | Cancel

URL Filtering

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

URL Filtering

- Dozens of Content Categories
- URLs Categorised by Risk



Applications are Often Encrypted

- Facebook and Google default to SSL
- Benefits of Sourcefire off-box decryption solution:
  - Improved Performance – acceleration and policy
  - Centralised Key Management
  - Interoperable with 3rd party products

SSL1500

1.5 Gbps

4 Gbps total

SSL2000

2.5 Gbps

10 Gbps total

SSL8200

3.5 Gbps

20 Gbps total

OpenAppID Overview

- What is OpenAppID?
  - An open source application-focused detection language that enables users to create, share and implement custom application detection.
- Key Advantages
  - New simple language to detect apps
  - Reduces dependency on vendor release cycles
  - Build custom detections for new or specific (ex. Geo-based) app-based threats
  - Easily engage and strengthen detector solutions
  - Application-specific detail with security events

OpenAppID Deliverables

- OpenAppID Language Documentation
- A special Snort release engine with the OpenAppID preprocessor
  - Detect apps on network
  - Report usage stats
  - Block apps by policy
  - Snort rule language extensions to enable app specification
  - Include 'App Context' to IPS events
- Library of OpenAppID Detectors
  - > 1000 detectors contributed by Cisco
  - Extendable sample detectors

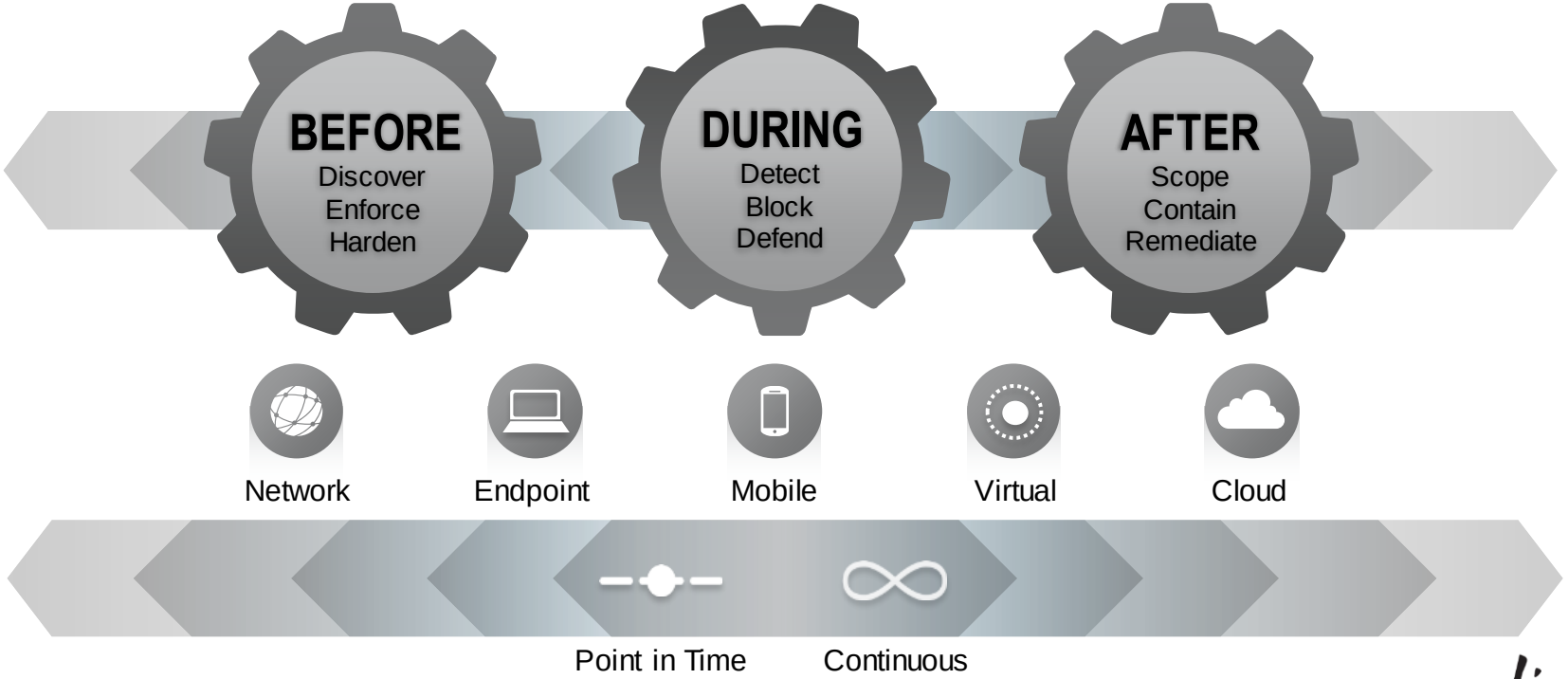
Available to community at Snort.org

Better Together: Sourcefire and Cisco

Cisco live!

Better Together Benefits

Address the Entire Attack Continuum



Better Together Benefits

See and Protect More Completely

- Broad range of attack vectors
- Application visibility and control for more than 2,000 applications
- Contextual awareness that extends beyond traditional NGIPS, NGFW

Network | Endpoint | Mobile | Virtual | Cloud

Better Together Benefits

Provide Lowest Cost of Ownership

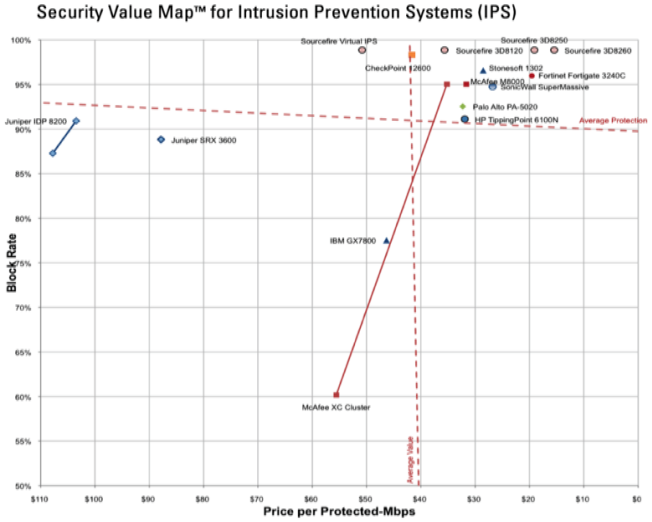
- Automation streamlines operations and reduces response time
- Industry-leading TCO – NSS Labs

IT Insight

Impact Assessment

Automated Tuning

User Identification

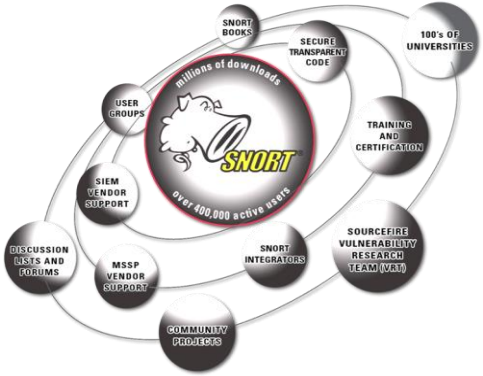


NSS Labs

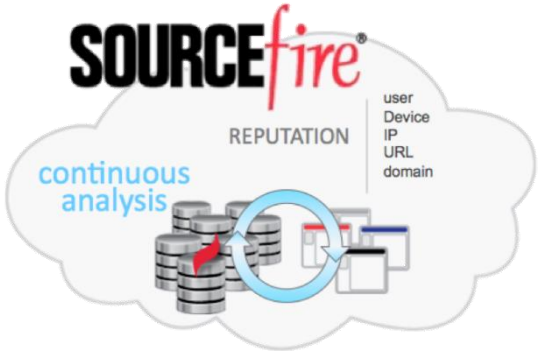
Better Together

Avail Collective Power and Openness

Open Industry Standards



Collective Security Intelligence



Solution Provider Community

Better Together

Delivering 'Best-in-Class' Cybersecurity Solutions that:

CISCO + SOURCEfire®

- ☑ Address entire attack continuum
- ☑ See and protect more completely
- ☑ Provide lowest cost of ownership
- ☑ Avail collective power and openness

Continue Your Education

- Demos in the Cisco Campus
- Walk-in Self-Paced Labs
- Meet the Expert 1:1 meetings

Q & A

Complete Your Online Session Evaluation

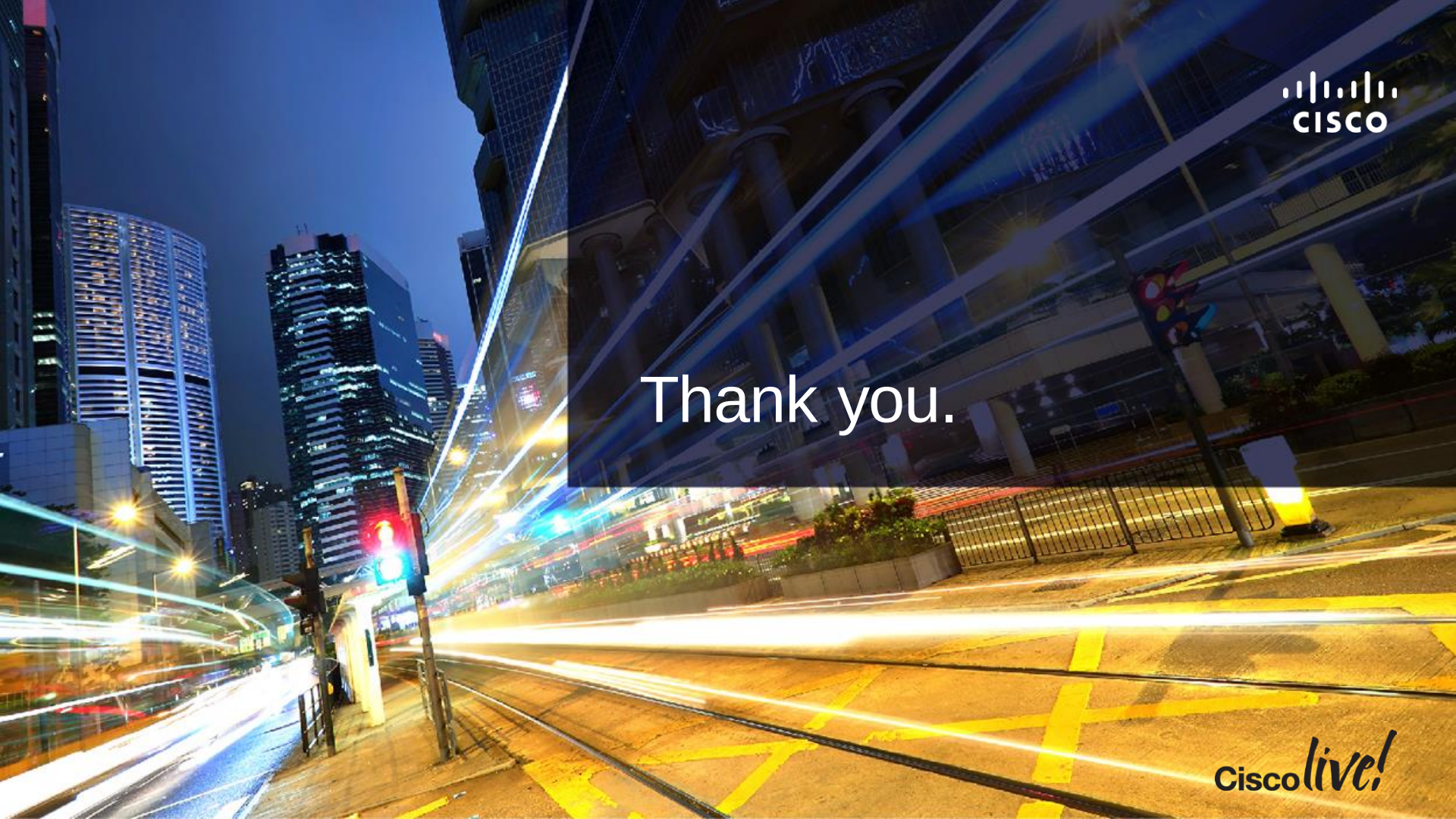
Give us your feedback and receive a Cisco Live 2015 T-Shirt!

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 http://showcase.genie-connect.com/clmelbourne2015
- Visit any Cisco Live Internet Station located throughout the venue

T-Shirts can be collected in the World of Solutions on Friday 20 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



Thank you.

CISCO