TOMORROW
starts here.

CISCO

Cisco live!

Sourcefire Network Security Analytics: Finding the Needle in the Haystack

BRKSEC-3034

Mark Pretty

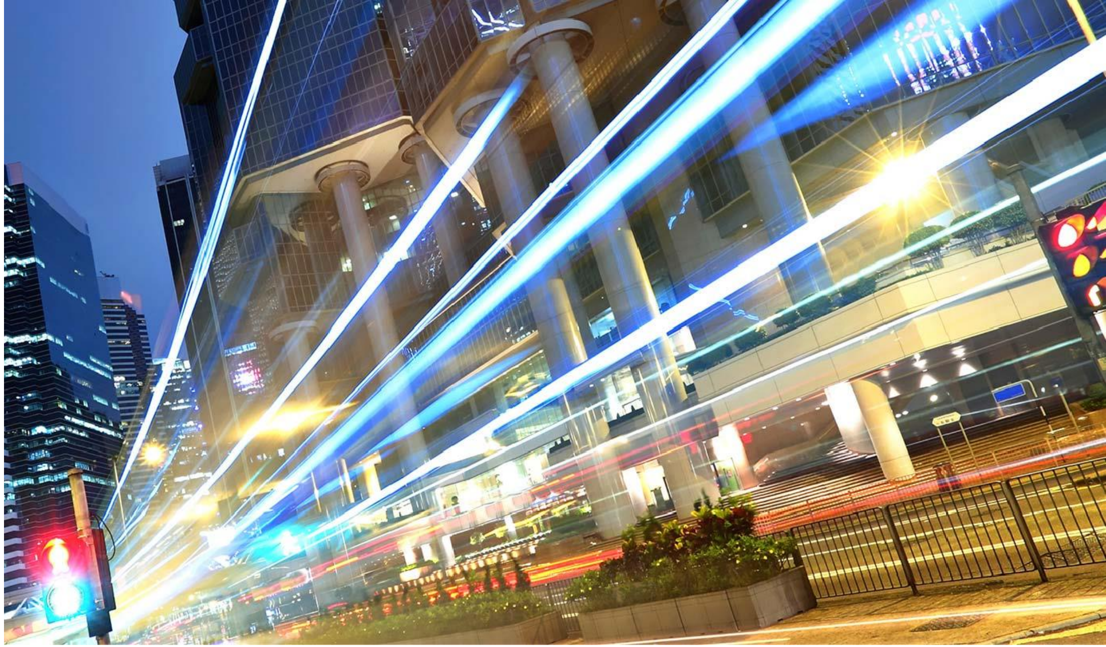
Consulting Systems Engineer

#clmel

Cisco live!

Agenda

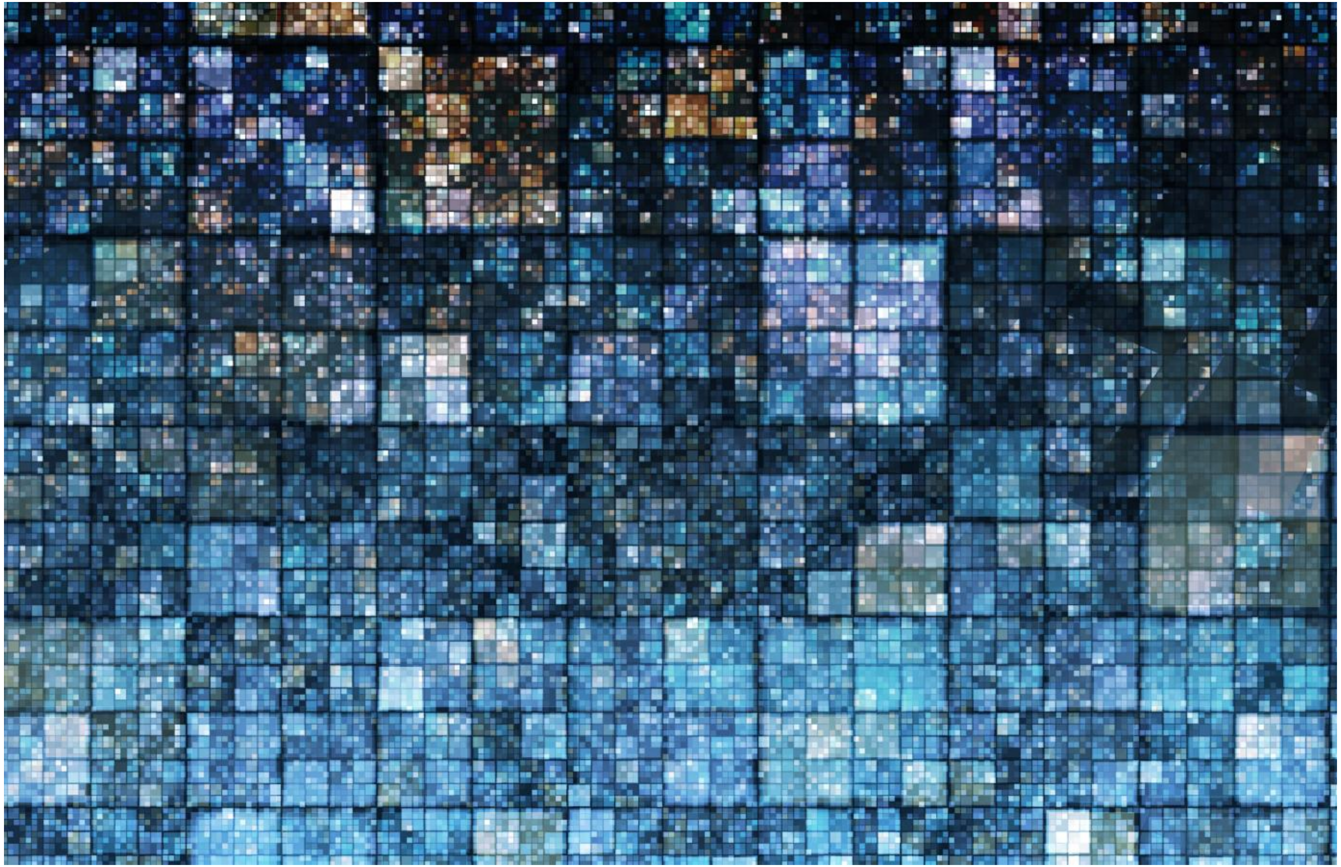
- Introduction
- The Sourcefire Solution
- Real-time Analytics
- On-Demand Analytics
- Putting the Tools to Work
- Q & A



“Analytics leverage data in a particular functional process (or application) to enable context-specific insight that is actionable”

Gartner

How Easy is it to Find Things?



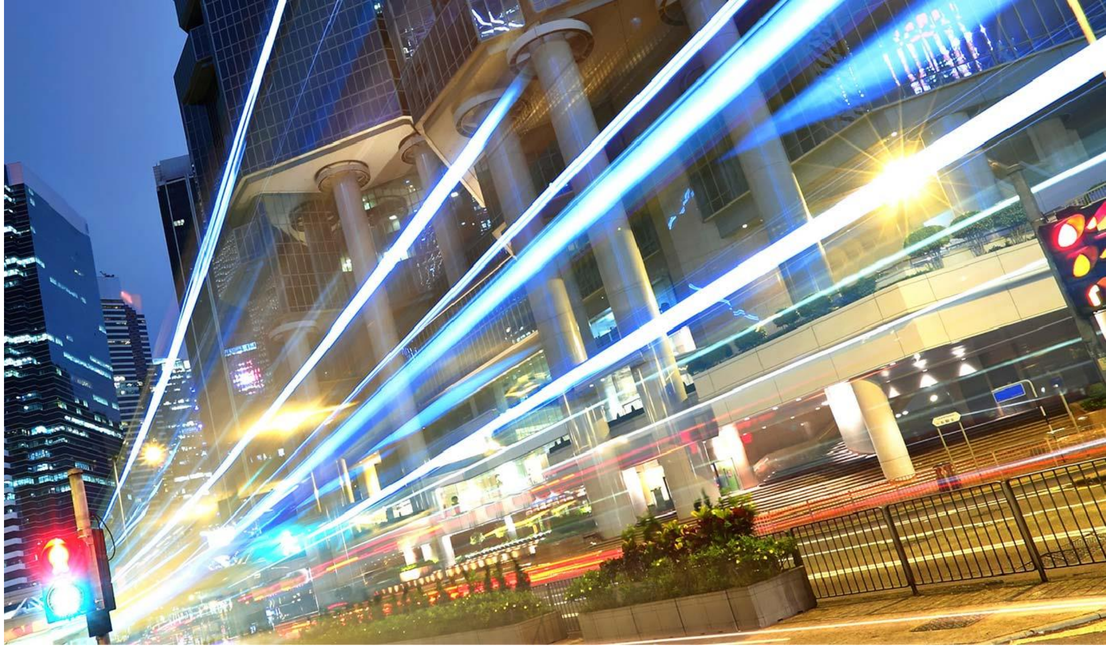
© 2015 Cisco and/or its affiliates. All rights reserved.

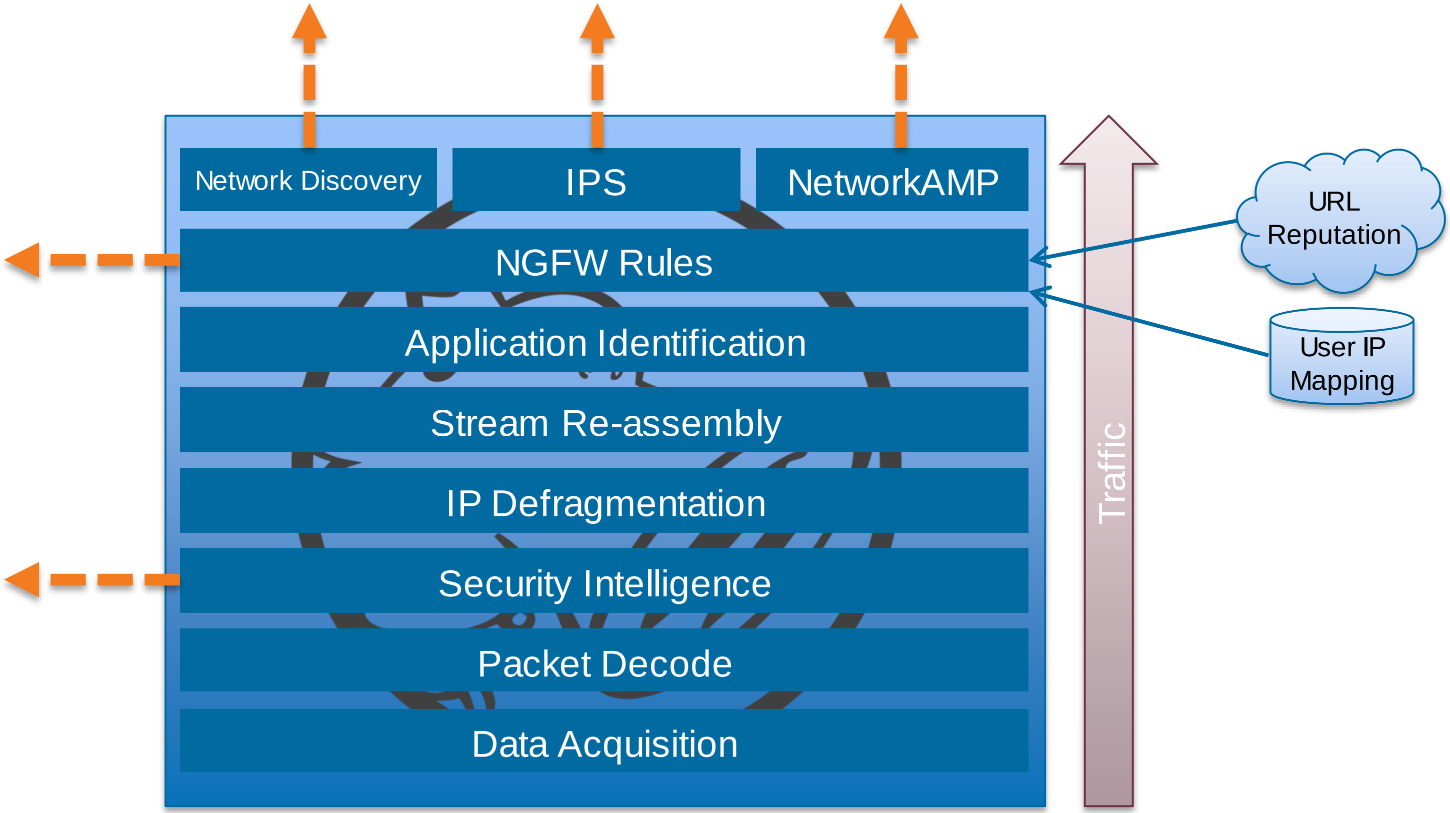
Sourcefire Analytics Solution

The Sourcefire Solution

Agenda

- Introduction
- The Sourcefire Solution
- Real-time Analytics
- On-Demand Analytics
- Putting the Tools to Work
- Q & A





Network Discovery

IPS

NetworkAMP

NGFW Rules

Application Identification

Stream Re-assembly

IP Defragmentation

Security Intelligence

Packet Decode

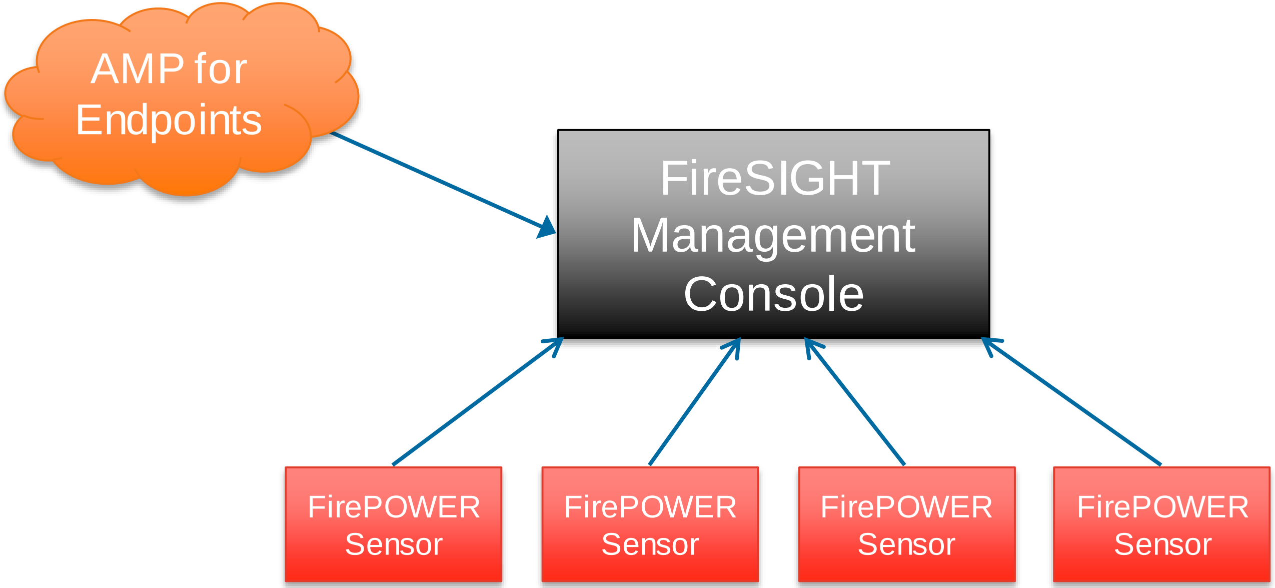
Data Acquisition

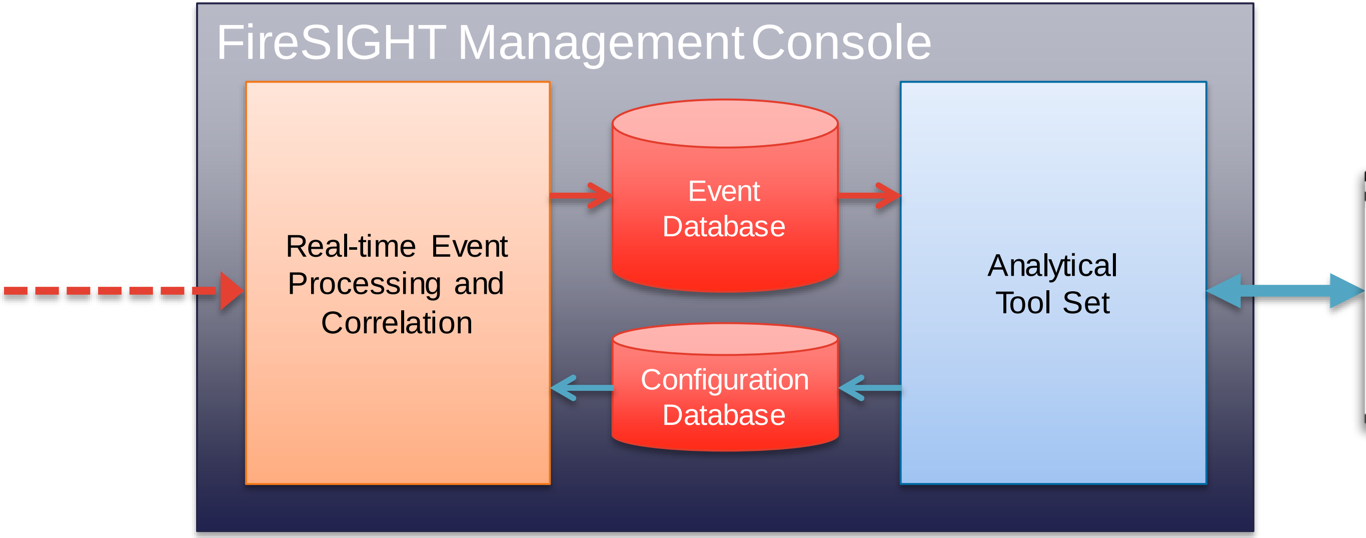
Traffic

URL Reputation

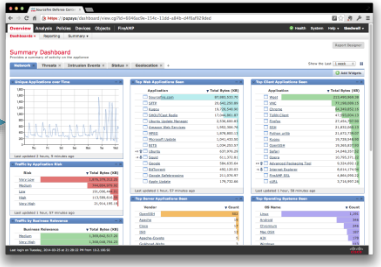
User IP Mapping

© 2015 Cisco and/or its affiliates. All rights reserved.


AMP for Endpoints
FireSIGHT Management Console
FirePOWER Sensor
FirePOWER Sensor
FirePOWER Sensor
FirePOWER Sensor



FireSIGHT Management Console
Real-time Event Processing and Correlation
Event Database
Configuration Database
Analytical Tool Set



Overview
Analysis
Policies
Devices
Objects
FireAMP
Health
System
Help
Dashboards
Reporting
Summary
Report Designer
Summary Dashboard
Provides a summary of activity on the appliance
Network
Threats
Intrusion Events
Status
Geolocation
Add Widgets
Unique Applications over Time
Top Web Applications Seen
Top Client Applications Seen
Traffic by Application Risk
Traffic by Business Relevance
Top Server Applications Seen
Top Operating Systems Seen

Data Sources

FirePOWER

FireSIGHT

FirePOWER Event Data

- Network Discovery Events
- Statistics Events
- Intrusion Events
- File & Malware Events
- Connection Events.

© 2015 Cisco and/or its affiliates. All rights reserved.

FireAMP Events

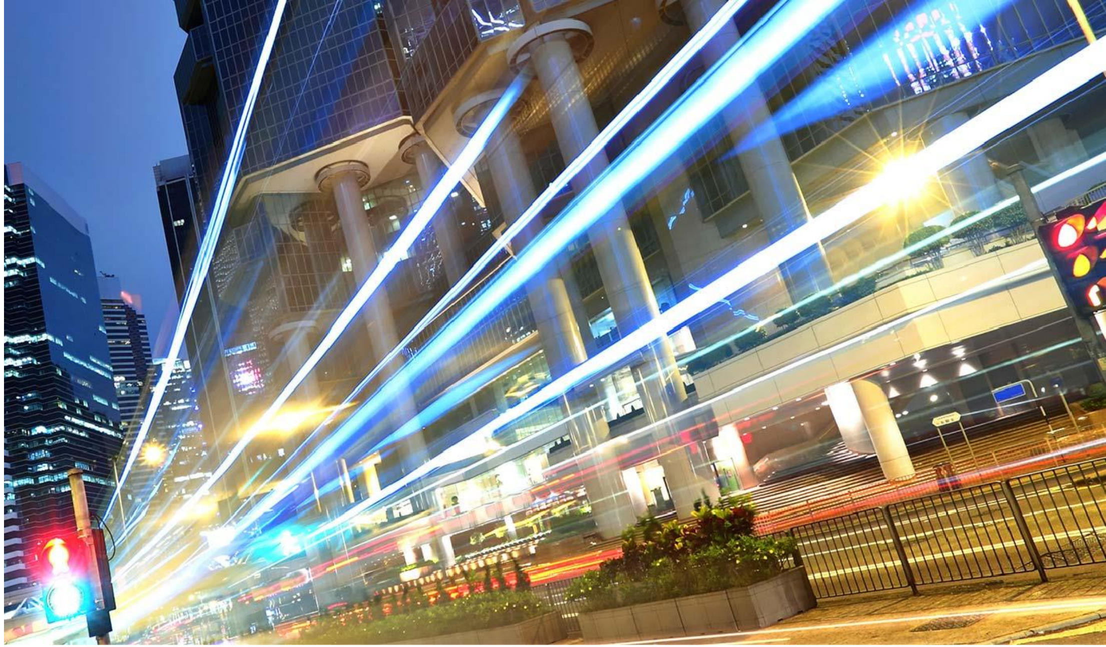
- Endpoint Malware Detection
- Quarantine Data
- Restore Information
- Scan Data
- Indicators of Compromise

FireSIGHT Management Console Events

- Indicators of Compromise
- Correlated Statistics
- Event Augmentation

Agenda

- Introduction
- The Sourcefire Solution
- Real-time Analytics
- On-Demand Analytics
- Putting the Tools to Work
- Q & A

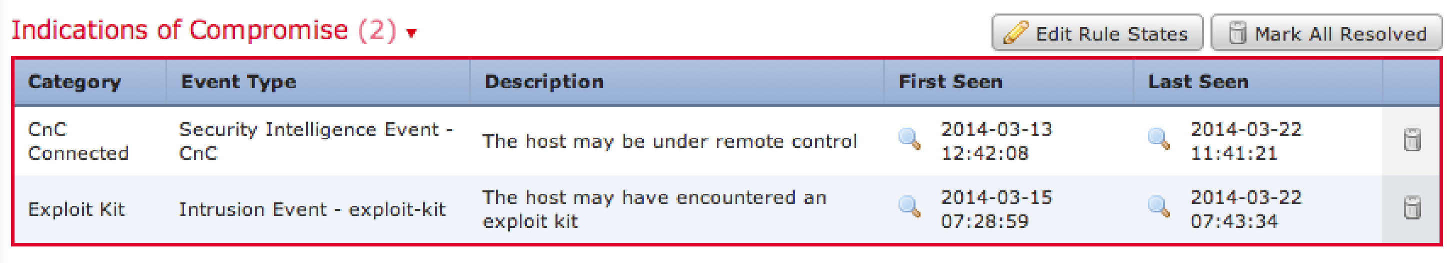


FireSIGHT – Context Context Context!

- Real-time Network Awareness
  - Device
  - User
- FireSIGHT Management Console Network Map
  - Context through asset state

Indications of Compromise

- Correlation of security events



Category	Event Type	Description	First Seen	Last Seen	
CnC Connected	Security Intelligence Event - CnC	The host may be under remote control	2014-03-13 12:42:08	2014-03-22 11:41:21	
Exploit Kit	Intrusion Event - exploit-kit	The host may have encountered an exploit kit	2014-03-15 07:28:59	2014-03-22 07:43:34	

– Threat detected
– Security Intelligence
– Malware detection
– AMP endpoint

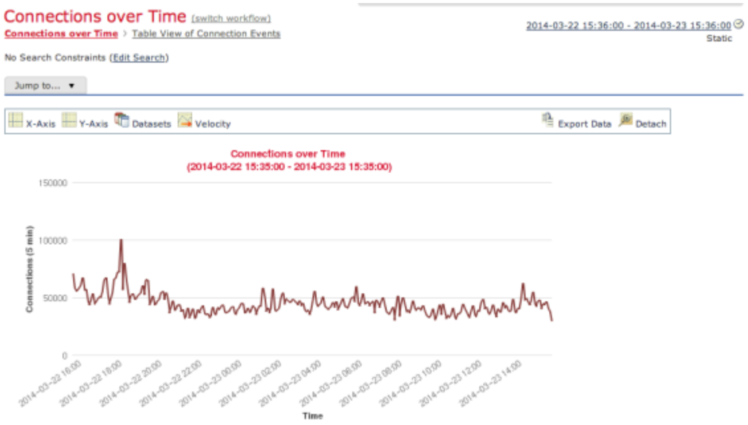
Intrusion Event Impact Flag

- Real-time threat Impact Assessment
- Leverage the Network Map

Demo

Flow Summaries

- Counters generated in real-time via key based connection event aggregation.



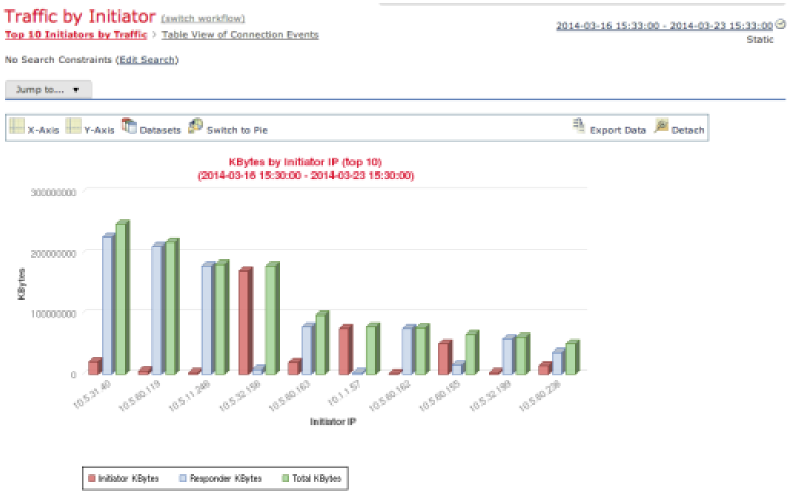
Connections over Time (switch workflow)

Connections over Time › Table View of Connection Events

2014-03-22 15:36:00 - 2014-03-23 15:36:00

Static

No Search Constraints (Edit Search)



Traffic by Initiator (switch workflow)

Top 10 Initiators by Traffic › Table View of Connection Events

2014-03-16 15:33:00 - 2014-03-23 15:33:00

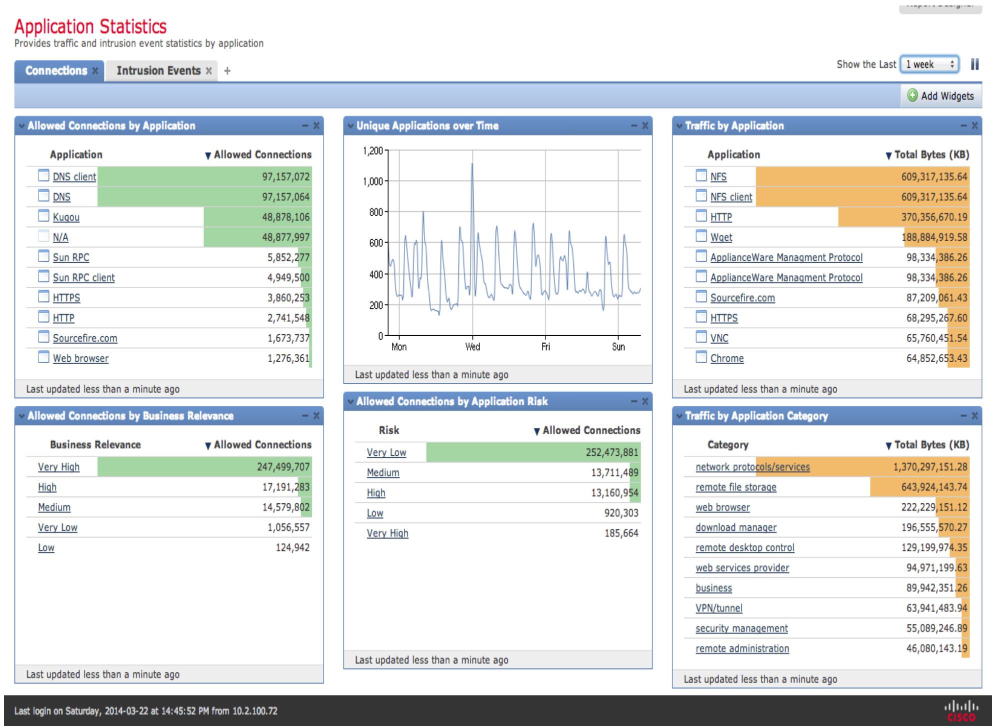
Static

No Search Constraints (Edit Search)

- Facilitates analytics over larger time ranges from a performance and retention perspective.

Time-series Statistics

- Fast, minimal storage, meaningful-trending data
- Gauges and Counters
- Sensor based stats are inclusive independent of logging policy
- Remember MRTG, RRDTool, Cacti?



Application Statistics

Provides traffic and intrusion event statistics by application

Allowed Connections by Application

Application	▼ Allowed Connections
□ DNS client	97,157,072
□ DNS	97,157,064
□ Kugou	48,878,106
□ N/A	48,877,997
□ Sun RPC	5,852,277
□ Sun RPC client	4,949,500
□ HTTPS	3,860,253
□ HTTP	2,741,548
□ Sourcefire.com	1,673,737
□ Web browser	1,276,361

Last updated less than a minute ago

Unique Applications over Time

Last updated less than a minute ago

Traffic by Application

Application	▼ Total Bytes (KB)
□ NFS	609,317,135.64
□ NFS client	609,317,135.64
□ HTTP	370,356,670.19
□ Wget	188,884,919.58
□ ApplianceWare Managment Protocol	98,334,386.26
□ ApplianceWare Managment Protocol	98,334,386.26
□ Sourcefire.com	87,209,061.43
□ HTTPS	68,295,267.60
□ VNC	65,760,451.54
□ Chrome	64,852,653.43

Last updated less than a minute ago

Allowed Connections by Business Relevance

Business Relevance	▼ Allowed Connections
Very High	247,499,707
High	17,191,283
Medium	14,579,802
Very Low	1,056,557
Low	124,942

Last updated less than a minute ago

Allowed Connections by Application Risk

Risk	▼ Allowed Connections
Very Low	252,473,881
Medium	13,711,489
High	13,160,954
Low	920,303
Very High	185,664

Last updated less than a minute ago

Traffic by Application Category

Category	▼ Total Bytes (KB)
network protocols/services	1,370,297,151.28
remote file storage	643,924,143.74
web browser	222,229,151.12
download manager	196,555,570.27
remote desktop control	129,199,974.35
web services provider	94,971,199.63
business	89,942,351.26
VPN/tunnel	63,941,483.94
security management	55,089,246.89
remote administration	46,080,143.19

Last updated less than a minute ago

Last login on Saturday, 2014-03-22 at 14:45:52 PM from 10.2.100.72

© 2015 Cisco and/or its affiliates. All rights reserved.

Time-series Statistics

- Sensor generated statistics
  - Application, User, URL Reputation, URL Category,
  - File Extraction & Storage

- DC generated statistics
  - IPS
  - GEO (Country), Security Intelligence
  - Compliance Whitelist

Correlation Engine

- Flexible Boolean rules engine functioning on the real-time event stream at the FireSIGHT Management Console.
  - Comprehensive access to events and all their columns
  - Arbitrarily complex rule conditions
  - Host profile qualification
  - Dynamic connection tracking triggered by rule criteria
- Responses
  - Email, Syslog, SNMP Traps
  - Remediation
    - API driven subsystem to dynamically respond to triggering Correlation Rules.

Correlation Engine – Anomaly Detection

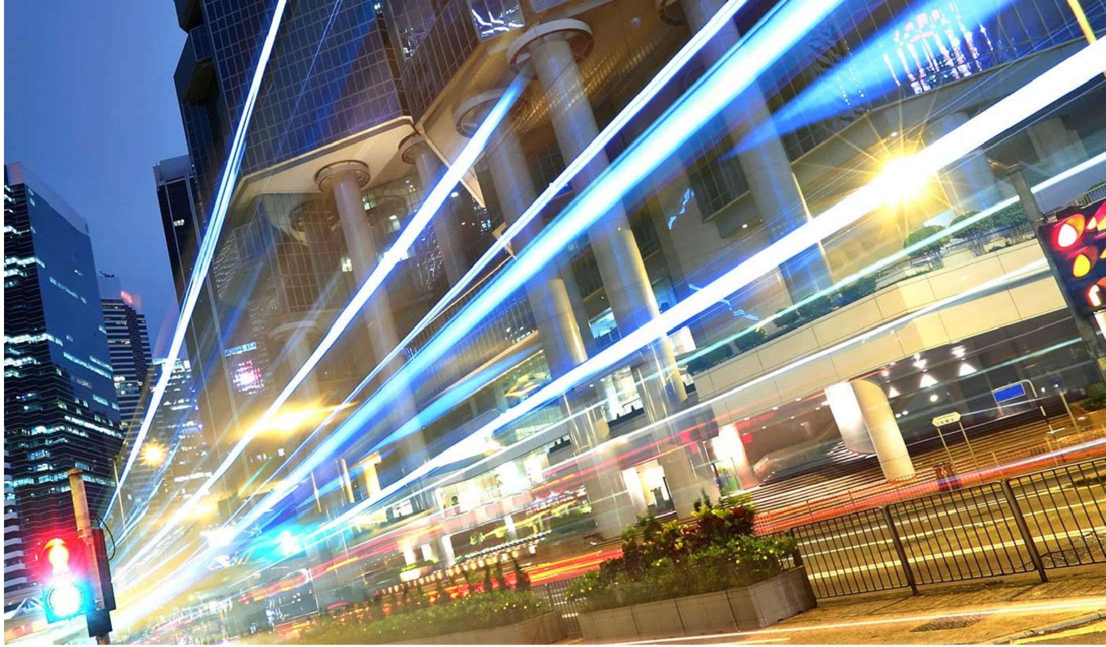
- Compliance Whitelists
  - Define a set of criteria against which to measure hosts on interest on your network
    - Operating System
    - Network Protocol, Application Protocol, Web Application, and Client Application

- Traffic Profiles
  - Set a baseline for connections that meet all the complex criteria provided by the correlation engine then alert on aberrant behaviour

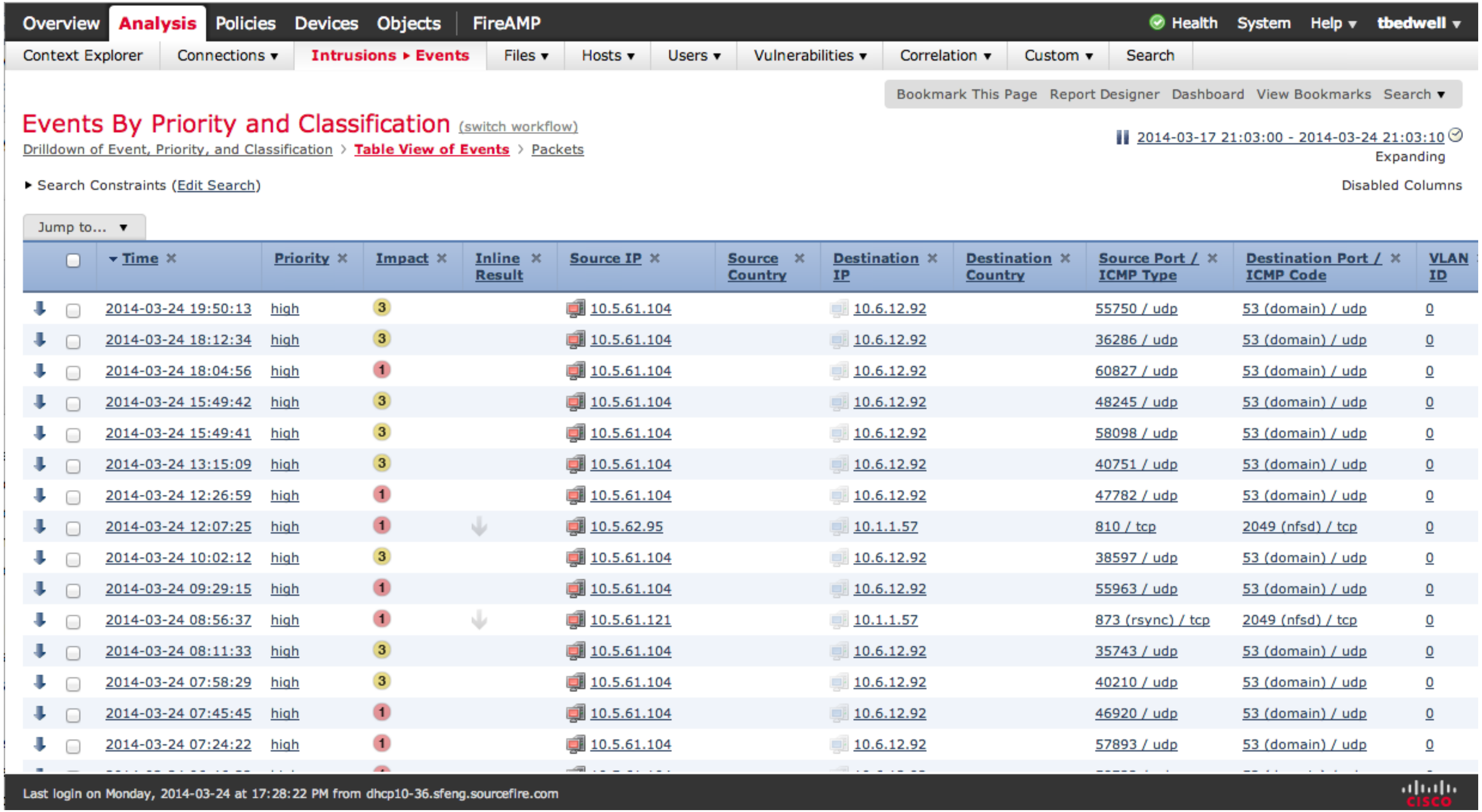
Demo

Agenda

- Introduction
- The Sourcefire Solution
- Real-time Analytics
- On-Demand Analytics
- Putting the Tools to Work
- Q & A



Event Viewer



Events By Priority and Classification (switch workflow)

Drilldown of Event, Priority, and Classification › Table View of Events › Packets

2014-03-17 21:03:00 - 2014-03-24 21:03:10
Expanding

▸ Search Constraints (Edit Search)

Disabled Columns

Jump to... ▾

	□	Time	Priority	Impact	Inline Result	Source IP	Source Country	Destination IP	Destination Country	Source Port / ICMP Type	Destination Port / ICMP Code	VLAN ID
↓	□	2014-03-24 19:50:13	high	3		10.5.61.104		10.6.12.92		55750 / udp	53 (domain) / udp	0
↓	□	2014-03-24 18:12:34	high	3		10.5.61.104		10.6.12.92		36286 / udp	53 (domain) / udp	0
↓	□	2014-03-24 18:04:56	high	1		10.5.61.104		10.6.12.92		60827 / udp	53 (domain) / udp	0
↓	□	2014-03-24 15:49:42	high	3		10.5.61.104		10.6.12.92		48245 / udp	53 (domain) / udp	0
↓	□	2014-03-24 15:49:41	high	3		10.5.61.104		10.6.12.92		58098 / udp	53 (domain) / udp	0
↓	□	2014-03-24 13:15:09	high	3		10.5.61.104		10.6.12.92		40751 / udp	53 (domain) / udp	0
↓	□	2014-03-24 12:26:59	high	1		10.5.61.104		10.6.12.92		47782 / udp	53 (domain) / udp	0
↓	□	2014-03-24 12:07:25	high	1	↓	10.5.62.95		10.1.1.57		810 / tcp	2049 (nfsd) / tcp	0
↓	□	2014-03-24 10:02:12	high	3		10.5.61.104		10.6.12.92		38597 / udp	53 (domain) / udp	0
↓	□	2014-03-24 09:29:15	high	1		10.5.61.104		10.6.12.92		55963 / udp	53 (domain) / udp	0
↓	□	2014-03-24 08:56:37	high	1	↓	10.5.61.121		10.1.1.57		873 (rsync) / tcp	2049 (nfsd) / tcp	0
↓	□	2014-03-24 08:11:33	high	3		10.5.61.104		10.6.12.92		35743 / udp	53 (domain) / udp	0
↓	□	2014-03-24 07:58:29	high	3		10.5.61.104		10.6.12.92		40210 / udp	53 (domain) / udp	0
↓	□	2014-03-24 07:45:45	high	1		10.5.61.104		10.6.12.92		46920 / udp	53 (domain) / udp	0
↓	□	2014-03-24 07:24:22	high	1		10.5.61.104		10.6.12.92		57893 / udp	53 (domain) / udp	0

Last login on Monday, 2014-03-24 at 17:28:22 PM from dhcp10-36.sfeng.sourcefire.com

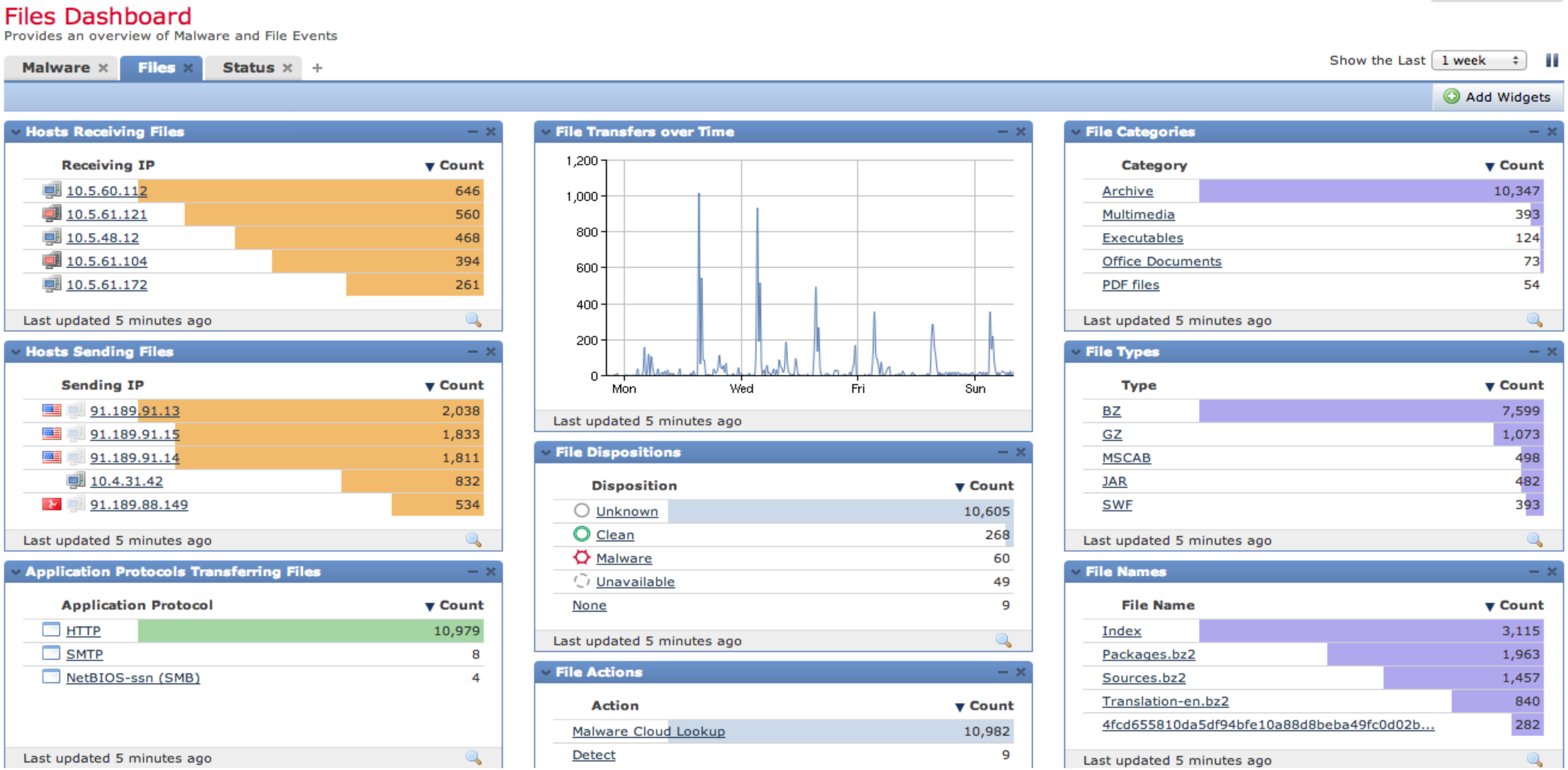
© 2015 Cisco and/or its affiliates. All rights reserved.

Event Viewer

- Workflow system
  - Pre-configured and Custom event roll-ups
- Single click constraints
  - Build filters as you explore your data
- Event type pivots
  - Unified constraints and time ranges
- Detail views
  - Packet View, User History, Host Profile, File Trajectory
- Contextual actions
  - IP Blacklisting, Intrusion Rule Suppression & Thresholding

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Dashboard



Files Dashboard

Provides an overview of Malware and File Events

Hosts Receiving Files

Receiving IP	▼ Count
10.5.60.112	646
10.5.61.121	560
10.5.48.12	468
10.5.61.104	394
10.5.61.172	261

Last updated 5 minutes ago

Hosts Sending Files

Sending IP	▼ Count
91.189.91.13	2,038
91.189.91.15	1,833
91.189.91.14	1,811
10.4.31.42	832
91.189.88.149	534

Last updated 5 minutes ago

Application Protocols Transferring Files

Application Protocol	▼ Count
HTTP	10,979
SMTP	8
NetBIOS-ssn (SMB)	4

Last updated 5 minutes ago

File Transfers over Time

Last updated 5 minutes ago

File Dispositions

Disposition	▼ Count
○ Unknown	10,605
○ Clean	268
Malware	60
Unavailable	49
None	9

Last updated 5 minutes ago

File Actions

Action	▼ Count
Malware Cloud Lookup	10,982
Detect	9

File Categories

Category	▼ Count
Archive	10,347
Multimedia	393
Executables	124
Office Documents	73
PDF files	54

Last updated 5 minutes ago

File Types

Type	▼ Count
BZ	7,599
GZ	1,073
MSCAB	498
JAR	482
SWF	393

Last updated 5 minutes ago

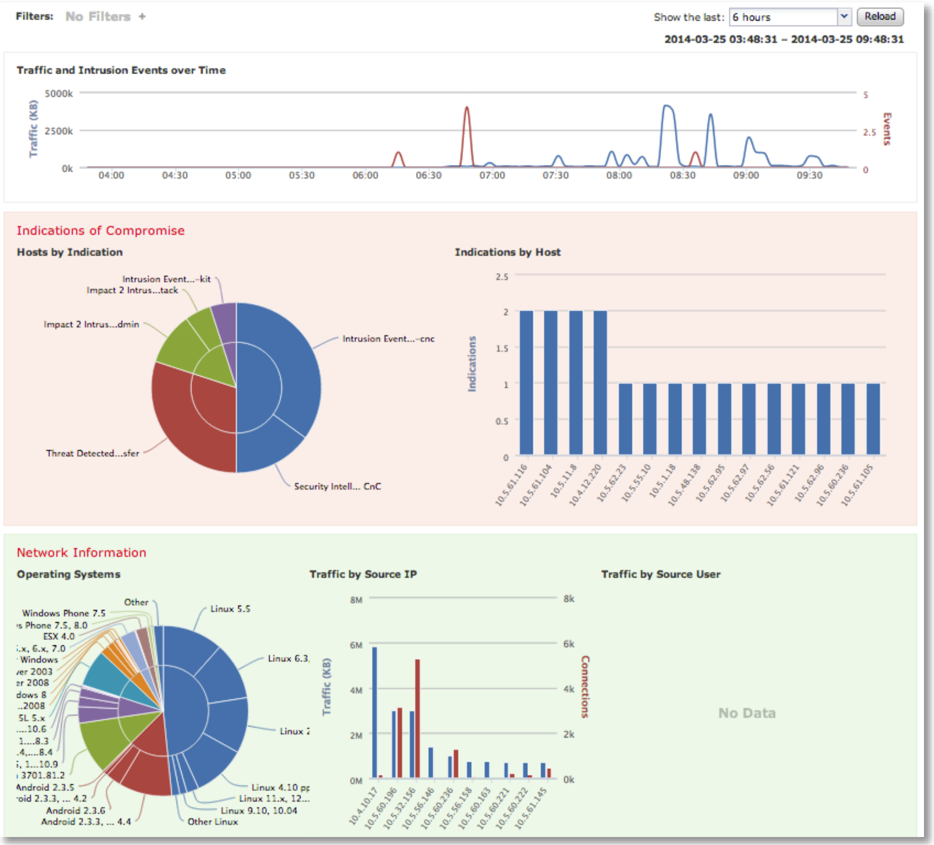
File Names

File Name	▼ Count
Index	3,115
Packages.bz2	1,963
Sources.bz2	1,457
Translation-en.bz2	840
4fcd655810da5df94bfe10a88d8beba49fc0d02b...	282

Last updated 5 minutes ago

Context Explorer

- Data exploration tool
- Visualisations of IoC, Network, Intrusion, File, App, User, and Geo info
- Advanced filtering across data silos
- Drill downs into detailed event analysis
- Accessible from analysis tools to provide context



Filters: No Filters +

Show the last: 6 hours

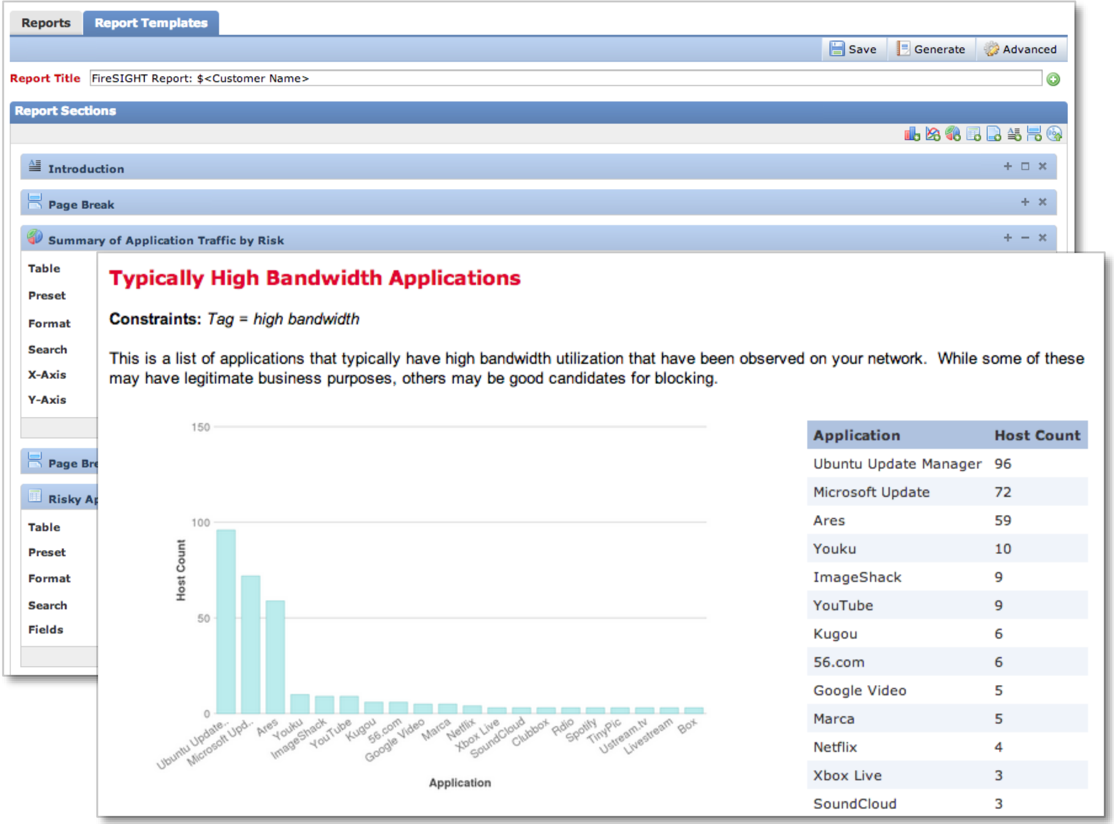
Reload

2014-03-25 03:48:31 – 2014-03-25 09:48:31

Demo

Flexible Reporting

- Highly customisable and reusable report templates
- Generate reports based on dashboards and event views
- Scheduling support
- Multiple output formats
- Variable support for template reuse



Report Title FireSIGHT Report: $<Customer Name>

Typically High Bandwidth Applications

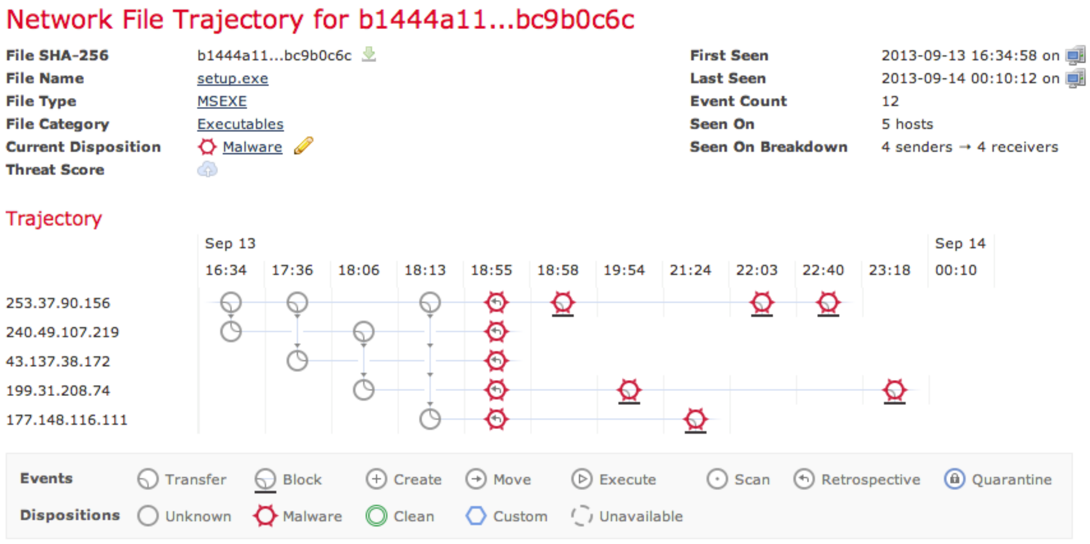
Constraints: *Tag = high bandwidth*

This is a list of applications that typically have high bandwidth utilization that have been observed on your network. While some of these may have legitimate business purposes, others may be good candidates for blocking.

Application	Host Count
Ubuntu Update Manager	96
Microsoft Update	72
Ares	59
Youku	10
ImageShack	9
YouTube	9
Kugou	6
56.com	6
Google Video	5
Marca	5
Netflix	4
Xbox Live	3
SoundCloud	3

Network File Trajectory

- Powerful visualisation approach influenced by the FireAMP product
- Allows for aggregation of FireAMP and NetworkAMP file intelligence to provide a comprehensive story of the lifecycle a file (or malware) within your enterprise.



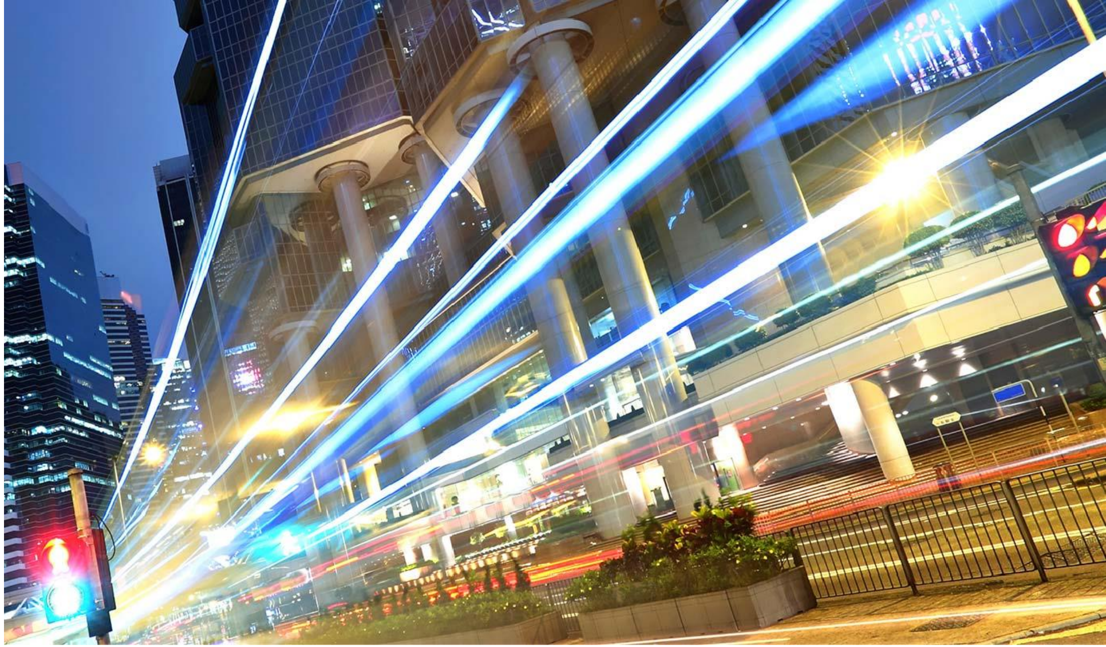
Network File Trajectory for b1444a11...bc9b0c6c

File SHA-256	b1444a11...bc9b0c6c	**First Seen**	2013-09-13 16:34:58 on 253.37.90.156
File Name	setup.exe	**Last Seen**	2013-09-14 00:10:12 on 199.31.208.74
File Type	MSEXE	**Event Count**	12
File Category	Executables	**Seen On**	5 hosts
Current Disposition	Malware	**Seen On Breakdown**	4 senders → 4 receivers
Threat Score			

Trajectory

Agenda

- Introduction
- The Sourcefire Solution
- Real-time Analytics
- On-Demand Analytics
- Putting the Tools to Work
- Q & A



Demo

Closing

- Real-time Analytics
  - FireSIGHT Context Awareness
  - Time-series Statistical Data
  - Use Case Specific Correlation
- On-demand Analytics
  - Event Viewer
  - Context Explorer
  - Dashboarding
  - File Trajectory

© 2014 Cisco and/or its affiliates. All rights reserved.

Continue Your Education

- Demos in the Cisco Campus
- Walk-in Self-Paced Labs
- Table Topics
- Meet the Engineer 1:1 meetings

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Q & A

Complete Your Online Session Evaluation

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

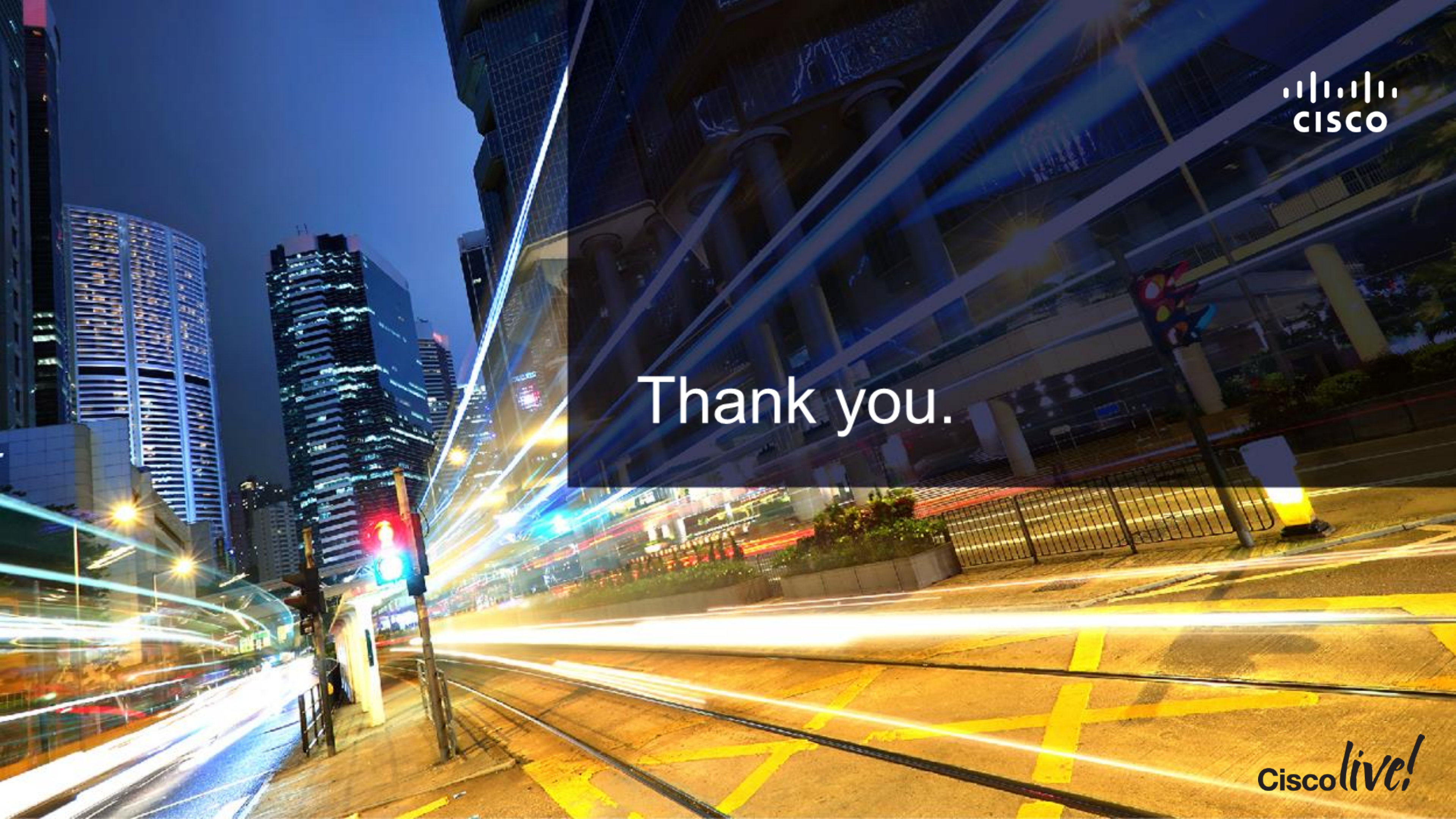
Complete your Overall Event Survey and 5 Session Evaluations.

- 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

© 2015 Cisco and/or its affiliates. All rights reserved.



Thank you.

CISCO