



# Cisco Next Generation Firewalls and IPS

Simple and Efficient Security you gonna like

---

Dragan Novaković

Cisco Systems



# ASA “Adaptive Security Appliance”



HA and Clustering



VPN



Protocol  
Inspection



Data Center  
Security



Network Firewall  
[Routing | Switching]



Mix Multi Context  
Mode



Identity Based  
Policy Control



Service Provider  
Security

ASDM (OnBox) / Command Line  
Cisco Security Manager / RESTful API for Management

# Sourcefire – Next Generation security

- Firepower Next Generation IPS
  - Best of breed IPS
  - Based on open source Snort
  - Integrated Advanced Malware Protection
- Acquired by Cisco in 2013



**SOURCE**fire®

fire**POWER**™



fire**AMP**™

# ASA with FirePOWER Services



better together

## Cisco Collective Security Intelligence Enabled



Cisco ASA

- ▶ Cisco ASA is world's most widely deployed, enterprise-class stateful firewall
- ▶ Granular Cisco® Application Visibility and Control (AVC)
- ▶ Industry-leading FirePOWER next-generation IPS (NGIPS)
- ▶ Reputation- and category-based URL filtering
- ▶ Advanced malware protection

# Firepower Threat Defense

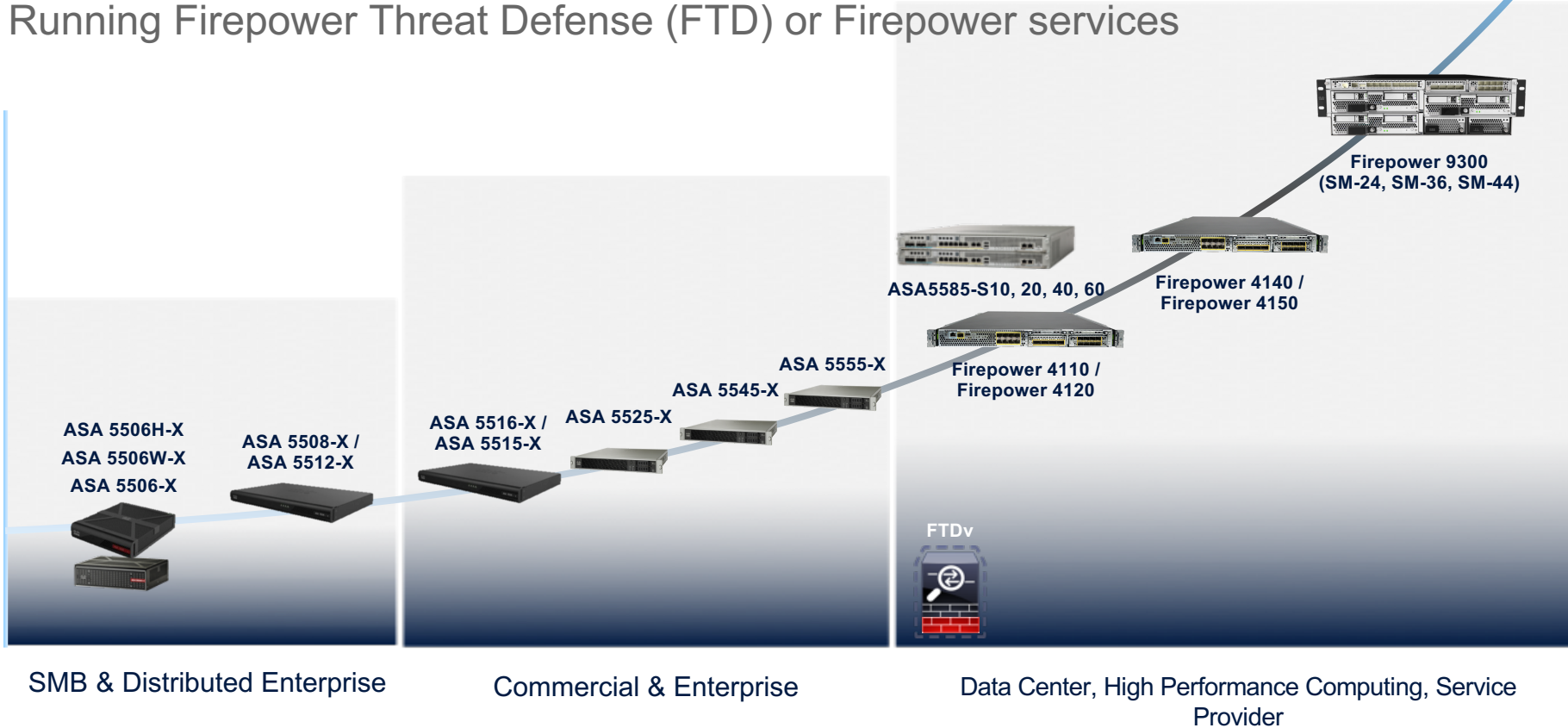


# Platforms & Capabilities

# Cisco Firepower NGFW Product Family

Running Firepower Threat Defense (FTD) or Firepower services

Performance and Scalability



# Cisco NGFW Platforms

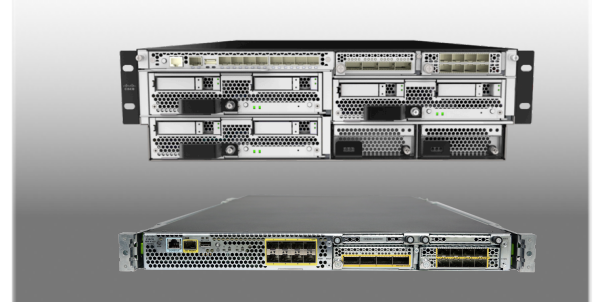
Firepower Threat Defense for  
ASA 5500-X



Firepower Services  
on ASA 5500-X and 5585-X



Firepower 4100 Series  
and Firepower 9300



250 Mb -> 1.75 Gb  
(Max AVC throughput)

4.5 Gb -> 15 Gb  
(Max AVC throughput)

41xx = 12 Gb -> 25 Gb  
93xx = 25 Gb -> 100Gb

NGFW capabilities all managed by Firepower Management Center



# A complete Unified Threat Management solution



## Security

NG Firewall, Client VPN,  
Site to Site VPN, IDS/IPS, Anti-  
Malware, Geo-Firewall



## Networking

NAT/DHCP, 3G/4G Cellular,  
Intelligent WAN (IWAN)



## Application Control

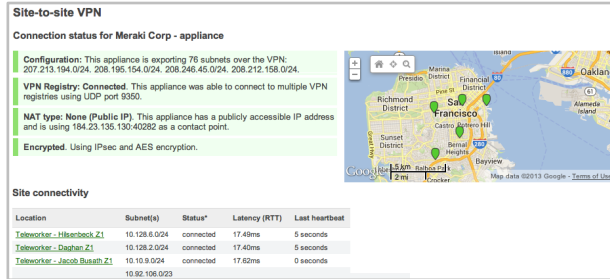
Web Caching, Traffic  
Shaping, Content Filtering

# Why customers choose the Cisco Meraki MX



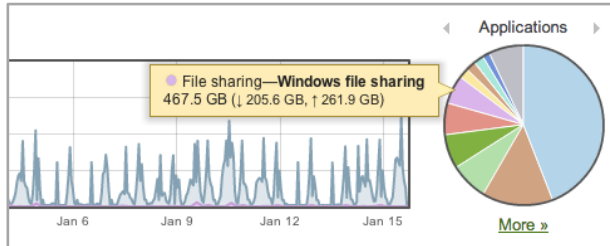
## Intuitive centralized management

- No training, no command line
- Templates to configure at-scale
- Packet capture, built-in tools and diagnostics



## Designed for distributed enterprises

- Single pane of glass visibility
- Zero-touch provisioning
- Seamless updates from the cloud
- Site-to-site IPsec VPN in 3 clicks



## Industry-leading visibility

- Fingerprints users, applications, and devices
- Network-wide monitoring and alerts
- Full stack: APs, switches, Security, MDM

# Cisco Firepower 9300 Platform

*High-speed, scalable security*



Modular

## Benefits

- Standards and interoperability
- Flexible architecture

## Features

- Template-driven security
- Secure containerization for customer apps
- RESTful/JSON API
- Third-party orchestration and management



Multiservice  
Security

## Benefits

- Integration of best-in-class security
- Dynamic service stitching

## Features\*

- Cisco® ASA container
- Cisco Firepower™ Threat Defense containers:
  - NGIPS, AMP, URL, AVC
- Third-party containers:
  - Radware DDoS
  - Other ecosystem partners



Carrier Class

## Benefits

- Industry-leading performance:
  - 600% higher performance
  - 30% higher port density

## Features

- Compact, 3RU form factor
- 10-Gbps/40-Gbps/100-Gbps I/O;
- Terabit backplane
- Low latency, intelligent fast path
- Network Equipment-Building System (NEBS) ready

# Firepower 9300 Overview

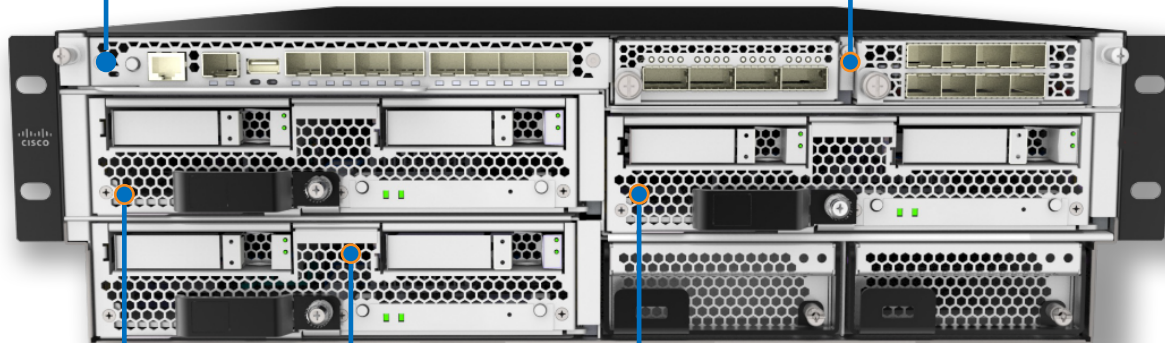
## Supervisor

- Application deployment and orchestration
- Network attachment and traffic distribution
- Clustering base layer for ASA/FTD

## Network Modules

- 10GE/40GE/100GE
- Hardware bypass for inline NGIPS

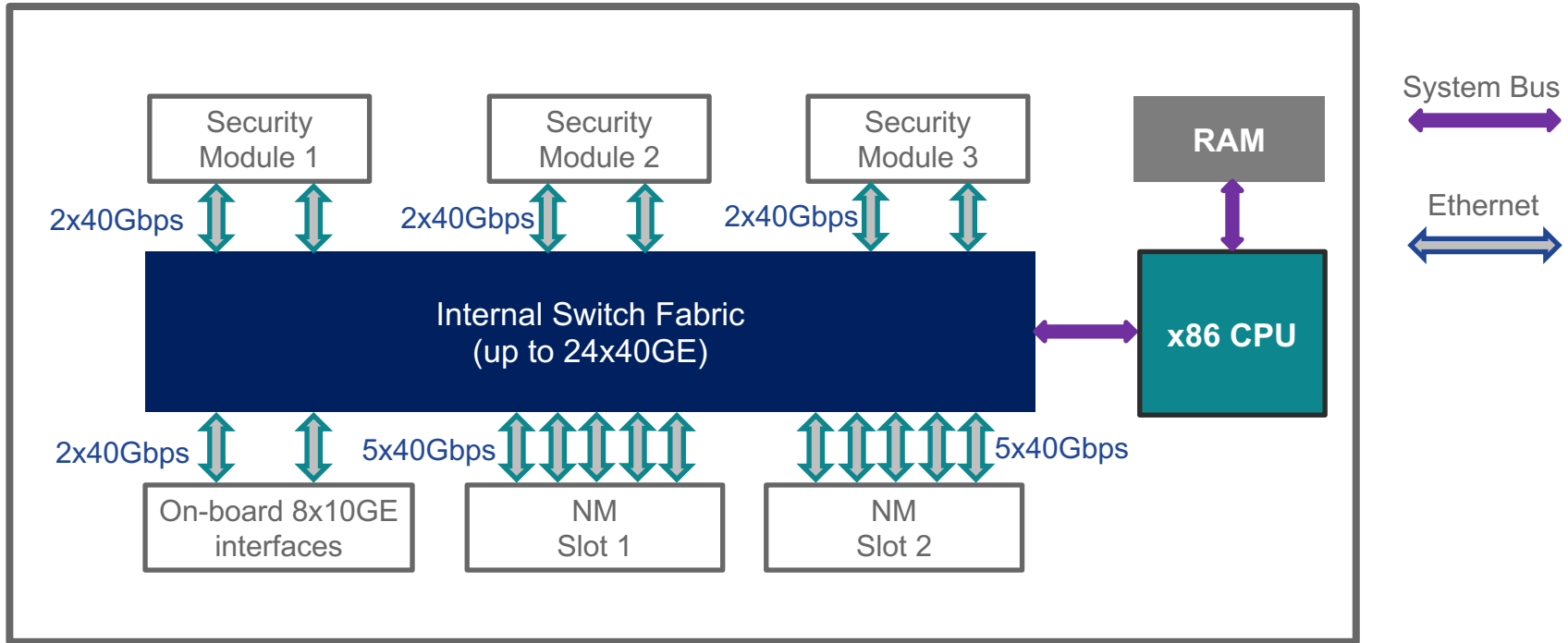
3RU



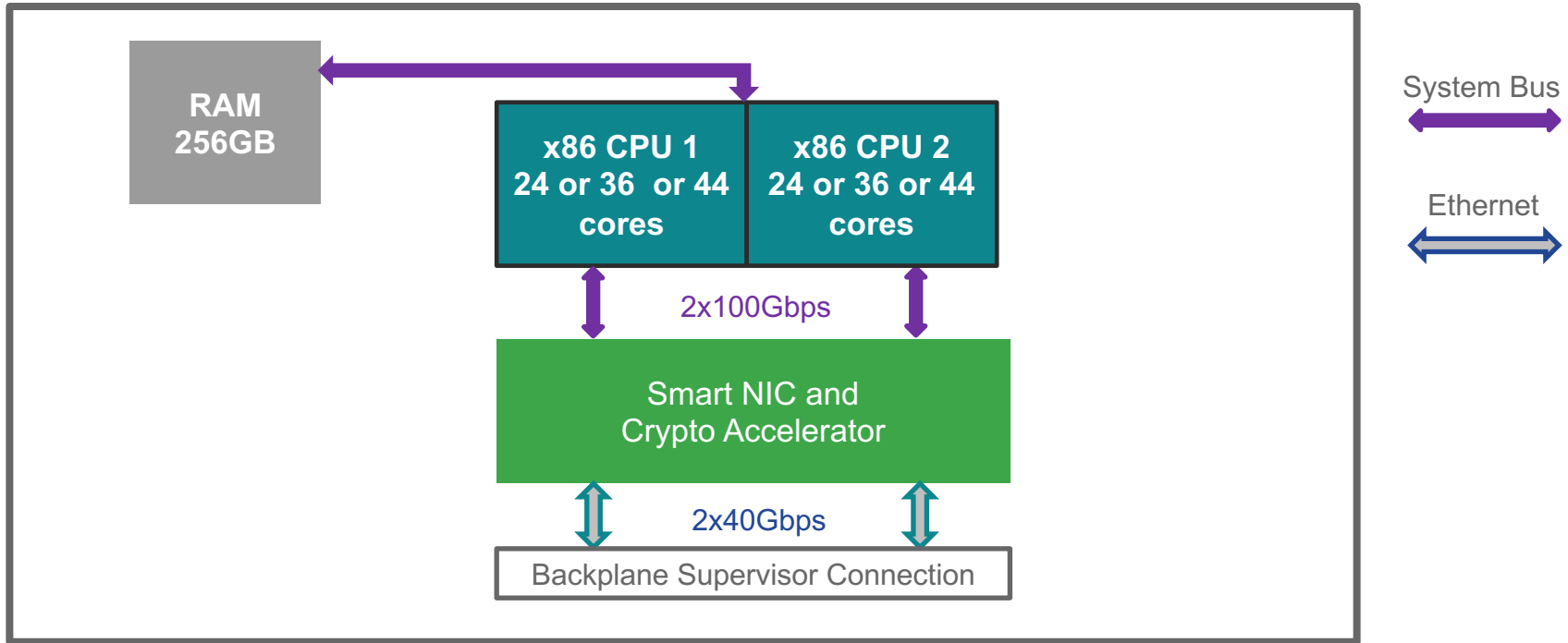
## Security Modules

- Embedded Smart NIC and crypto hardware
- Cisco (ASA, FTD) and third-party (Radware DDoS) applications
- Standalone or clustered within and across chassis

# Supervisor Simplified Hardware Diagram



# Security Module Simplified Diagram



# Firepower 4100 Series

*Introducing four new high-performance models*



## Performance and Density Optimization

- 10-Gbps and 40-Gbps interfaces
- Up to 80-Gbps throughput
- 1-rack-unit (RU) form factor
- Low latency



## Multiservice Security

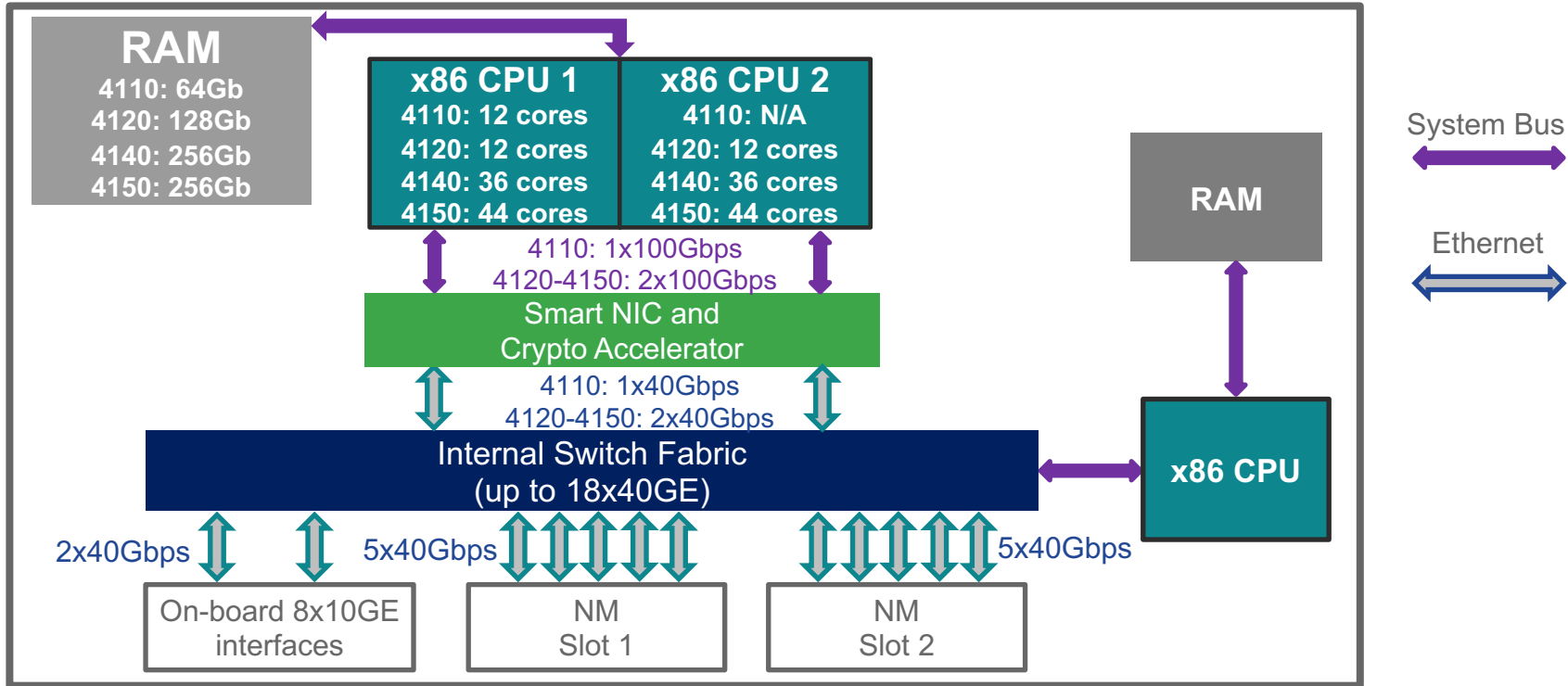
- Integrated inspection engines for FW, NGIPS, Application Visibility and Control (AVC), URL, Cisco Advanced Malware Protection (AMP)
- Radware DefensePro DDoS
- ASA and other future third party



## Unified Management

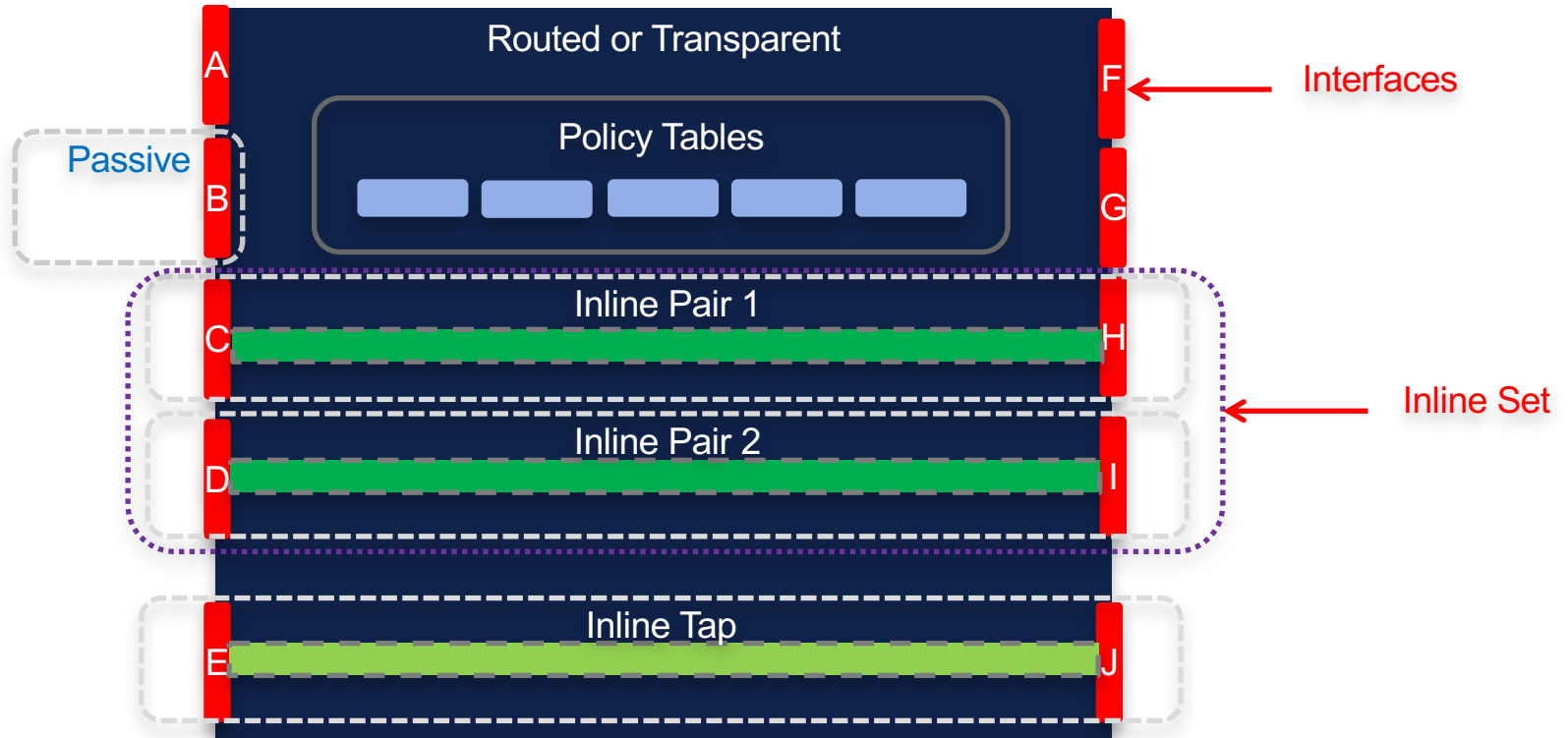
- Single management interface with Firepower Threat Defense
- Unified policy with inheritance
- Choice of management deployment options

# Firepower 4100 Architecture

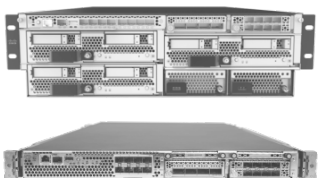




# Mix and Match Interface Modes



# Cisco Firepower and ASA NGFW



## Cisco Firepower™ NGFW



Stop more  
threats



Gain more  
insight



Detect earlier,  
act faster



Reduce  
complexity



Get more from  
your network

Threat Focused

Fully Integrated

# Firepower Management Center

Nice and useful features

# Easily manage NGFWs across multiple sites

## Firepower Management Center

### Centralized management for multi-site deployments



Multi-domain management



Firewall & AVC



Role-based access control



NGIPS



High availability



AMP



APIs and pxGrid integration



Security Intelligence

...Available in physical and virtual options



Manage across many sites

Control access and set policies

Investigate incidents

Prioritize response

# Detection Capabilities

## Talos Collective Security Intelligence

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

# Context comes from knowing the hosts on your network

## Host Profile

IP Addresses **192.168.0.249**

NetBIOS Name

Device (Hops) 198.18.133.11 (0)

MAC Addresses (TTL) 00:29:B0:2B:95:C2 (128)  
00:F1:E8:9E:56:FE (127)

Host Type Host

Last Seen 2015-03-24 01:48:09

Current User

View [Context Explorer](#) | [Connection Events](#) | [Intrusion Events](#) | [File Events](#) | [Malware Events](#)

Scan Host Generate White List Profile

## Indications of Compromise (4)

Category	Event Type	Description	First Seen	Last Seen
Excel Compromise	Excel Compromise Detected by FireAMP	Generic Microsoft Excel Compromise	2015-03-23 02:54:41	2015-03-24 03:34:23
Word Compromise	Word Compromise Detected by FireAMP	Generic Microsoft Word Compromise	2015-03-23 02:54:41	2015-03-23 21:04:39
Java Compromise	Java launched shell	A shell was launched on the host by Java	2015-03-23 02:54:41	2015-03-23 05:59:27
PowerPoint Compromise	PowerPoint launched shell	A shell was launched on the host by Microsoft PowerPoint	2015-03-23 02:54:41	2015-03-23 02:54:41

## Operating System

Vendor	Product	Version	Source
Microsoft	Windows	2000, XP, Server 2003, Vista, 7, Server 2008	FireSIGHT

## Servers (4)

Protocol	Port	Application Protocol	Vendor and Version
tcp	1863	MSNP	
tcp	443	HTTPS	
tcp	80	HTTP	Microsoft-IIS 7.5
tcp	80	HTTP	Microsoft-IIS 6.0
tcp	80	HTTP	Microsoft-IIS 7.0
tcp	7001	MSNP	

## Applications (7)

Application Protocol	Client	Version	Web Application
HTTP	Internet Explorer	6.0	Atlas Advertiser Suite
HTTP	Internet Explorer	6.0	MSN
HTTP	Internet Explorer	6.0	Match.com
HTTP	Dr. Watson		Microsoft
HTTP	Internet Explorer	6.0	Microsoft
HTTP	Microsoft CryptoAPI	5.131.2600.5512	Microsoft
HTTP	Internet Explorer	6.0	Windows Live

## Users (no user history available)

### Attributes

Host Criticality None  
Default White ListNon-Compliant  
Network Survey Non-Compliant

### Host Protocols

Protocol	Layer
icmp	Transport
tcp	Transport
udp	Transport
IP	Network

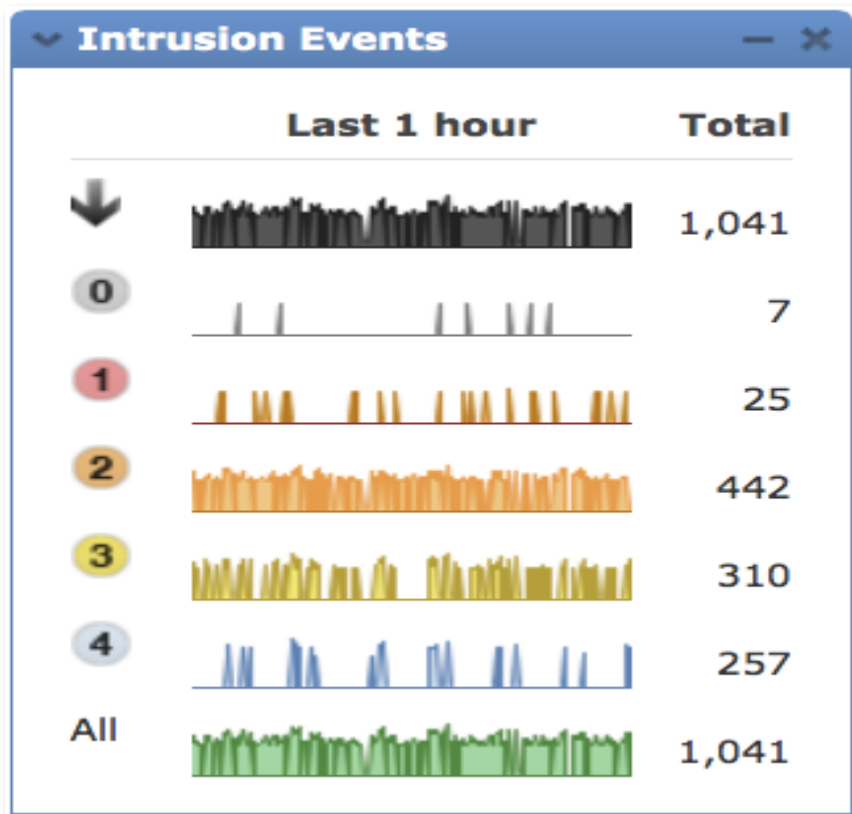
## White List Violations (34)

## Most Recent Malware Detections (4)

## Vulnerabilities (1522)

Name	Remote	Component	Port
<a href="#">4D WebStar Symbolic Link Vulnerability</a>		Windows 2000, XP, Server 2003, Vista, 7, Server 2008	
<a href="#">A certain ActiveX control in the Indexing Service in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 does not properly process URLs, which allows remote attackers to execute arbitrary programs via unspecified vectors that cause a "vulnerable"</a>		Windows 2000, XP, Server 2003, Vista, 7, Server 2008	
<a href="#">Acer LunchApp.APlunch ActiveX Control Remote Code Execution Vulnerability</a>	Yes	Internet Explorer 6.0	

# Impact Assessment - Identify Where to Start



If this is all there was then the “Order of Investigation” is easy.

From the FMC Dashboard

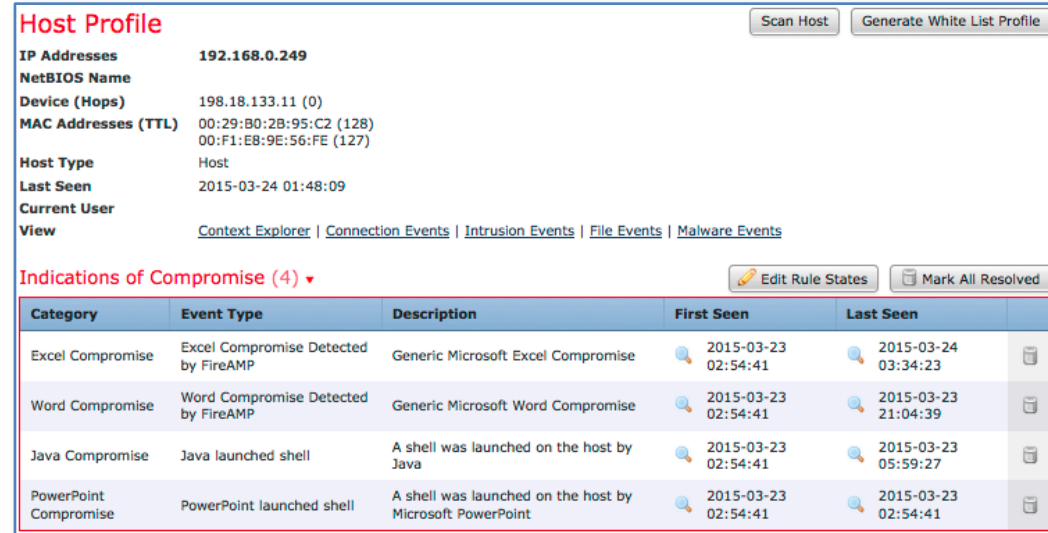
# Indications of Compromise

Leverages correlation of multiple event types, such as:

- Impact 1 & 2 events
  - CNC connection events (IPS)
  - Compromise events (IPS)
- Security Intelligence Events
- AMP for Endpoint Events
- AMP for Network
  - Includes some file events
- Built in Cisco correlation rules

Goal:

1. What needs to be fixed now!
2. Have enough data to know what can be prevented in the future.

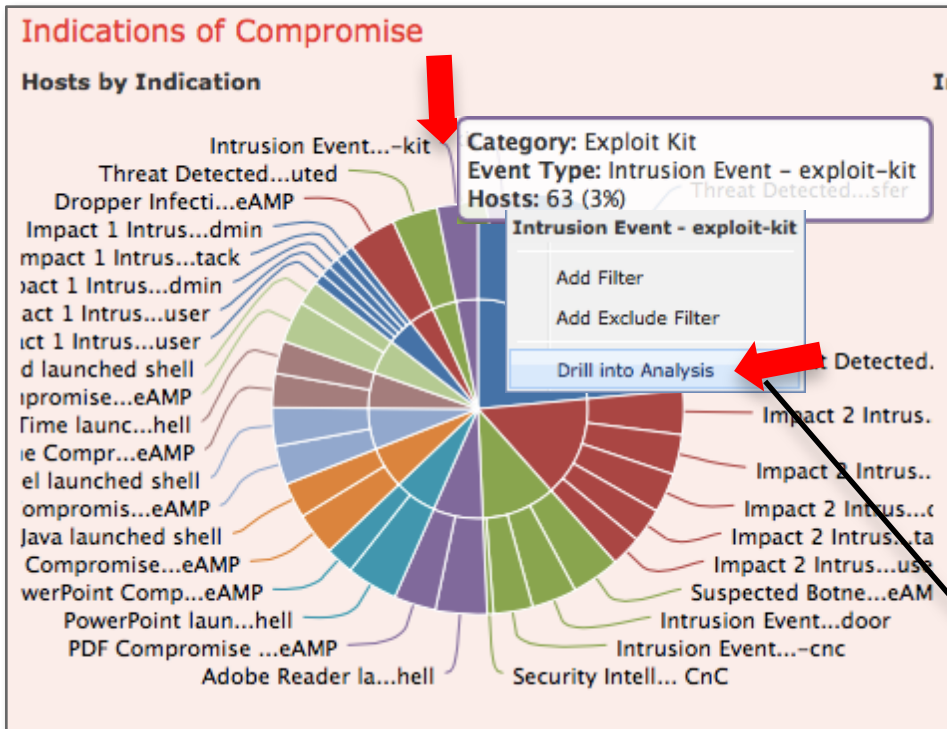


The screenshot displays a 'Host Profile' interface for IP address 192.168.0.249. It includes fields for NetBIOS Name, Device (Hops), MAC Addresses (TTL), Host Type, Last Seen, and Current User. Below this, there is a section titled 'Indications of Compromise (4)' which contains a table of events.

Category	Event Type	Description	First Seen	Last Seen
Excel Compromise	Excel Compromise Detected by FireAMP	Generic Microsoft Excel Compromise	2015-03-23 02:54:41	2015-03-24 03:34:23
Word Compromise	Word Compromise Detected by FireAMP	Generic Microsoft Word Compromise	2015-03-23 02:54:41	2015-03-23 21:04:39
Java Compromise	Java launched shell	A shell was launched on the host by Java	2015-03-23 02:54:41	2015-03-23 05:59:27
PowerPoint Compromise	PowerPoint launched shell	A shell was launched on the host by Microsoft PowerPoint	2015-03-23 02:54:41	2015-03-23 02:54:41



# What too many networks look like



From the FMC Context Explorer

Some ways to choose

- Look for Malware Executed (Endpoint AMP)
- Dropper Infection (Endpoint AMP)
- Threat detected in file transfer
- CNC Connected Events
- Shell Code Executed
- Impact 1 (these were probably blocked)
- Impact 2 (these were probably blocked)

Let's see what these 63 events are all about.

# Drilling into the IOC

## Indications of Compromise (switch workflow)

[Indications of Compromise Summary](#) > [Indications of Compromise Details](#) > [Table View of Indications of Compromise](#) > [Hosts](#)

▶ Search Constraints ([Edit Search](#) [Save Search](#))

Jump to... ▼

<input type="checkbox"/>	Category	Count
↓ <input type="checkbox"/>	<a href="#">Exploit Kit</a>	76

Displaying row 1 of 1 rows |<< Page 1 of 1 >>|



Busy event. Looks like we're getting more.



















# Digging into the IOC

## Indications of Compromise (switch workflow)

[Indications of Compromise Summary](#) > [Indications of Compromise Details](#) > **[Table View of Indications of Compromise](#)** > [Hosts](#)

► Search Constraints ([Edit Search](#) [Save Search](#))

Jump to... ▼

<input type="checkbox"/>	<a href="#">IP Address</a> ×	<a href="#">Category</a> ×	<a href="#">Event Type</a> ×	<a href="#">Description</a> ×	<a href="#">First Seen</a> ×	<a href="#">Last Seen</a> ×
<input type="checkbox"/>	 <a href="#">10.0.231.56</a>	<a href="#">Exploit Kit</a>	<a href="#">Intrusion Event - exploit-kit</a>	<a href="#">The host may have encountered an exploit kit</a>	 <a href="#">2015-10-01 13:04:50</a>	 <a href="#">2015-10-01 18:46:59</a>
<input type="checkbox"/>	 <a href="#">10.0.164.115</a>	<a href="#">Exploit Kit</a>	<a href="#">Intrusion Event - exploit-kit</a>	<a href="#">The host may have encountered an exploit kit</a>	 <a href="#">2015-10-01 13:04:50</a>	 <a href="#">2015-10-01 18:46:59</a>
<input type="checkbox"/>	 <a href="#">10.131.12.147</a>	<a href="#">Exploit Kit</a>	<a href="#">Intrusion Event - exploit-kit</a>	<a href="#">The host may have encountered an exploit kit</a>	 <a href="#">2015-10-01 13:01:47</a>	 <a href="#">2015-10-01 17:45:44</a>
<input type="checkbox"/>	 <a href="#">10.0.112.107</a>	<a href="#">Exploit Kit</a>	<a href="#">Intrusion Event - exploit-kit</a>	<a href="#">The host may have encountered an exploit kit</a>	 <a href="#">2015-10-01 13:01:47</a>	 <a href="#">2015-10-01 17:45:44</a>
<input type="checkbox"/>	 <a href="#">10.0.192.78</a>	<a href="#">Exploit Kit</a>	<a href="#">Intrusion Event - exploit-kit</a>	<a href="#">The host may have encountered an exploit kit</a>	 <a href="#">2015-10-01 13:36:53</a>	 <a href="#">2015-10-01 16:47:03</a>
<input type="checkbox"/>	 <a href="#">10.200.1.74</a>	<a href="#">Exploit Kit</a>	<a href="#">Intrusion Event - exploit-kit</a>	<a href="#">The host may have encountered an exploit kit</a>	 <a href="#">2015-10-01 14:04:36</a>	 <a href="#">2015-10-01 16:10:25</a>

Seems active across 6 hosts. Let's drill into one.

## Host Profile

[Scan Host](#)[Generate White List Profile](#)

**IP Addresses** 10.131.12.147

**NetBIOS Name**

**Device (Hops)** 198.18.133.11 (0)

**MAC Addresses (TTL)** 00:11:22:33:44:55 (CIMSYS Inc) (64)  
00:55:44:33:22:11 (64)

**Host Type** Host

**Last Seen** 2015-10-01 17:45:45

**Current User** Kim Ralls (kralls, LDAP)

**View** [Context Explorer](#) | [Connection Events](#) | [Intrusion Events](#) | [File Events](#) | [Malware Events](#)



Looks like Kim Ralls has a lot going on her Windows host.

## Indications of Compromise (4) ▾

[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	2015-10-01 13:01:47	2015-10-01 17:45:44	
Dropper Infection	Dropper Infection Detected by FireAMP	The host may be infected with Dropper	2015-10-01 13:52:10	2015-10-01 14:48:06	
Malware Detected	Threat Detected in File Transfer	The host has encountered malware	2015-10-01 13:52:10	2015-10-01 14:37:48	
CnC Connected	Intrusion Event - malware-backdoor	The host may be under remote control	2015-10-01 13:35:17	2015-10-01 13:52:10	



Events from multiple sources:

- IPS Engine
- File Protection
- AMP for Networks

## Operating System ▾

[Edit Operating System](#)

	Vendor	Product	Version	Source
	Microsoft	Windows	Vista, 7	FireSIGHT

## Servers (1) ▾

	Protocol	Port	Application Protocol	Vendor and Version	
	tcp	80	pending		

## Applications (1) ▾

	Application Protocol	Client	Version	Web Application	
	HTTP	Firefox	2.0.0.17	Web Browsing	

# Events By Priority and Classification

**Rule Documentation (1:15306:22)**

This rule generates events when a portable executable file is downloaded.

Search Constraints (Edit Search Save Search)  
 Source / Destination IP 10.131.12.1

19:08:00 - 2015-10-01 19:08:00  
 Static

# Events By Priority and Classification (switch workflow)

Search Constraints (Edit Search Save Search)

2015-09-30 19:08:00 - 2015-10-01 19:08:00  
 Static  
 Disabled Columns

Jump to... ▾

<input type="checkbox"/>	Time ×	Priority ×	Impact ×	Inline Result ×	Source IP ×	Source Country ×	Destination IP ×	Destination Country ×	Source Port / ICMP Type ×	Destination Port / ICMP Code ×	SSL Status ×
▾ <input type="checkbox"/>	2015-10-01 17:45:44	high	4	↓	10.131.12.147		10.120.10.194		80 (http) / tcp	22737 / tcp	Unknown (Unknown)
▾ <input type="checkbox"/>	2015-10-01 17:45:44	high	4	↓	10.0.112.107		10.131.12.147		80 (http) / tcp	25234 / tcp	Unknown (Unknown)
▾ <input type="checkbox"/>	2015-10-01 17:45:44	high	4	↓	10.131.12.147		172.16.0.194		80 (http) / tcp	20215 / tcp	Unknown (Unknown)
▾ <input type="checkbox"/>	2015-10-01 17:45:44	high	4	↓	10.131.12.147		10.120.10.19		80 (http) / tcp	18266 / tcp	Unknown (Unknown)
▾ <input type="checkbox"/>	2015-10-01 13:52:10	high	4	↓	10.131.12.147		10.120.10.194		80 (http) / tcp	22737 / tcp	Unknown (Unknown)
▾ <input type="checkbox"/>	2015-10-01 13:52:10	high	4	↓	10.131.12.147		10.120.10.19		80 (http) / tcp	18266 / tcp	Unknown (Unknown)

<< Page 1 of 1 >> | Displaying rows 1-6 of 6 rows

**False Negatives** None known.

**Corrective Action** NA

**Contributors** Sourcefire Vulnerability Research Team

**References**

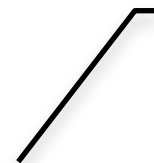
**View** [Context Explorer](#)

- .145 Tried to send the file 5 times
- .145 was sent the file once
- IPS blocked it! (yeah)
- What does Impact 4 mean?
- Should we investigate more?

## Host Profile

[Scan Host](#)[Generate White List Profile](#)

**IP Addresses** 10.131.12.147  
**NetBIOS Name**  
**Device (Hops)** 198.18.133.11 (0)  
**MAC Addresses (TTL)** 00:11:22:33:44:55 (CIMSYS Inc) (64)  
00:55:44:33:22:11 (64)  
**Host Type** Host  
**Last Seen** 2015-10-01 17:45:45  
**Current User** Kim Ralls (kralls, LDAP)  
**View** [Context Explorer](#) | [Connection Events](#) | [Intrusion Events](#) | [File Events](#) | [Malware Events](#)



Did you forget about these?

Let's see if that file moved around without the IPS seeing it.

## Indications of Compromise (4) ▾

[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	2015-10-01 13:01:47	2015-10-01 17:45:44	
Dropper Infection	Dropper Infection Detected by FireAMP	The host may be infected with Dropper	2015-10-01 13:52:10	2015-10-01 14:48:06	
Malware Detected	Threat Detected in File Transfer	The host has encountered malware	2015-10-01 13:52:10	2015-10-01 14:37:48	
CnC Connected	Intrusion Event - malware-backdoor	The host may be under remote control	2015-10-01 13:35:17	2015-10-01 13:52:10	



## Operating System ▾

[Edit Operating System](#)

	Vendor	Product	Version	Source
	Microsoft	Windows	Vista, 7	FireSIGHT

## Servers (1) ▾

	Protocol	Port	Application Protocol	Vendor and Version	
	tcp	80	pending		

## Applications (1) ▾

	Application Protocol	Client	Version	Web Application	
	HTTP	Firefox	2.0.0.17	Web Browsing	

## File Summary [\(switch workflow\)](#)

[File Summary](#) > [Table View of File Events](#)

2015-09-30 19:08:00 - 2015-10-01 19:08:00

Static

▼ Search Constraints ([Edit Search](#) [Save Search](#))

[Sending /](#)  
[Receiving IP](#) 10.131.12.147

Jump to... ▼

<input type="checkbox"/>	Category	Type	Disposition	Action	Count
↓ <input type="checkbox"/>	Executables	MSEXE	Malware	<a href="#">Malware Cloud Lookup</a>	1

||<< Page  of 1 >>| Displaying row 1 of 1 rows

Yep. That file is malware

## Malware Summary [\(switch workflow\)](#)

[Malware Summary](#) > [Table View of Malware Events](#)

2015-09-30 19:08:00 - 2015-10-01 19:08:00

Static

▼ Search Constraints ([Edit Search](#) [Save Search](#))

[Sending /](#)  
[Receiving IP](#) 10.131.12.147

Jump to... ▼

<input type="checkbox"/>	Threat Name	File Name	File SHA256	File Type	Count
↓ <input type="checkbox"/>	Packed_NSPack:Bifrose-tpd	Hiloti.exe	24a4a681...e4193696	MSEXE	1

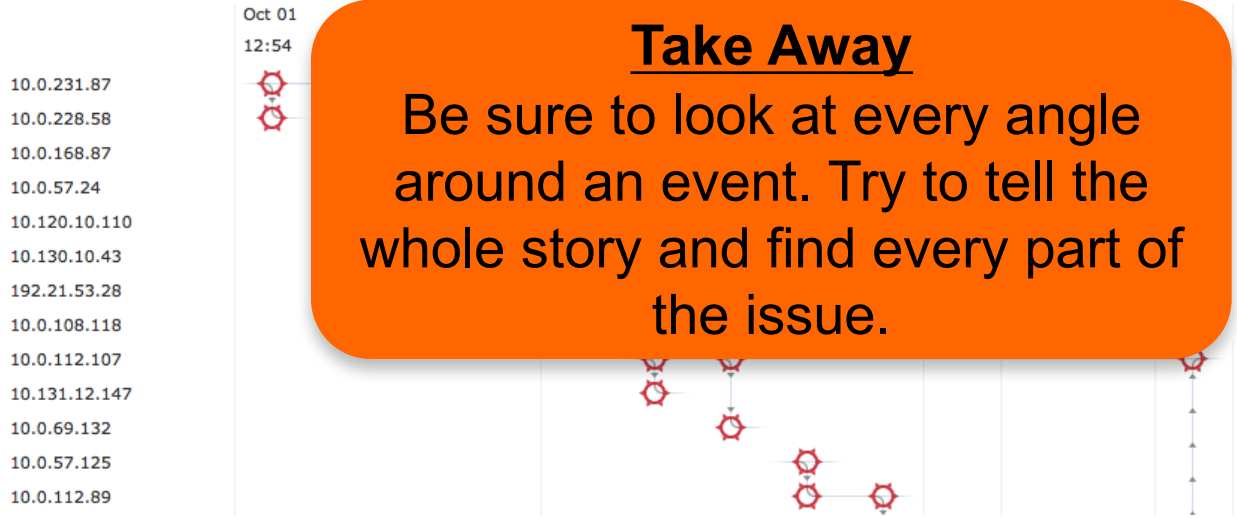
||<< Page  of 1 >>| Displaying row 1 of 1 rows

We see it in the malware summary, too.

## Network File Trajectory for 24a4a681...e4193696

<b>File SHA256</b>	24a4a681...e4193696	<b>First Seen</b>	2015-10-01 12:54:30 on <a href="#">10.0.231.87</a>
<b>File Names</b>	<a href="#">Babonock.exe</a> , <a href="#">Bubnix.exe</a> , <a href="#">Corripio.exe</a> , <a href="#">FakeVimes.exe</a> (+8 more)	<b>Last Seen</b>	2015-10-01 17:45:45 on <a href="#">10.0.112.107</a>
<b>File Type</b>	MSEXE	<b>Event Count</b>	13
<b>File Category</b>	<a href="#">Executables</a>	<b>Seen On</b>	19 hosts
<b>Current Disposition</b>	<a href="#">Malware</a>	<b>Seen On Breakdown</b>	10 senders → 12 receivers
<b>Threat Score</b>	●●●● Very High		
<b>Threat Name</b>	Packed_NSpack:Bifrose-tpd		

### Trajectory



**Take Away**  
Be sure to look at every angle around an event. Try to tell the whole story and find every part of the issue.

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

**Dispositions** Unknown Malware Clean Custom Unavailable

- A lot more than the 6 file transfers and hosts the IPS engine stopped.
- Good thing they have AMP for Endpoints, too.
- Bet they wished they enabled quarantining.
- Problem scoped. Time to remediate.
- Maybe a good time to look at file analysis / Threatgrid to learn what other artifacts are left behind.



# Security Automation is more than just Operations



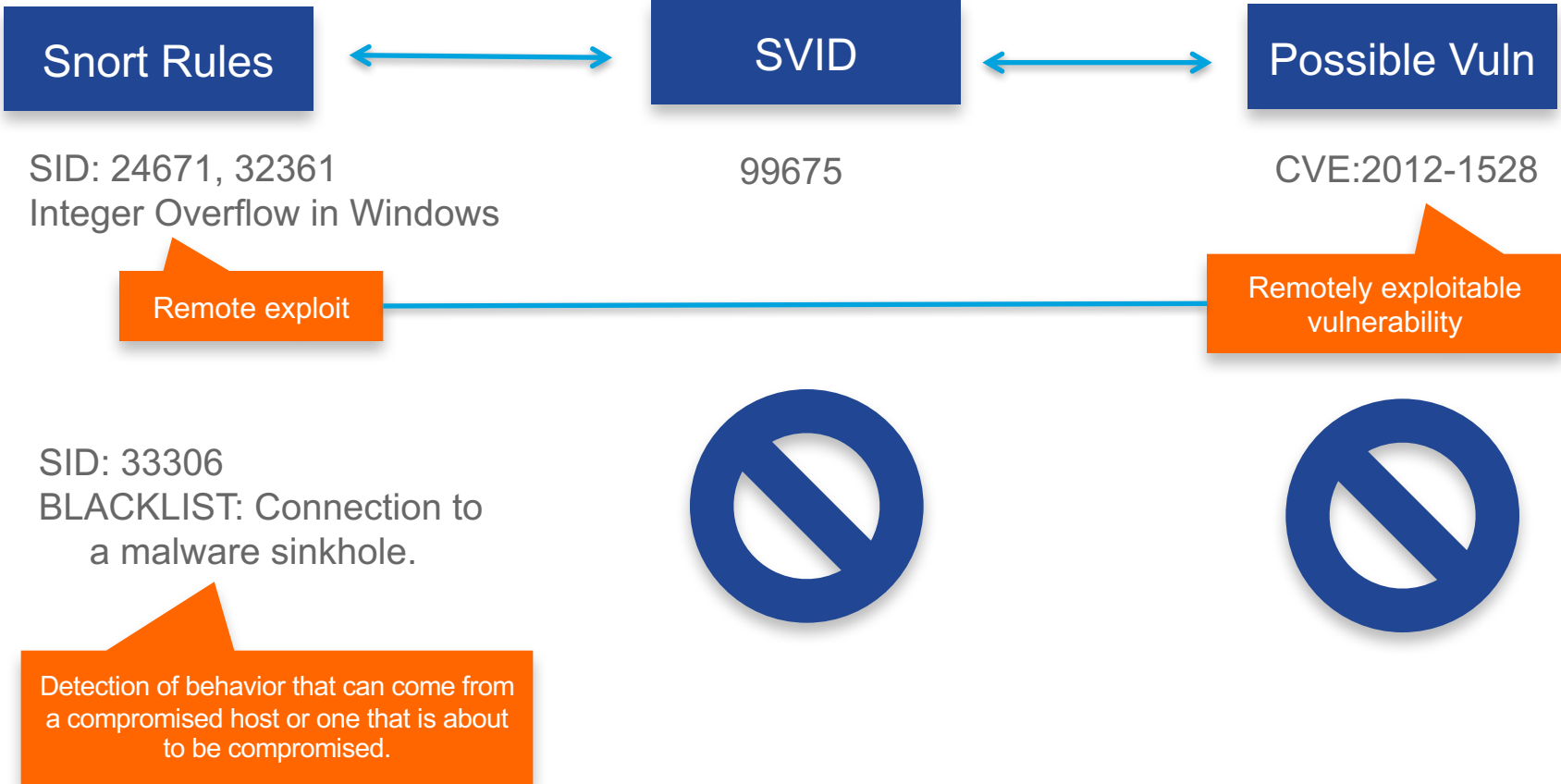
Impact Analysis  
Indications of Compromise  
Correlation Rules

Reporting  
Correlation Rules  
Remediation API



Firesight Recommendations  
Rule Updates  
VDB Updates  
Software Updates  
Policy Updates

# Recommended Rules – How it works



# Recommended Rules – the details

```
alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"BROWSER-IE
ActiveX installer broker object sandbox escape attempt"; flow:to_server,established;
flowbits:isset,file.exe; file_data; content:"|55 8B EC 6A FF 68 A8 31 01 10 64 A1 00 00
00 00 50 83 EC 0C A1 20 B0 01 10 33 C5 89 45 F0 56 50|"; fast_pattern:only;
metadata:policy balanced-ips drop, policy security-ips drop, service smtp;
reference:cve,2014-4123; reference:url,technet.microsoft.com/en-
us/security/bulletin/ms14-056; classtype:attempted-user; sid:32265; rev:1; )
```

Rule that will map to Recommended Rules

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"BLACKLIST Connection to
malware sinkhole"; flow:to_client,established; dsize:22; content:"Sinkholed by
abuse.ch|0A|"; fast_pattern:only; metadata:impact_flag red, policy balanced-ips drop, policy
security-ips drop, service http; reference:url,en.wikipedia.org/wiki/Sinkhole_Server;
classtype:trojan-activity; sid:33306; rev:1; )
```

Some rules will ALWAYS be turned off by Recommended Rules

WF-IPS (2015-08-27 01:09:33 by admin)		
Rules	Event	Action
INDICATOR-COMPROMISE Keylog string over FTP detected (1:31711)	Drop and generate events	Drop and generate events
INDICATOR-COMPROMISE known malicious SSL certificate - Win.Trojan.D	Drop and generate events	Drop and generate events
INDICATOR-COMPROMISE LizardM php shell download attempt (1:31503)	Drop and generate events	Drop and generate events
INDICATOR-COMPROMISE Windows Internet Explorer EMET check and gar	Drop and generate events	Drop and generate events
INDICATOR-OBFUSSATION DOC header followed by PDF header (1:25458)	Drop and generate events	Drop and generate events
INDICATOR-OBFUSSATION GIF header followed by PDF header (1:25455)	Drop and generate events	Drop and generate events
INDICATOR-OBFUSSATION Javascript stealth executable download attempt	Drop and generate events	Drop and generate events
INDICATOR-OBFUSSATION JPEG header followed by PDF header (1:25457)	Drop and generate events	Drop and generate events
INDICATOR-OBFUSSATION Multiple character encodings detected (1:2951)	Drop and generate events	Drop and generate events
INDICATOR-OBFUSSATION PNG header followed by PDF header (1:25456)	Drop and generate events	Drop and generate events

WF-IPS (2015-08-28 07:04:08 by admin)		
Rules	Event	Action
INDICATOR-COMPROMISE Keylog string over FTP detected (1:31711)	Disabled	Disabled
INDICATOR-COMPROMISE known malicious SSL certificate - Win.Trojan.D	Disabled	Disabled
INDICATOR-COMPROMISE LizardM php shell download attempt (1:31503)	Disabled	Disabled
INDICATOR-COMPROMISE Windows Internet Explorer EMET check and gar	Disabled	Disabled
INDICATOR-OBFUSSATION DOC header followed by PDF header (1:25458)	Disabled	Disabled
INDICATOR-OBFUSSATION GIF header followed by PDF header (1:25455)	Disabled	Disabled
INDICATOR-OBFUSSATION Javascript stealth executable download attempt	Disabled	Disabled
INDICATOR-OBFUSSATION JPEG header followed by PDF header (1:25457)	Disabled	Disabled
INDICATOR-OBFUSSATION Multiple character encodings detected (1:2951)	Disabled	Disabled
INDICATOR-OBFUSSATION PNG header followed by PDF header (1:25456)	Disabled	Disabled

Rules disabling by default

# Correlation Rules

# Correlation Rules / Correlation Policy

**Rule Information**

Rule Name: Critical phone Attacks **100,000 events**

Rule Description: Attacks on Executives Android-based phones

Rule Group:

Select the type of event to generate:

If an intrusion event is detected:

- AND
- Destination Host is Jailbroken is Yes

Host Profile Correlation

Only generate an event if the host has the following properties:

- OS Vendor is Google
- OS Name is Android
- OS Version is any

User Identity Qualification

Only generate an event if the user(s) involved have the following properties:

- Identity on Destination Department is Executives

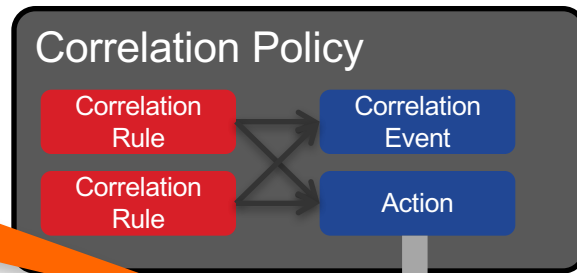
**10 events**

Value:

- Automate Security Decisions
- Track Business Outcome
- Trigger Automated Response to specific conditions

**3 Events**

Correlation Rules allow for BOOLEAN decisions on one or more sets of data within the FireSIGHT console. These rules can then lead to Actions such as Email, Syslog, SNMP events or Remediation actions.




# Correlating Event Data


Flow and connection conditions over time or volume.


Data from User Table (name, group info, etc)




Data from Host Profiles

When a...

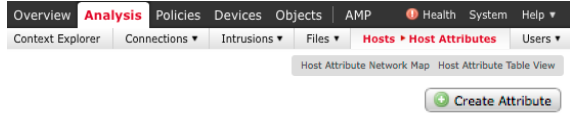
 Add Connection Tracker

 Add User Qualification

 Add Host Profile Qualification

	 Add Connection Tracker	 Add User Qualification	 Add Host Profile Qualification
<b>Intrusion Event</b>	✓	✓	✓
<b>Discovery Event</b>	✓	✓	✓
<b>Connection Event</b>	✓	✓	✓
<b>Host Input Event</b>	✓	✓	✓
<b>User Activity Occurs</b>	✓		✓
<b>Traffic Profile Changes</b>			
<b>Malware Event</b>			

# Correlation Rules – Leveraging Host Attributes



### Create Host Attribute

Name: <Custom Host Attribute>

Type:

- Text
- Integer
- List
- URL

Save Cancel

### Edit Host Attribute

Name: Location

Type: List

List Values

Name
Lab
Management
Production
POS
PCI
Guest

Auto-Assign Networks

Value	IP Address	Netmask
Lab	192.168.3.0	24
Management	192.168.1.0	24
Production	192.168.2.0	26
POS	192.168.2.64	26
PCI	192.168.2.128	26
Guest	192.168.4.0	24

Save Cancel

### Host Profile

Scan Host Generate White List Profile

**IP Addresses** 192.168.3.3 (esxi)  
**NetBIOS Name**  
**Device (Hops)** 192.168.1.9 (0)  
192.168.1.16 (0)  
**MAC Addresses (TTL)** F0:7F:06:45:7A:52 (Cisco) (64)  
00:18:0A:45:43:86 (Meraki, Inc.) (64)  
**Host Type** Host  
**Last Seen** 2015-09-21 21:25:57  
**Current User**  
**View** Context Explorer | Connection Events | Intrusion Events | File Events | Malware Events

**Indications of Compromise (0)** Edit Rule States

**Operating System** Edit Operating System

**Servers (2)**

Protocol	Port	Application Protocol	Vendor and Version
tcp	902	<input type="checkbox"/> VNC	
tcp	443	<input type="checkbox"/> HTTPS	

**Users (no user history available)**

**Attributes** Edit Attributes

**Host Criticality** None  
**Location** Lab

**VLAN Tag**

**Host Protocols**

## Host Attributes:

- Localization of Host Profile information
- Multiple Data Types
- Can be modified via FMC or Host Input API
- Can be leveraged in Correlation Rules

# Enable automated scanning of new hosts

As new IP addresses appear on the network, Firepower Correlation Policies can trigger Nmap to perform an active scan of the new hosts.

The screenshot shows the 'Policies' section of the Firepower Correlation interface. The 'Rule Management' tab is active, displaying the configuration for a rule named 'COND-nmap-new-IP'. The rule description is 'scan a new IP address for more accurate host profile' and it is in the 'Ungrouped' group. The trigger is set to 'If a discovery event occurs a new IP host is detected and it meets the following conditions:'. Two conditions are listed: 'IP Address is in 192.168.22.0/24' and 'IP Address is in 91.82.94.176/28'. The 'Rule Options' section shows a snooze time of 0 hours and no inactive periods defined.

Overview Analysis **Policies** Devices Objects AMP

Access Control ▾ Network Discovery Application Detectors **Correlation** Actions ▾

Policy Management **Rule Management** White List Traffic Profiles

### Rule Information

Rule Name: COND-nmap-new-IP

Rule Description: scan a new IP address for more accurate host profile

Rule Group: Ungrouped

Select the type of event for this rule

If a discovery event occurs a new IP host is detected and it meets the following conditions:

+ Add condition + Add complex condition

OR

- IP Address is in 192.168.22.0/24
- IP Address is in 91.82.94.176/28

### Rule Options

Snooze: If this rule generates an event, snooze for 0 hours

Inactive Periods: There are no defined inactive periods. To add an inactive period, click "Add Inactive Period".



# Action example: NMAP Scan

## Edit Remediation

Remediation Name

REMIATION-NMAP

Remediation Type

Nmap Scan

Description

Scan Which Address(es) From Event?

Scan Source and Destination Addresses

Scan Type

TCP Connect Scan

Scan for UDP ports

On  Off

Use Port From Event

On  Off

Scan from reporting device

On  Off

Fast Port Scan

On  Off

Port Ranges and Scan Order (blank for Nmap defaults)

Probe open ports for vendor and version information

On  Off

Service Version Intensity

7

Detect Operating System

On  Off

Treat All Hosts As Online

On  Off

Host Discovery Method

TCP SYN

Host Discovery Port List (advanced option)

Default NSE scripts

On  Off

Timing Template (Higher Is Faster)

3

Create

Cancel

# Correlation Rule – Putting it together

Overview Analysis **Policies** Devices Objects AMP Deploy 3 System Help **scordas**

Access Control Network Discovery Application Detectors **Correlation** Actions

Alerts Remediations Groups

**Policy Management** Rule Management White List Traffic Profiles

**Correlation Policy Information** Save Cancel

Policy Name

Policy Description

Default Priority

**Policy Rules** Add Rules

Rule	Responses	Priority
<b>COND-nmap-new-IP</b> scan a new IP address for more accurate host profile	REMEDIATION-NMAP (Remediation)	Default



Condition



Action

# Correlation Rule – A new IP pops UP in the management ZONE

## Correlation Events

[Correlation Events](#)

2016-11-11 22:59:00 - 2016-11-12 00:04:18

Expanding

Disabled Columns

Search Constraints ([Edit Search](#) [Save Search](#))

Jump to...

	Time	Source IP	Description	Policy	Rule	Priority	Source Host Criticality	
	2016-11-11 23:58:41	192.168.22.6	<*- New Host From "192.168.22.5" at Fri Nov 11 22:58:41 2016 UTC -*>	IP Address: 192.168.22.6 Host Type: Host	CORRELATION-Nmap	COND-nmap-new-IP	None	None

## Discovery Events

[Table View of Events](#) > Hosts

2016-11-11 22:59:00 - 2016-11-12 00:01:03

Expanding

Search Constraints ([Edit Search](#) [Save Search](#))

Jump to...

	Time	Event	IP Address	User	MAC Address	MAC Vendor	Port	Description	Device
	2016-11-12 00:00:45	Add Scan Result	192.168.22.6					Scanner Nmap; 192.168.22.6	guardian.budlab.net
	2016-11-12 00:00:44	Set Operating System Definition	192.168.22.6		00:0C:29:0C:BF:68	VMware, Inc.		Scanner Nmap; Juniper, embedded, (null)	guardian.budlab.net
	2016-11-11 23:58:41	DHCP: IP Address Changed	192.168.22.6		00:0C:29:0C:BF:68	VMware, Inc.		Merged Hosts	192.168.22.5
	2016-11-11 23:58:41	New Transport Protocol	192.168.22.6		00:0C:29:0C:BF:68	VMware, Inc.	tcp		192.168.22.5
	2016-11-11 23:58:41	New Network Protocol	192.168.22.6		00:0C:29:0C:BF:68	VMware, Inc.	IP		192.168.22.5
	2016-11-11 23:58:41	New OS	192.168.22.6		00:0C:29:0C:BF:68	VMware, Inc.		OS unknown	192.168.22.5
	2016-11-11 23:58:41	New Host	192.168.22.6		00:0C:29:0C:BF:68	VMware, Inc.			192.168.22.5

# Building a Correlation Rule

## Correlation Rule to:

- Ensure only HTTPS traffic is used on port 443
- Ensure traffic is initiated by a Host with a defined Location (host Attribute) is POS
- Ensure the HTTPS traffic from the POS host is received on hosts in the PCI network.
- Any traffic outside this profile will generate an event.

The screenshot displays the 'Rule Management' tab in the Cisco Policy Management console. The rule is named 'Unauthorized POS Traffic' and is currently ungrouped. The configuration is as follows:

- Rule Information:** Rule Name: Unauthorized POS Traffic; Rule Description: (empty); Rule Group: Ungrouped.
- Select the type of event for this rule:** If a connection event occurs at either the beginning or the end of the connection and it meets the following conditions:
  - Application Protocol is not HTTPS
  - Responder Port / ICMP Code is not 443
- Host Profile Qualification:** Only generate an event if the host(s) involved have the following properties:
  - Initiator Host Location is POS
  - Responder Host Location is not PCI
- Rule Options:** Snooze: If this rule generates an event, snooze for 0 hours; Inactive Periods: There are no defined inactive periods.

# Correlation Rule example: Production Network Change

The screenshot displays the 'Rule Management' section of the Cisco Policy Management interface. The rule is named 'Production Changes' and is currently ungrouped. The event type is set to 'a discovery event occurs'. A dropdown menu is open, showing a list of event types. A red arrow points to the option 'a new IP host is detected'.

**Rule Information**

- Rule Name: Production Changes
- Rule Description: [Empty]
- Rule Group: Ungrouped

**Select the type of event for this rule**

If a discovery event occurs and it meets the following conditions:

- + Add condition
- X [Empty]

**Rule Options**

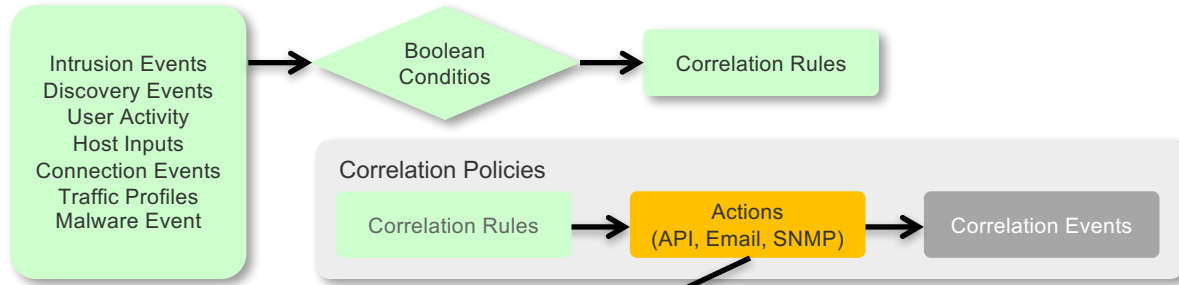
- Snooze: If this rule [Empty]
- Inactive Periods: There are [Empty]
- + Add Inactive Period
- Save Cancel

**Event Type List (from dropdown):**

- a client has changed
- a client timed out
- a host ip address is reused
- a host is deleted because the host limit was reached
- a host is identified as a network device
- a host timed out
- a host's IP address has changed
- an IOC was set
- a NETBIOS name change is detected
- a new client is detected
- a new IP host is detected**
- a new MAC address is detected
- a new MAC host is detected
- a new network protocol is detected
- a new transport protocol is detected
- an open TCP port is detected
- an open UDP port is detected
- the OS information for a host has changed
- the OS or server identity for a host has a conflict
- the OS or server identity for a host has timed out
- a TCP port closed
- a TCP port timed out
- there is any type of event
- there is new information about a MAC address
- there is new information about a TCP server
- there is new information about a UDP server
- a UDP port closed
- a UDP port timed out
- a VLAN tag was updated

# Remediation

# Automating Response – Remediation API



## Sample Remediation Modules

- Cisco ISE – FIRE & ISE
- Guidance Encase
- Set Host Attributes
- Security Intelligence Blacklisting
- Nmap Scan
- SSH / Expect Scripts
- F5 iRules
- Solera DeepSee
- Netscaler
- PacketFence
- Bradford















# Remediation Modules

Overview Analysis **Policies** Devices Objects AMP Health System Help **admin**

Access Control Intrusion **Files** Network Discovery SSL Application Detectors Users Correlation **Actions ▶ Modules**

Alerts Remediations Groups

## Installed Remediation Modules

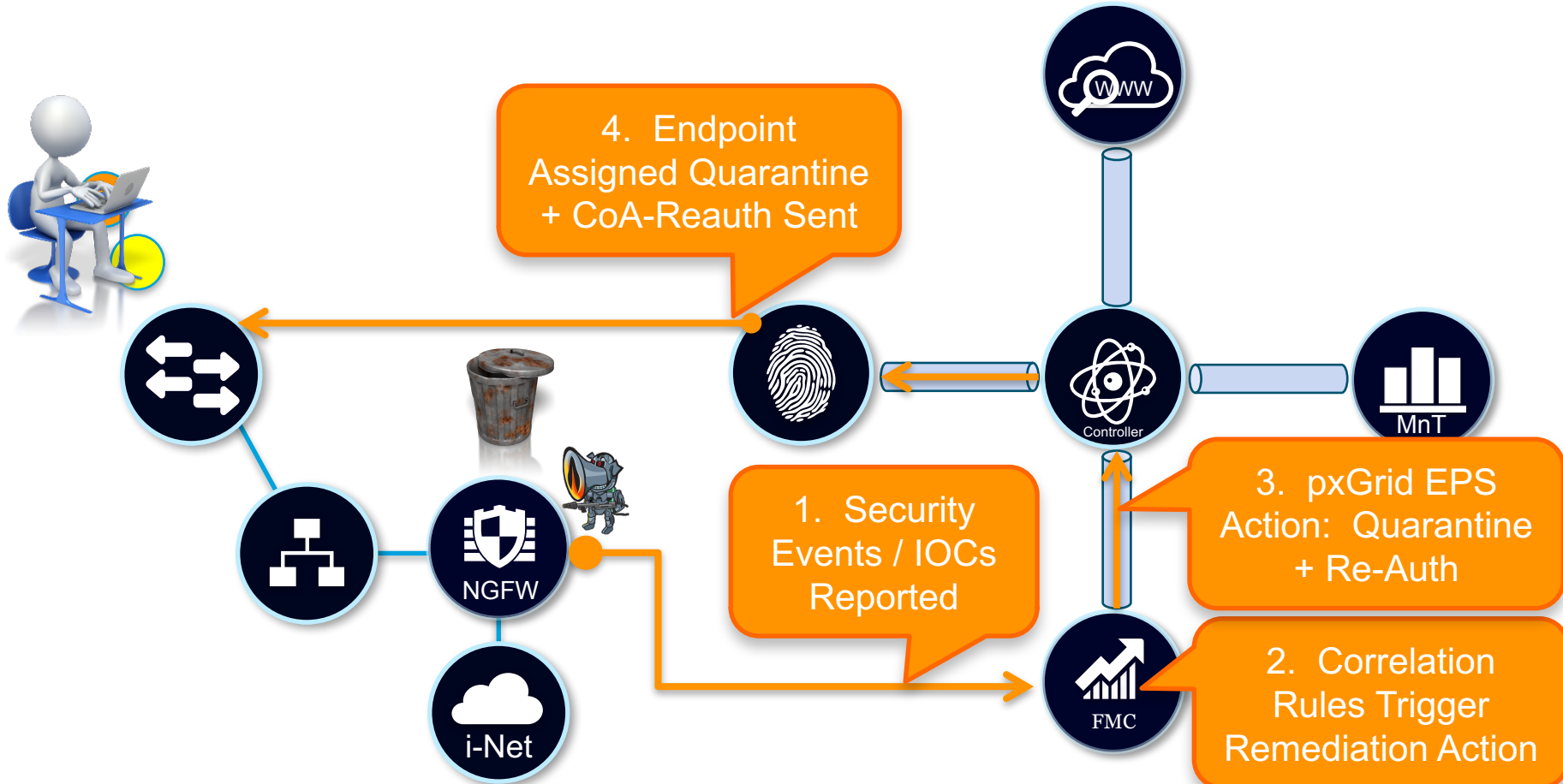
Module Name	Version	Description	
Blacklist IP	1.0	Add an IP Address to a feed used as a blacklist	 
Cisco IOS Null Route	1.0	Block an IP address in a Cisco IOS router	 
Cisco PIX Shun	1.1	Shun an IP address in the PIX firewall	 
ISE 1.2 Remediation	1.3.19	Quarantine IP addresses using Identity Services Engine 1.2	 
Nmap Remediation	2.0	Perform an Nmap Scan	 
Set Attribute Value	1.0	Set an Attribute Value	 

**Install a new module**

no file selected



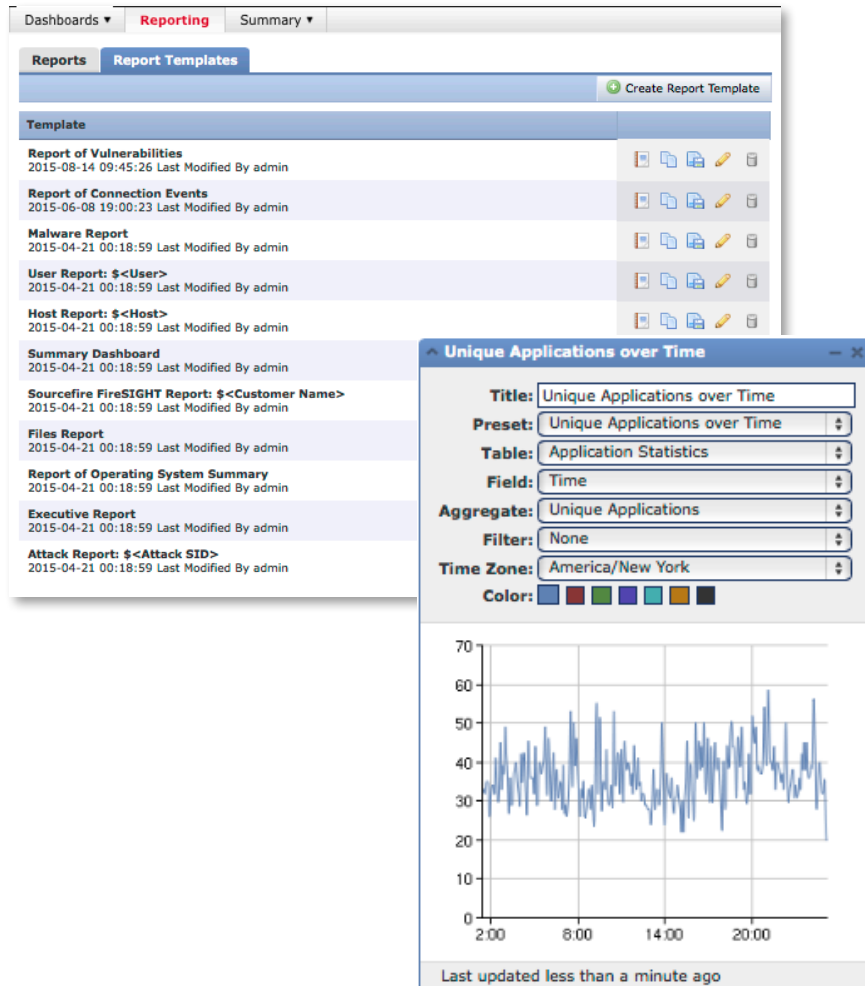
# ISE + Firepower = Rapid Threat Containment



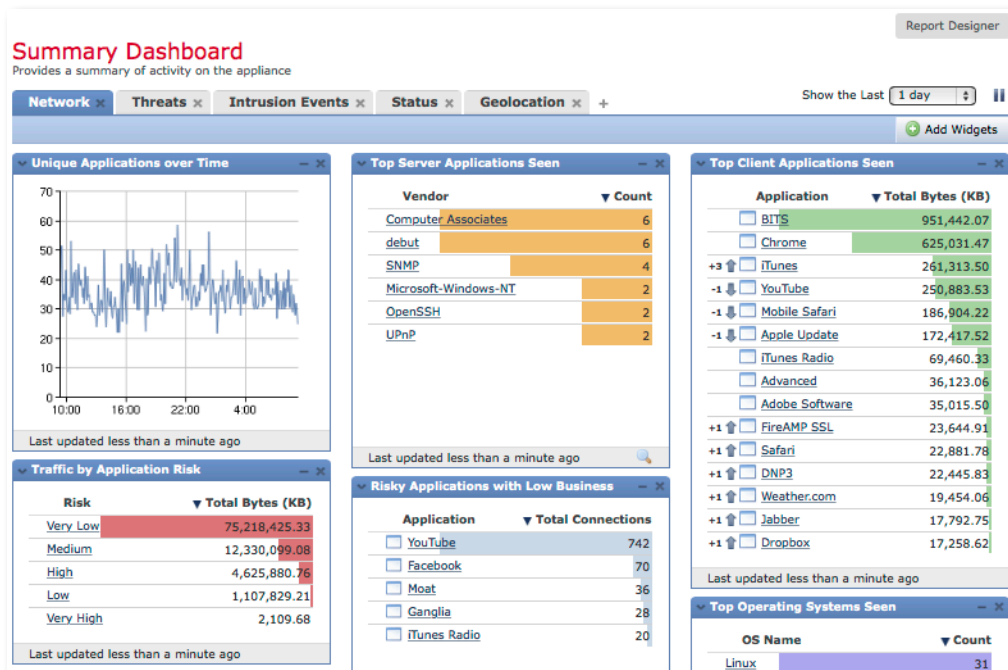
# Reporting

# Default Reports

- Not just what's in the templates
- Dashboard widgets have almost 120 preset reports
- Customizing Widgets means thousands of reporting options.
- Think of the Dashboard as your report designer.
- Tools:
  - Searches
  - Custom Workflows
  - Custom Tables = Data goldmine



# Customize The Dashboard



- There are a number of default dashboards
- All of them have customizable widgets
- Create / Customize your own for better visibility and report designs

# Customize The Dashboard

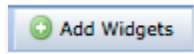
### Top Server Applications Seen

**Title:** Top Server Applications Seen  
**Preset:** Top Server Applications Seen  
**Table:** Servers  
**Field:** Vendor  
**Aggregate:** Count  
**Search:** Known Servers  
**Show:** Top  
**Results:** 10

**Show Movers:**   
**Color:**

Vendor	Count
Computer Associates	6
debut	6
SNMP	4
Microsoft-Windows-NT	2
OpenSSH	2
UPnP	2

Last updated 2 minutes ago

 Add Widgets

### Add Widgets

Summary Dashboard - Network

**Categories**

- All Categories (16)
  - Analysis & Reporting (5)
  - Miscellaneous (1)
  - Operations (10)

#### Appliance Information

This widget displays local appliance information including software versions, Remote Management, and High Availability status.

**Add**

#### Appliance Status

This widget displays the current Health Monitoring appliance status.

**Add**

#### Correlation Events

This widget displays Correlation events

**Add**

#### Current Interface Status

This widget displays the current status of all local network interfaces.

**Add**

#### Current Sessions

This widget displays a list of the user sessions currently logged-in to this appliance.

**Add**

#### Custom Analysis

The Custom Analysis widget shows the top or bottom set of events (5, 10, 15, 20, or 25 events) from a user-selectable event table, search, and field.

**Add**

10 on Tab

#### Disk Usage

This widget displays current disk

**Add**

This is your most powerful widget



# Dashboards That Meet Your Needs

Threat Focused

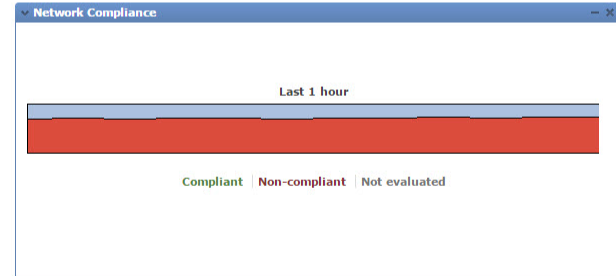
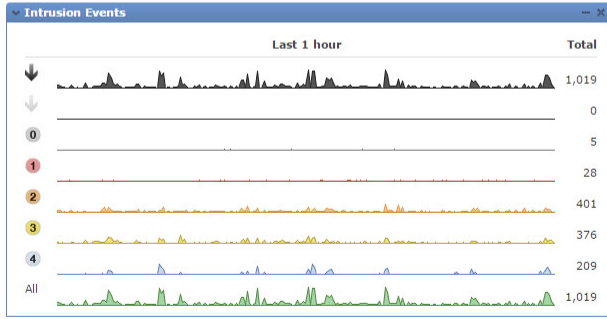
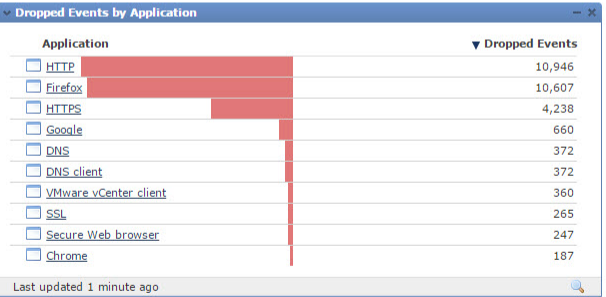
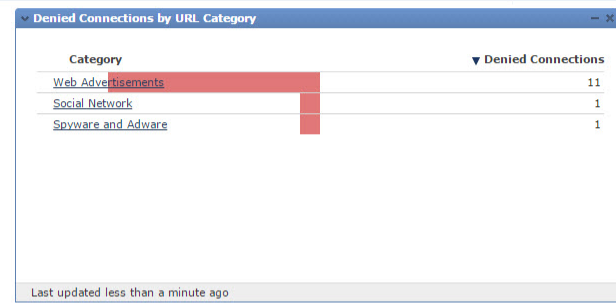
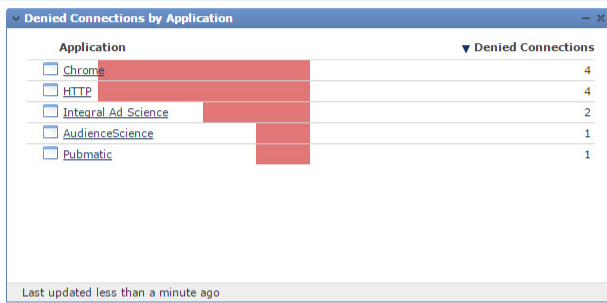
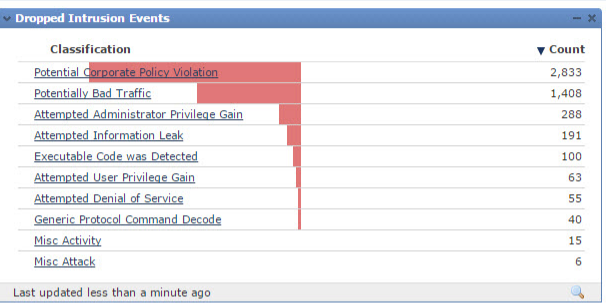
Report Designer

## Operation Flamethrower

Show the Last 1 hour

Add Widgets

Network Threat Blocked Status



# Dashboards That Meet Your Needs

Network Focused

Overview Analysis Policies Devices Objects AMP Health System Help admin

Dashboards Reporting Summary Report Designer

## Operation Flamethrower

Network Threat Blocked Status + Show the Last 1 hour Add Widgets

### Application Usage

Application	Total Bytes (KB)
HTTP	1,883,659.50
Firefox	890,328.79
Chrome	309,863.68
FireAMP	240,467.09
iTunes_Desktop	239,519.67
Apple_Update	229,613.67
YouTube	135,388.15
HTTPS	120,156.59
Web_browser	100,714.09
Advanced_Packaging_Tool	82,782.54

Last updated 2 minutes ago

### Top Sources

Initiator IP	Traffic (KB)
69.244.85.47	555,655.73
10.112.10.21	255,709.95
10.131.12.204	120,643.10
10.131.12.168	89,341.66
192.168.3.7	62,972.92
255.255.255.255	37,675.33
172.16.0.75	32,684.99
10.131.10.1	28,203.94
192.168.1.7	26,993.71
10.131.10.11	24,050.13

Last updated 2 minutes ago

### Top Source Countries

Initiator Country	Total Connections
USA (United States)	294
NOR (Norway)	4
CHN (China)	3
GBR (United Kingdom)	2
JPN (Japan)	2
BRA (Brazil)	1
DEU (Germany)	1
FRA (France)	1

Last updated 2 minutes ago

### Users

Username	Total Bytes (KB)
Jolie Lenehan (jlenehan, LDAP)	583,932.98
Joe Smith (jsmith, LDAP)	500,597.60
Diane Tibbott (dtibbott, LDAP)	133,125.96
Barbara Hoffman (bhoffman, LDAP)	100,863.62
Jim Stewart (jstewart, LDAP)	93,843.68
Scott Gode (sgode, LDAP)	64,526.05
Mike Seamans (mseamans, LDAP)	36,839.12
Cynthia Randall (crandall, LDAP)	35,929.05
Jeff Henshaw (jhenshaw, LDAP)	32,811.69
Mike Tiano (mtiano, LDAP)	24,956.66

Last updated less than a minute ago

### Traffic by Responder IP

Responder IP	Traffic (KB)
10.131.10.122	73,026.18
10.131.10.11	23,310.25
10.0.168.106	18,899.92
10.0.37.85	18,896.13
10.112.10.21	17,304.10
10.131.12.168	15,454.27
10.131.10.1	15,187.92
10.131.10.120	14,093.15
10.0.108.75	12,680.33
10.0.228.14	12,679.10

Last updated 2 minutes ago

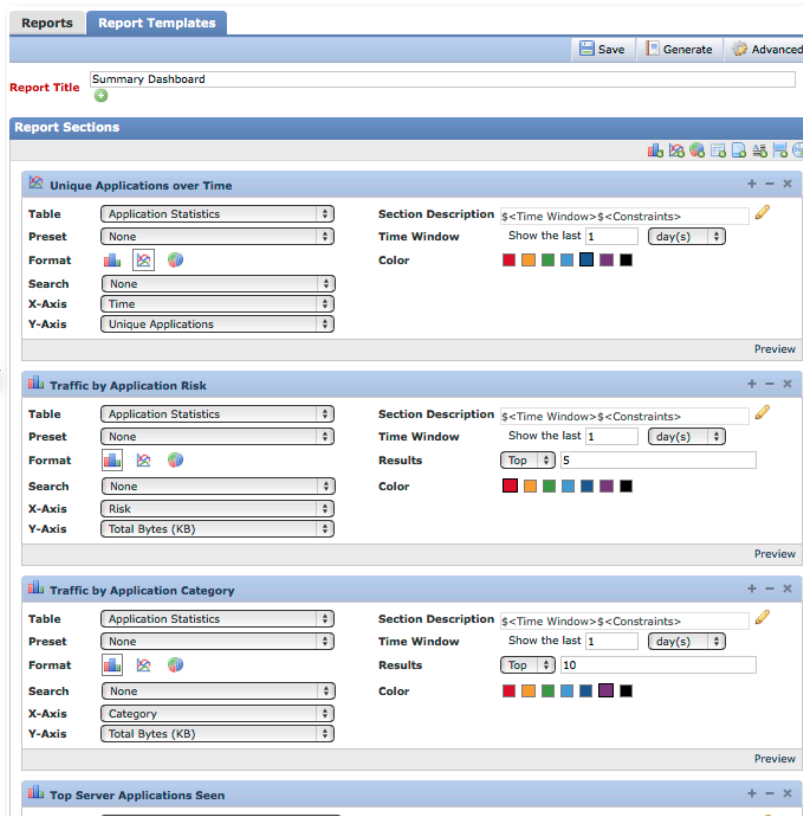
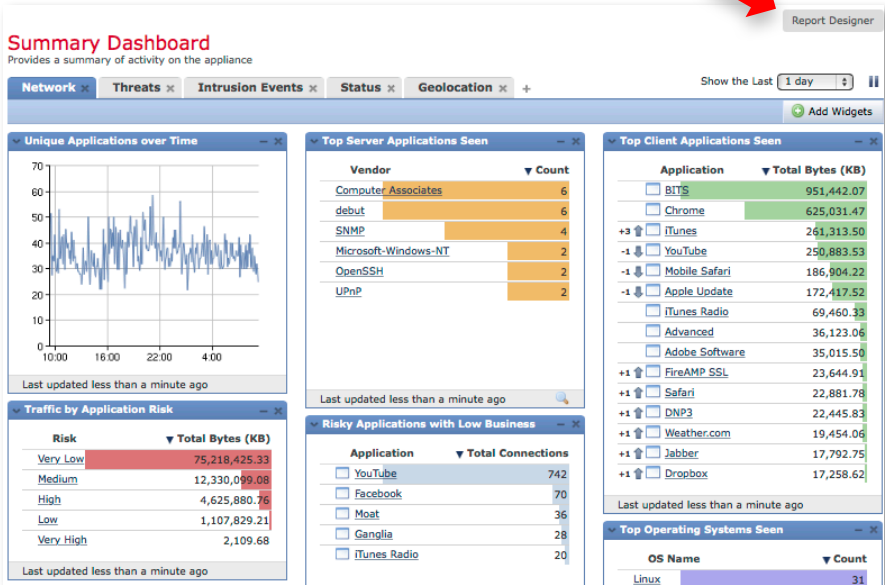
### Top Destination Countries

Responder Country	Total Bytes (KB)
USA (United States)	1,187,358.90
NLD (Netherlands)	25,359.72
JPN (Japan)	16,921.29
CHN (China)	7,138.61
NOR (Norway)	2,995.10
BRA (Brazil)	2,966.77
SVK (Slovakia (slovak Republic))	2,885.41
VNM (Viet Nam)	1,527.32
GBR (United Kingdom)	1,347.76
CAN (Canada)	1,322.82

Last updated 2 minutes ago

# Build Reports Straight from the Dashboard

Report Designer





# Risk Reports

- Integrated in Firepower Management Center
  - No need to download scripts
  - Accessible through Menu item (Overview > Reporting > Report Templates)
- All three existing reports
  - Advanced Malware Risk Report
  - Attacks Risk Report
  - Network Risk Report
- Available in all Firepower Management Center models

## Typical Use Case

- Proof of Value during Sales
- Ongoing Monitoring of Value & Communication to Executives

## IV. RECOMMENDATIONS

Despite your existing network and endpoint protections, critical attacks are taking place and placing your organization at risk. New countermeasures and security controls are required to mitigate the risk.

Cisco recommends deployment of network-based protections via the threat-focused Cisco Firepower Next Generation Firewall and NGIPS Appliances to complement existing protections. These will provide the following new capabilities and benefits:

NEW CAPABILITY	BENEFIT
Real-Time Contextual Awareness	Profile hosts, applications, users, and network infrastructure in real time. Assess potential vulnerabilities and identify network changes.
Automatic Impact Assessment	Determine the risk of any attack to your business in real time in order to optimize response to it.
File Identification and Control	Detect and optionally block files by file type. Capture files for offline analysis, if desired.
Advanced Malware Protection (AMP)	Protect against malware with AMP for networks, which includes integration with AMP ThreatGRID for superior sandboxing, security intelligence and advanced file analysis. Also, AMP for Endpoints provides endpoint protection to offer defense in depth.
URL filtering	Enforce acceptable use of the internet.
Application Visibility and Control	Identify and control over 3000 applications. By leveraging OpenAppID, application detectors can be created for custom application. Furthermore, Snort rules can be written to address specific applications.
Security Intelligence	With unparalleled visibility into the Internet, Cisco Talos provides dynamic IP and URL black list to protect against malicious websites.
Automatic Policy Tuning	Automatically tune IPS protections in response to changes in your network composition.
Association of Users with Security and Compliance Events	Associate users with activity on the network, including attacks and application usage, through integration with Active Directory servers.
Collective Intelligence	Get rapid detection and insight into emerging threats so that defenses stay effective.
Virtual Protection	Protect VM-to-VM communications the same as physical networks.

In addition, Cisco offers optional Advanced Malware Protection for networks and hosts, and optional Application Control and URL Filtering, to help better protect against the latest threats. Please contact your Cisco representative or reseller for more information.



# Thank you

---

Dragan Novaković  
Cisco Systems  
[dnovakov@cisco.com](mailto:dnovakov@cisco.com)

