Advanced Security Analytics: NetFlow for Incident Response

2015: The Year of the Breach

2016 – The Year of Ransomware

> 200 Million PII exposed

- Ashley Madison
- Office of Personnel Management
- Anthem
- VTech
- Hilton
- LATEST – Wendy's

comeback

Member

From: Diana Jones [mailto:diana.[redacted]@[redacted].com]
Sent: Thursday, April 10, 2014 2:03 PM
To: '[redacted]@Plixer.com'
Subject: VOIP, Unified Communications and Video Conferencing Users

Hi,

We have rec[redacted] few:

Few of the li[redacted]

- Cisco[redacted]
- Tand[redacted]
- Avaya users list
- Shoretel users list
- Lync users list
- Nortel users list
- Polycom users list
- 3Com users list
- Mitel users list
- Siemens users list and more

[redacted] Company, based in [redacted], Maine, sued Ocean Bank, now called People's United Bank, after fraudsters made six wire transfers using the Automated Clearing House (ACH) transfer system amounting to more than $588,000 in May 2009. About $243,000 was recovered.

my ID.

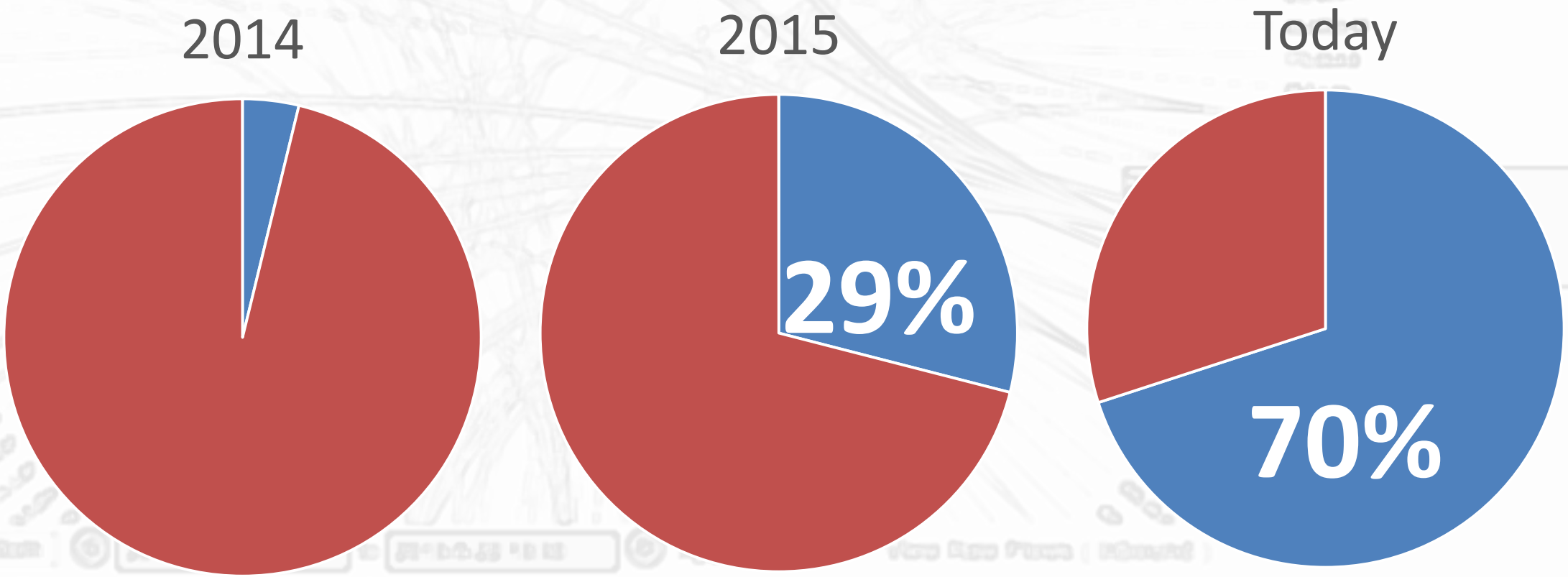
- Us Bin 10$, US Dob 15$

- Us fullz info = 25$ per 1

Why Can’t You Detect Them?

- Zero Day
  - No signature match
- They make outbound connections
- They embrace encryption for secure connections
- They know DNS in your blind spot
- They use the authentication system you setup!

Encryption Growth Rate



What is NetFlow/IPFIX

NetFlow – What it is…

TELEPHONE USAGE CHARGES

Charges Billed to **BRAHM, LAURENCE** **AUTHCODE**

DATE	TIME	PLACE		NUMBER	MIN	CHARGE
21-AUG-2005	09:35	ELKHORN	NE	4025531620	0.4	0.02
22-AUG-2005	09:41	MISSOULA	MT	4069283507	6.8	0.37
23-AUG-2005	09:48	GRASS VLY	CA	5302614689	1.0	0.06
24-AUG-2005	14:12	LARAMIE	WY	3073426413	2.4	0.13
27-AUG-2005	14:17	GREELEY	CO	9703306310	1.0	0.06
09-SEP-2005	14:22	SPOKANE	WA	5098381370	2.7	0.15
20-SEP-2005	14:25	FLAGSTAFF	AZ	9287143707	0.4	0.02
		CC	**8431464613**			
DATE	**TIME**	**PLACE**		**NUMBER**	**MIN**	**CHARGE**
28-AUG-2005	15:12	CHEYENNE	WY	3078218059	1.0	0.94
28-AUG-2005	15:22	PORTLAND	OR	5038256809	0.0	0.78
29-AUG-2005	15:23	FRESNO	CA	5592337953	1.0	0.12
15-SEP-2005	09:52	FT COLLINS	CO	9704745937	4.0	0.25
19-SEP-2005	16:25	HILLSBORO	OR	5035475794	2.0	0.90
		DT	**5037256659**			
DATE	**TIME**	**PLACE**				
22-AUG-2005	10:47	EUGENE	OR			
26-AUG-2005	13:51	PORTLAND	OR			
01-SEP-2005	11:44	CORVALLIS	OR			
16-SEP-2005	09:39	ASHLAND	OR			

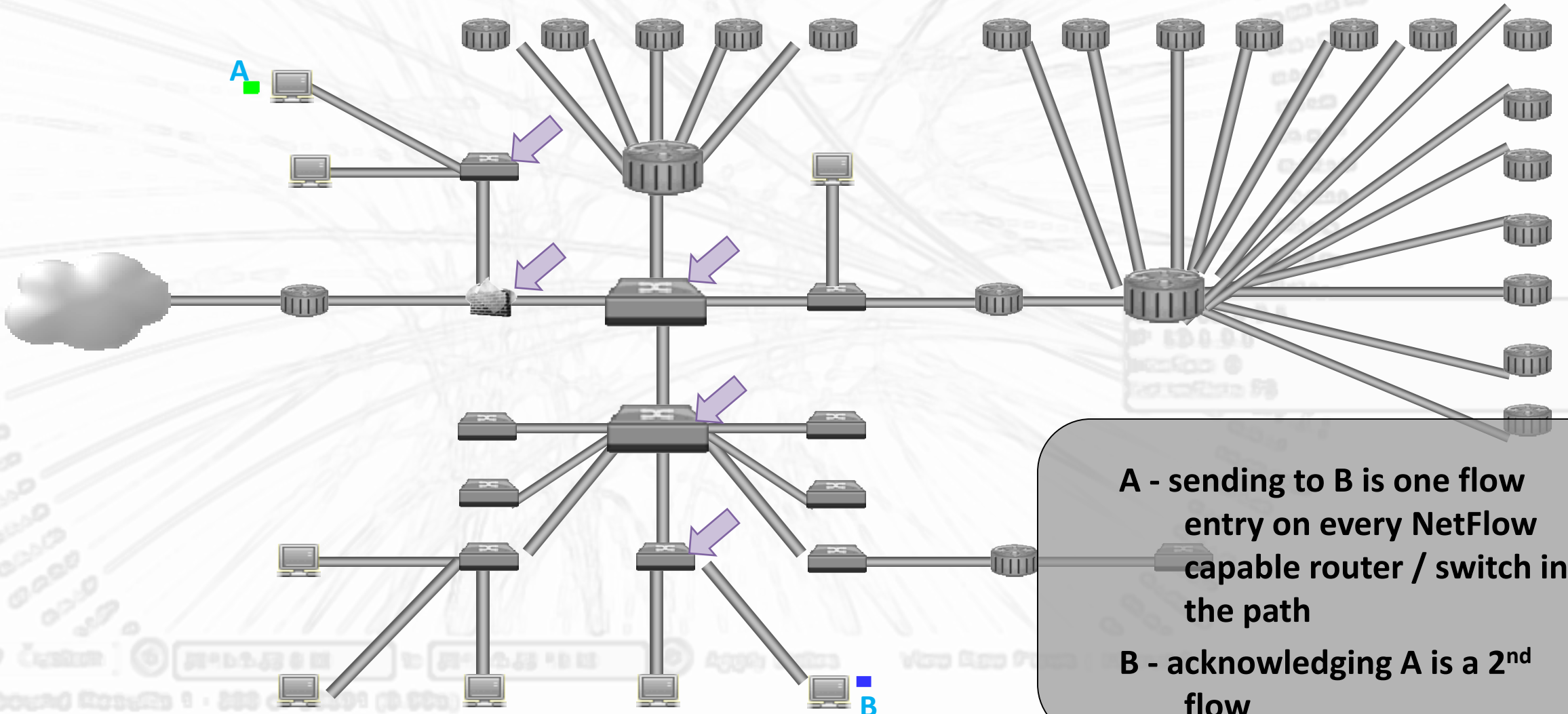
Outbound Phone Calls

Outbound Flow Data

	Flow Start	Source	Destination	Common Port	Protocol	Pkts	Bits
1	2012-11-18 05:22:43	66 [redacted] 84.196	157.55.133.202	https (443 TCP)	TCP	0.24 p/s	2.42 Kb/s
2	2012-11-18 05:20:43	66 [redacted] 84.196	157.55.133.202	https (443 TCP)	TCP	0.24 p/s	2.40 Kb/s
3	2012-11-18 05:23:43	66 [redacted] 84.196	157.55.133.202	https (443 TCP)	TCP	0.23 p/s	2.31 Kb/s
4	2012-11-18 05:21:42	66 [redacted] 84.196	157.55.133.202	https (443 TCP)	TCP	0.22 p/s	2.31 Kb/s
5	2012-11-18 05:20:40	66 [redacted] 84.196	65.55.184.155	http (80 TCP)	TCP	0.01 p/s	13.49 b/s
6	2012-11-18 05:21:39	66 [redacted] 84.196	65.55.184.155	http (80 TCP)	TCP	0.01 p/s	13.49 b/s
7	2012-11-18 05:22:40	66 [redacted] 84.196	65.55.184.155	http (80 TCP)	TCP	0.01 p/s	13.49 b/s
8	2012-11-18 05:23:40	66 [redacted] 84.196	65.55.184.155	http (80 TCP)	TCP	0.01 p/s	13.49 b/s
9	2012-11-18 05:20:43	66 [redacted] 84.196	157.55.133.202	https (443 TCP)	TCP	0.01 p/s	5.47 b/s
10	2012-11-18 05:22:43	66 [redacted] 84.196	157.55.133.202	https (443 TCP)	TCP	0.01 p/s	5.47 b/s
Total	(from conv tables)					1.01 p/s	9.50 Kb/s

Prev 1 Next

NetFlow – How it works…



A - sending to B is one flow entry on every NetFlow capable router / switch in the path

B - acknowledging A is a 2nd flow

IPFIX

- Internet Protocol Flow Information Export (IPFIX)
  - Designed as a common standard for defining how IP Flow information can be exported from routers, measurement probes, or other devices for billing and network management systems.
- The RFC draft of 5101 was approved as standard – July ’13
- What does this mean?
- Who supports IPFIX?

NetFlow/IPFIX Supported Vendors

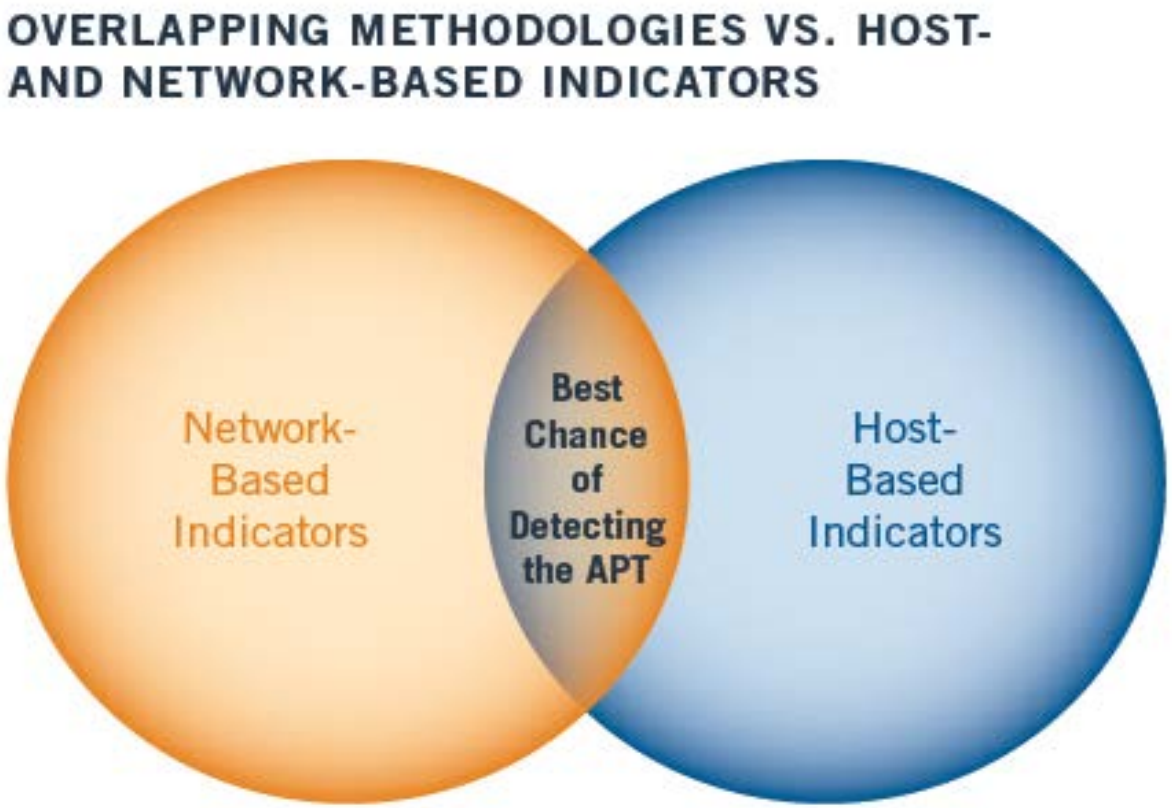
- 3Com
- Adtran
- Barracuda
- Blue Coat
- Cisco
- Citrix
- Dell
- Enterasys
- Expand
- Extreme
- FatPipe
- Juniper
- Mikrotik
- Nortel
- YAF
- Palo Alto
- Plixer
- Riverbed
- SonicWALL
- VMware
- Vyatta
- Xirrus
- Others …

How to Combat: Reduce Complexity

1. Analyze Behavior
2. Profile
3. Threshold
4. Correlate DNS
5. Alarm

Identifying Malware Requires

- Network Traffic Monitoring
- Host-based information monitoring



Profile Your Oracles – Critical Resources

- Before setting thresholds, use flow data to determine certain behaviors that are normal. For example:
  - Volume of flows from a host
  - Max number of end systems it communicates within 5 minutes
  - Average bytes transmitted
  - The ports it communicates on
- Loaded with a historical profile, you can set thresholds which build upon your threat index!

Index Search

Search IP:

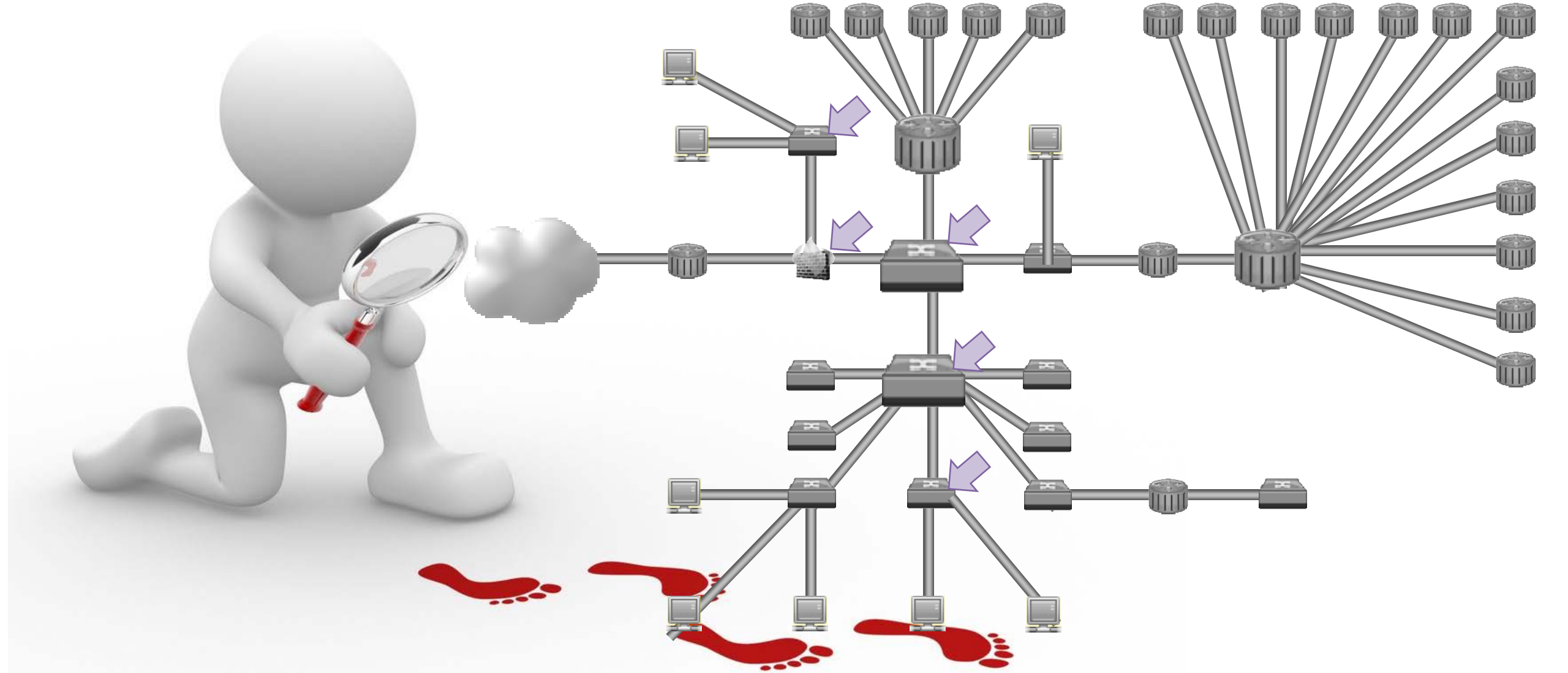
24.39.1.171 Search

The IP has been seen by these exporters

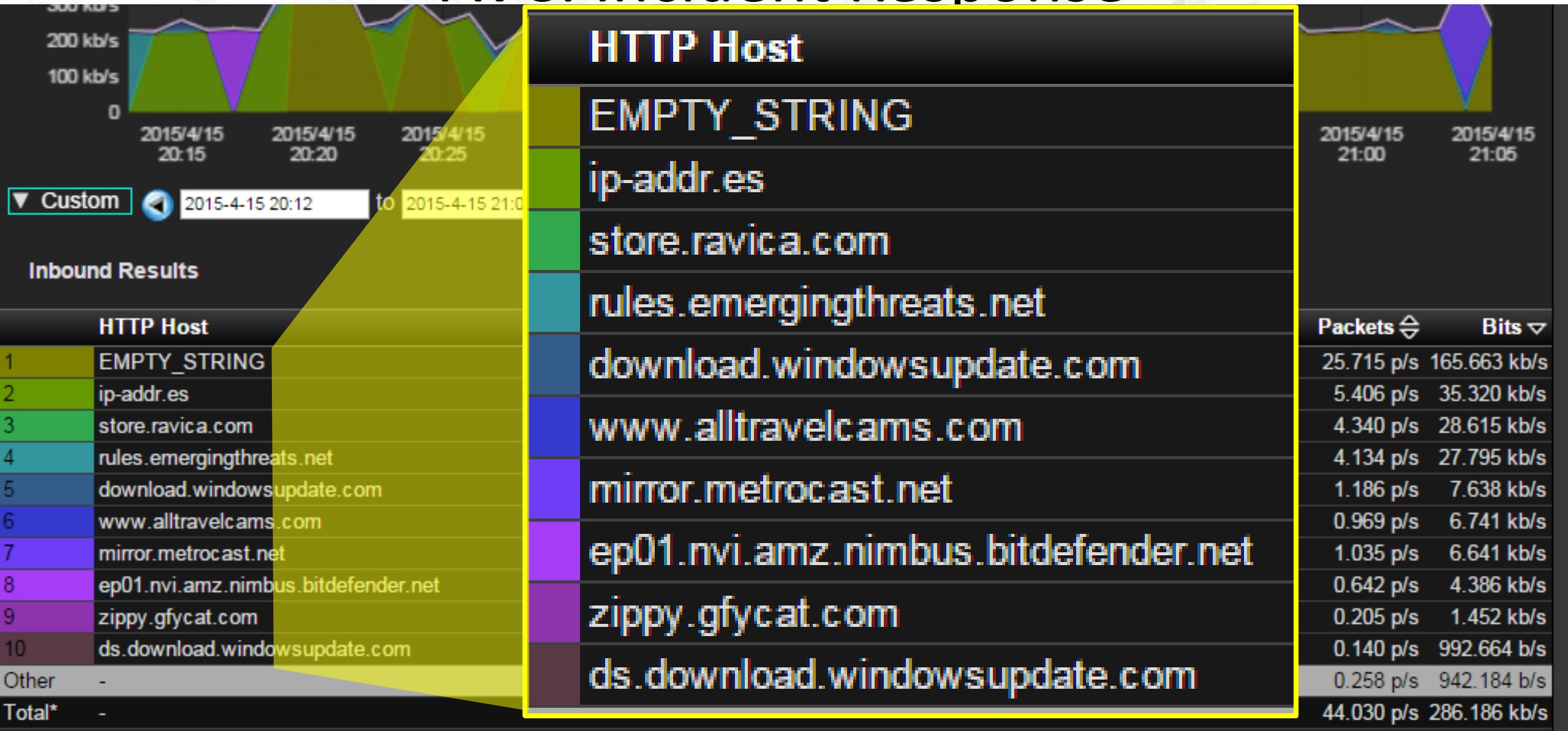
IP

Device	First Seen	Last Seen	Flow Count
10.1.1.251	Tue Nov 24 15:11:00 2015	Tue Jan 26 12:39:00 2016	1305769
10.1.1.3	Tue Nov 24 15:11:00 2015	Tue Jan 26 12:39:00 2016	733513
10.1.1.7	Tue Nov 24 15:16:00 2015	Sat Dec 5 18:09:00 2015	31914
10.1.1.9	Fri Dec 4 15:54:00 2015	Fri Dec 4 16:09:00 2015	13
10.1.15.180	Tue Nov 24 15:11:00 2015	Tue Jan 26 12:39:00 2016	236964
10.1.2.29	Sat Dec 5 18:19:00 2015	Sat Dec 5 22:29:00 2015	36
10.1.2.76	Tue Nov 24 15:31:00 2015	Sat Dec 5 18:09:00 2015	34455
10.1.3.1	Sat Dec 5 18:09:00 2015	Sat Dec 5 22:34:00 2015	558
10.1.4.110	Fri Jan 22 09:16:00 2016	Mon Jan 25 17:39:00 2016	77
10.1.4.36	Tue Nov 24 15:16:00 2015	Tue Jan 26 12:39:00 2016	250503
10.30.1.18	Fri Dec 25 11:24:00 2015	Tue Jan 26 10:19:00 2016	15
64.140.243.134	Tue Nov 24 17:41:00 2015	Tue Jan 26 12:29:00 2016	18689
64.140.243.140	Wed Dec 9 20:14:00 2015	Tue Jan 26 07:59:00 2016	15157

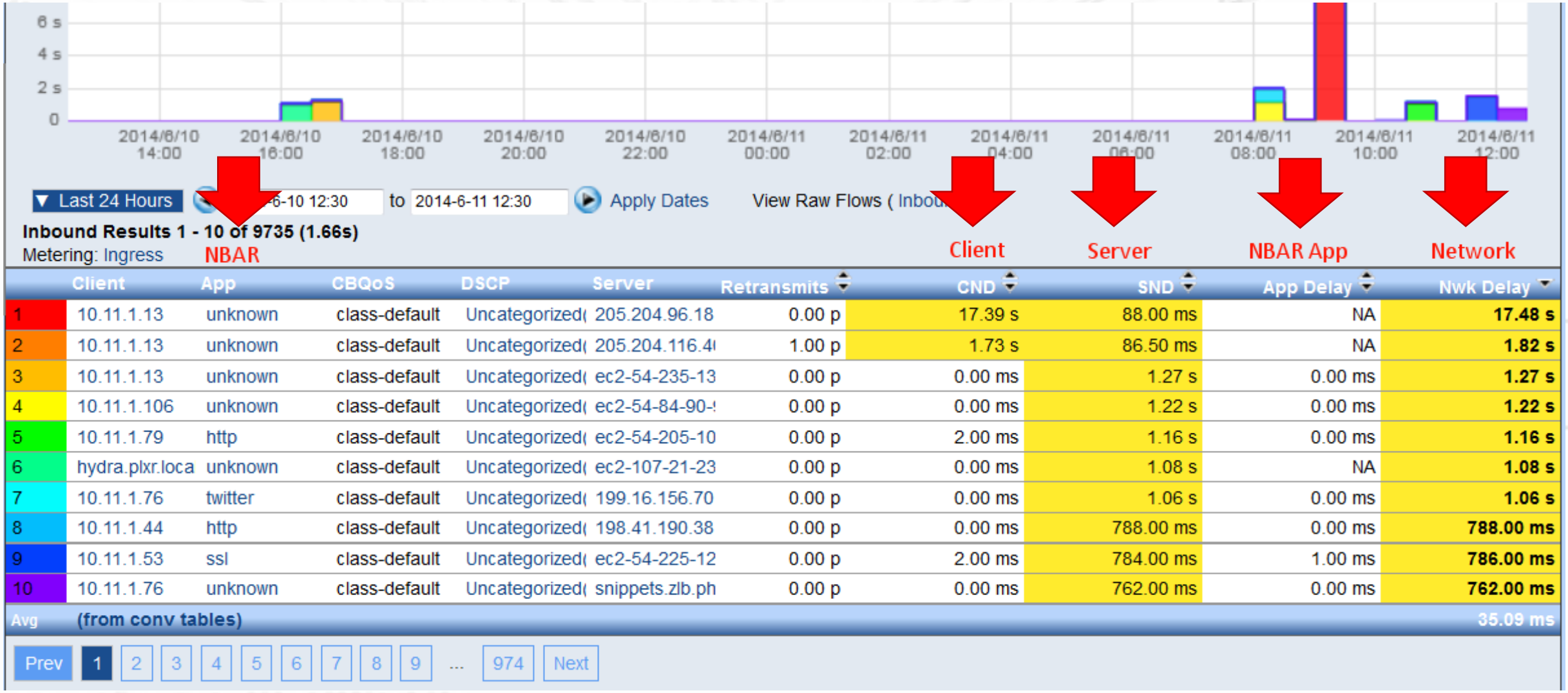
Network as a Sensor: Collect AVC Flows



AVC: Incident Response



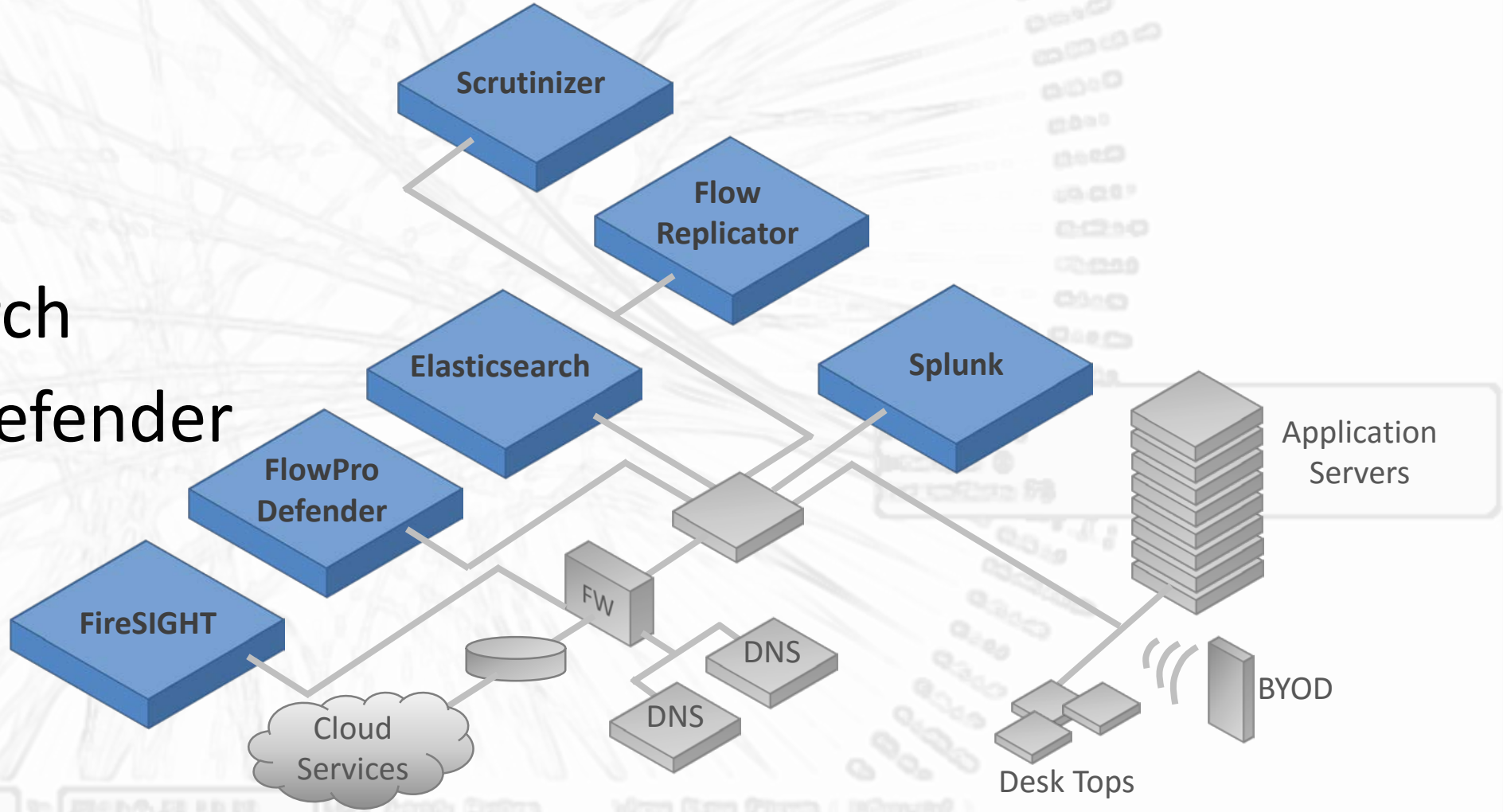
AVC: Performance



	Client	App	CBQoS	DSCP	Server	Retransmits	CND	SND	App Delay	Nwk Delay
1	10.11.1.13	unknown	class-default	Uncategorized(	205.204.96.18	0.00 p	17.39 s	88.00 ms	NA	**17.48 s**
2	10.11.1.13	unknown	class-default	Uncategorized(	205.204.116.4(	1.00 p	1.73 s	86.50 ms	NA	**1.82 s**
3	10.11.1.13	unknown	class-default	Uncategorized(	ec2-54-235-13	0.00 p	0.00 ms	1.27 s	0.00 ms	**1.27 s**
4	10.11.1.106	unknown	class-default	Uncategorized(	ec2-54-84-90-(	0.00 p	0.00 ms	1.22 s	0.00 ms	**1.22 s**
5	10.11.1.79	http	class-default	Uncategorized(	ec2-54-205-10	0.00 p	2.00 ms	1.16 s	0.00 ms	**1.16 s**
6	hydra.plxr.loca	unknown	class-default	Uncategorized(	ec2-107-21-23	0.00 p	0.00 ms	1.08 s	NA	**1.08 s**
7	10.11.1.76	twitter	class-default	Uncategorized(	199.16.156.70	0.00 p	0.00 ms	1.06 s	0.00 ms	**1.06 s**
8	10.11.1.44	http	class-default	Uncategorized(	198.41.190.38	0.00 p	0.00 ms	788.00 ms	0.00 ms	**788.00 ms**
9	10.11.1.53	ssl	class-default	Uncategorized(	ec2-54-225-12	0.00 p	2.00 ms	784.00 ms	1.00 ms	**786.00 ms**
10	10.11.1.76	unknown	class-default	Uncategorized(	snippets.zlb.ph	0.00 p	0.00 ms	762.00 ms	0.00 ms	**762.00 ms**
Avg	(from conv tables)									35.09 ms

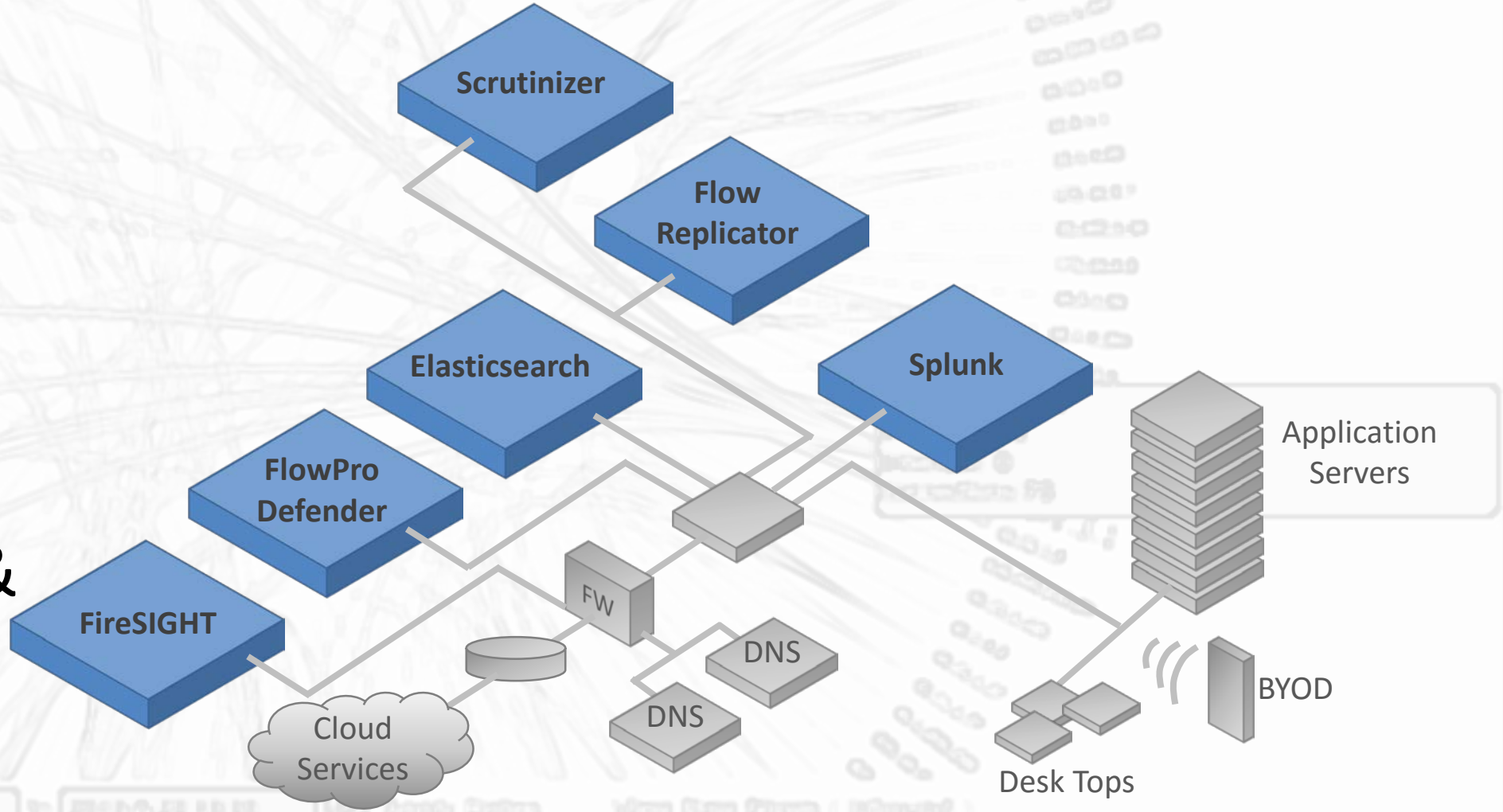
Security as a Platform

- FireSIGHT
- Splunk
- Elasticsearch
- FlowPro Defender

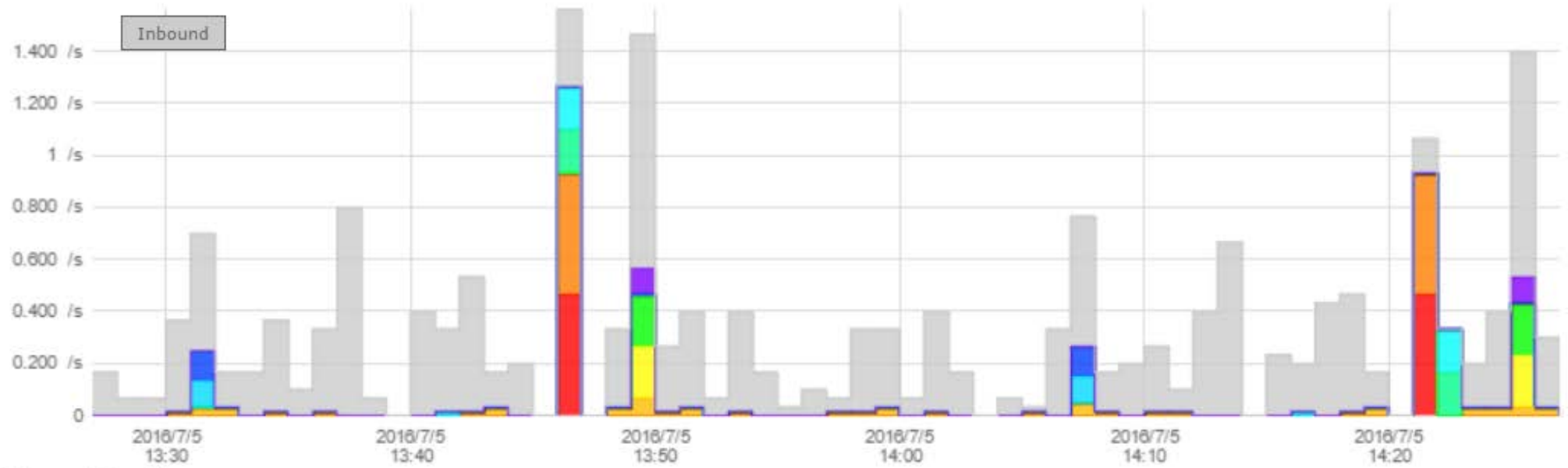


FireSIGHT Integration

- Username
- Application
- FS App
- URL
- HTTP Host
- Web event & Rule Details

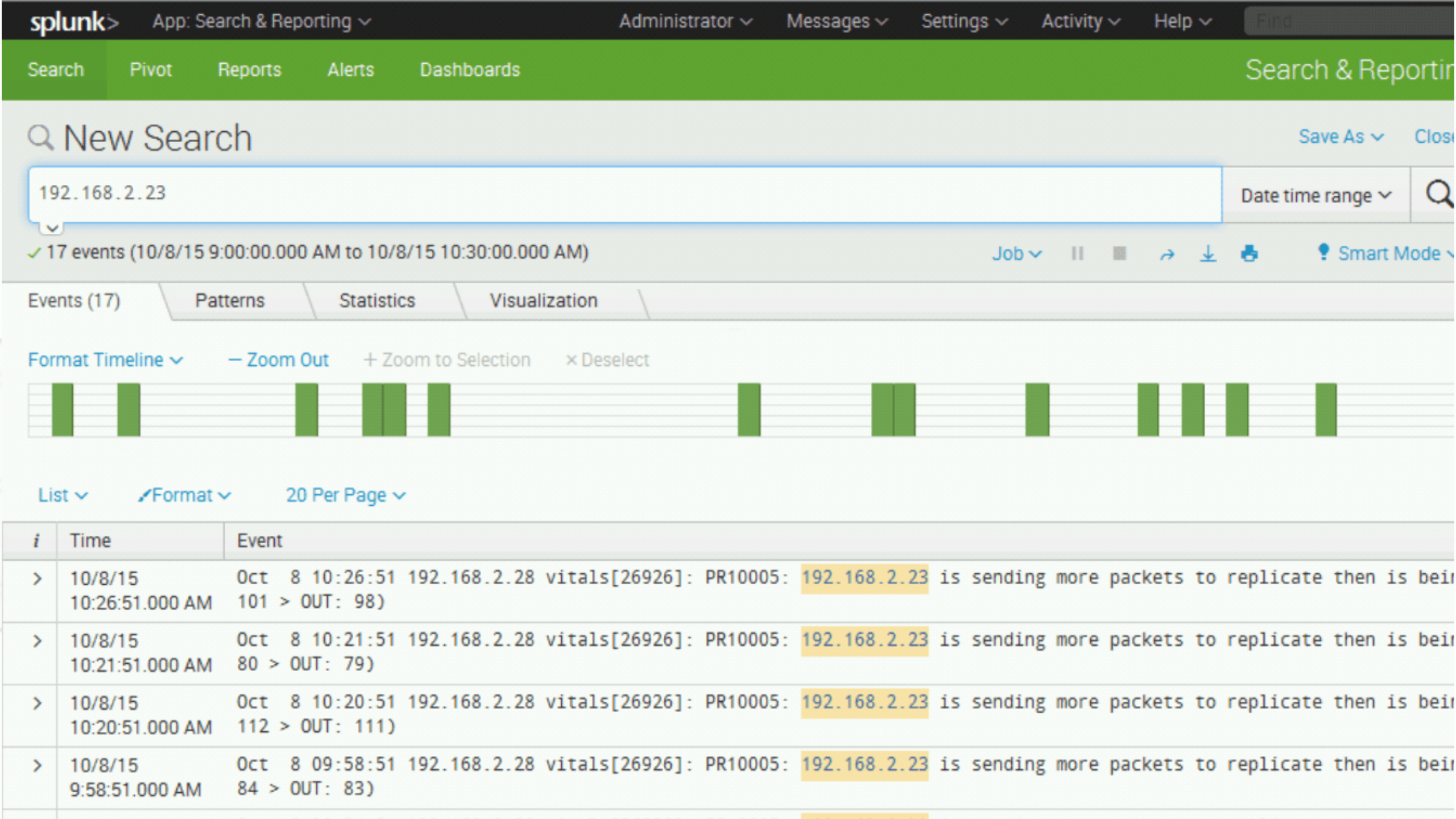


FirePOWER » User App HTTP Host

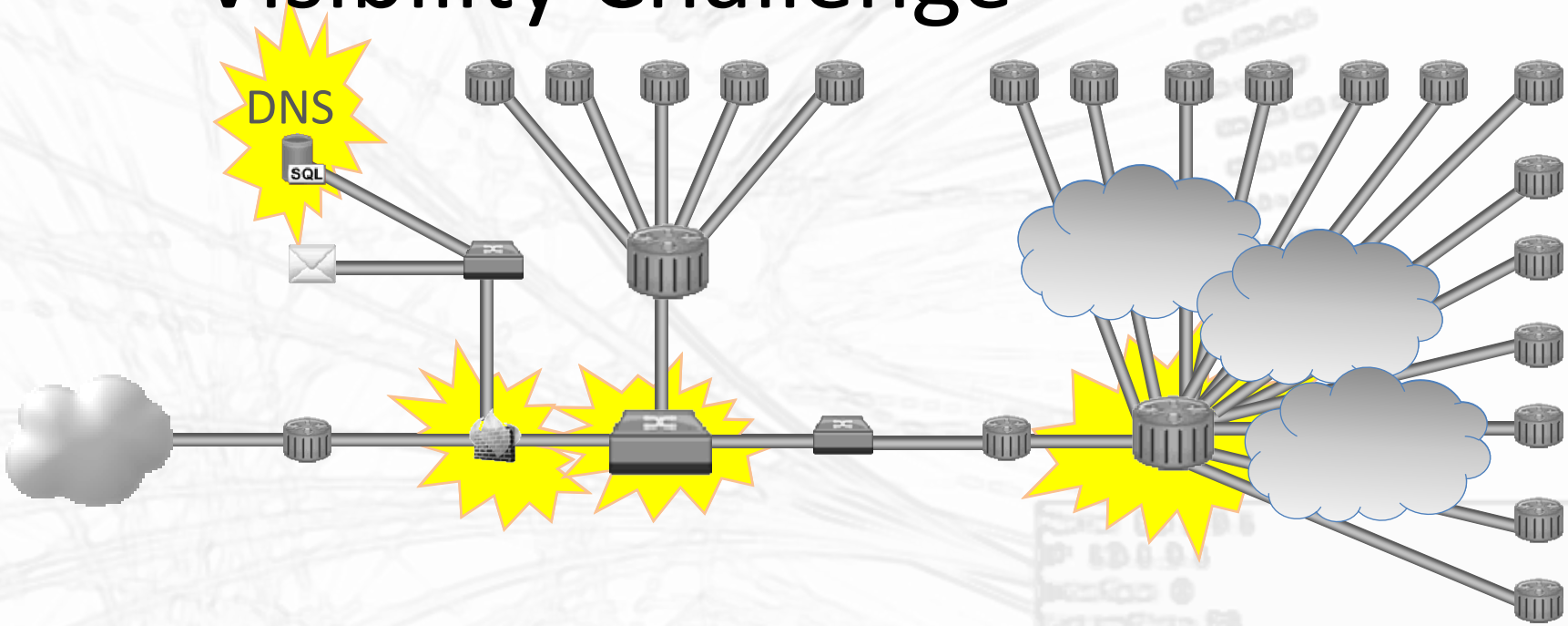


Inbound Results

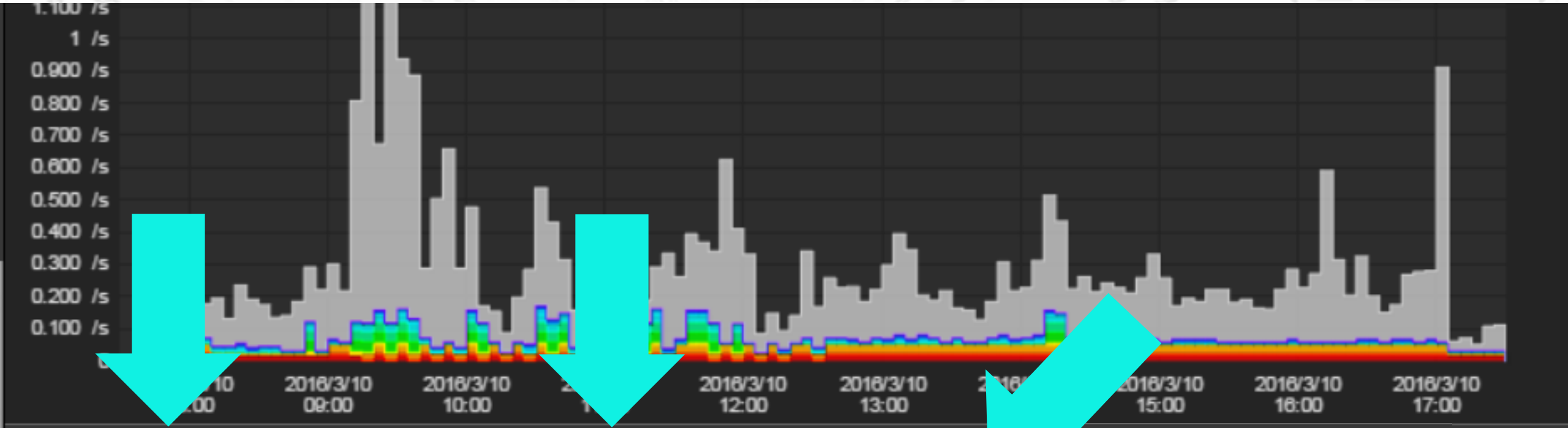
	Source IP	User Name(s)	Application	FS App	HTTP Host	Flows	Bits
1	su69g6h72joannab.plxr.local	plxr/christinau	Chrome	HTTP	assets.myregisteredsite.com	0.016 /s	88.640 b/s
2	64.69.216.234	plxr/christineo	Chrome	HTTP	assets.myregisteredsite.com	0.016 /s	467.280 b/s
3	161.69.25.233	plxr/steve	Internet Explorer	HTTP	vs.mcafeeasap.com	0.012 /s	2.642 kb/s
4	sd4w5ldz1heather.plxr.local	plxr/tyler.pendleton	Chrome	HTTP	www.cantonschools.net	0.007 /s	628.604 b/s
5	dap-209-114-152-190.pri.pm3-...	plxr/calvin.patterson	Chrome	HTTP	www.cantonschools.net	0.007 /s	10.580 kb/s
6	sdcrnl6y1ryann.plxr.local	plxr/philc	Chrome	HTTP	cdn.vidible.tv	0.006 /s	251.449 b/s
7	93.184.215.245	plxr/jeremy.rousselle	Chrome	HTTP	cdn.vidible.tv	0.006 /s	4.391 kb/s
8	a23-208-80-170.deploy.static.ak...	plxr/alexc	Chrome	HTTP	www.cisco.com	0.004 /s	39.454 kb/s
9	192.168.7.104	plxr/chrisp	Chrome	HTTP	www.cisco.com	0.004 /s	947.649 b/s
10	10.60.1.56	plxr/simonj	Firefox	HTTP	tags.tiqcdn.com	0.003 /s	37.093 b/s
Other						0.244 /s	431.543 kb/s


splunk> App: Search & Reporting Administrator Messages Settings Activity Help
Search Pivot Reports Alerts Dashboards Search & Reportin
New Search
Save As Close
192.168.2.23
Date time range
17 events (10/8/15 9:00:00.000 AM to 10/8/15 10:30:00.000 AM)
Job Smart Mode
Events (17) Patterns Statistics Visualization
Format Timeline Zoom Out Zoom to Selection Deselect
List Format 20 Per Page
i Time Event
10/8/15 10:26:51.000 AM Oct 8 10:26:51 192.168.2.28 vitals[26926]: PR10005: 192.168.2.23 is sending more packets to replicate then is bei
101 > OUT: 98)
10/8/15 10:21:51.000 AM Oct 8 10:21:51 192.168.2.28 vitals[26926]: PR10005: 192.168.2.23 is sending more packets to replicate then is bei
80 > OUT: 79)
10/8/15 10:20:51.000 AM Oct 8 10:20:51 192.168.2.28 vitals[26926]: PR10005: 192.168.2.23 is sending more packets to replicate then is bei
112 > OUT: 111)
10/8/15 9:58:51.000 AM Oct 8 09:58:51 192.168.2.28 vitals[26926]: PR10005: 192.168.2.23 is sending more packets to replicate then is bei
84 > OUT: 83)

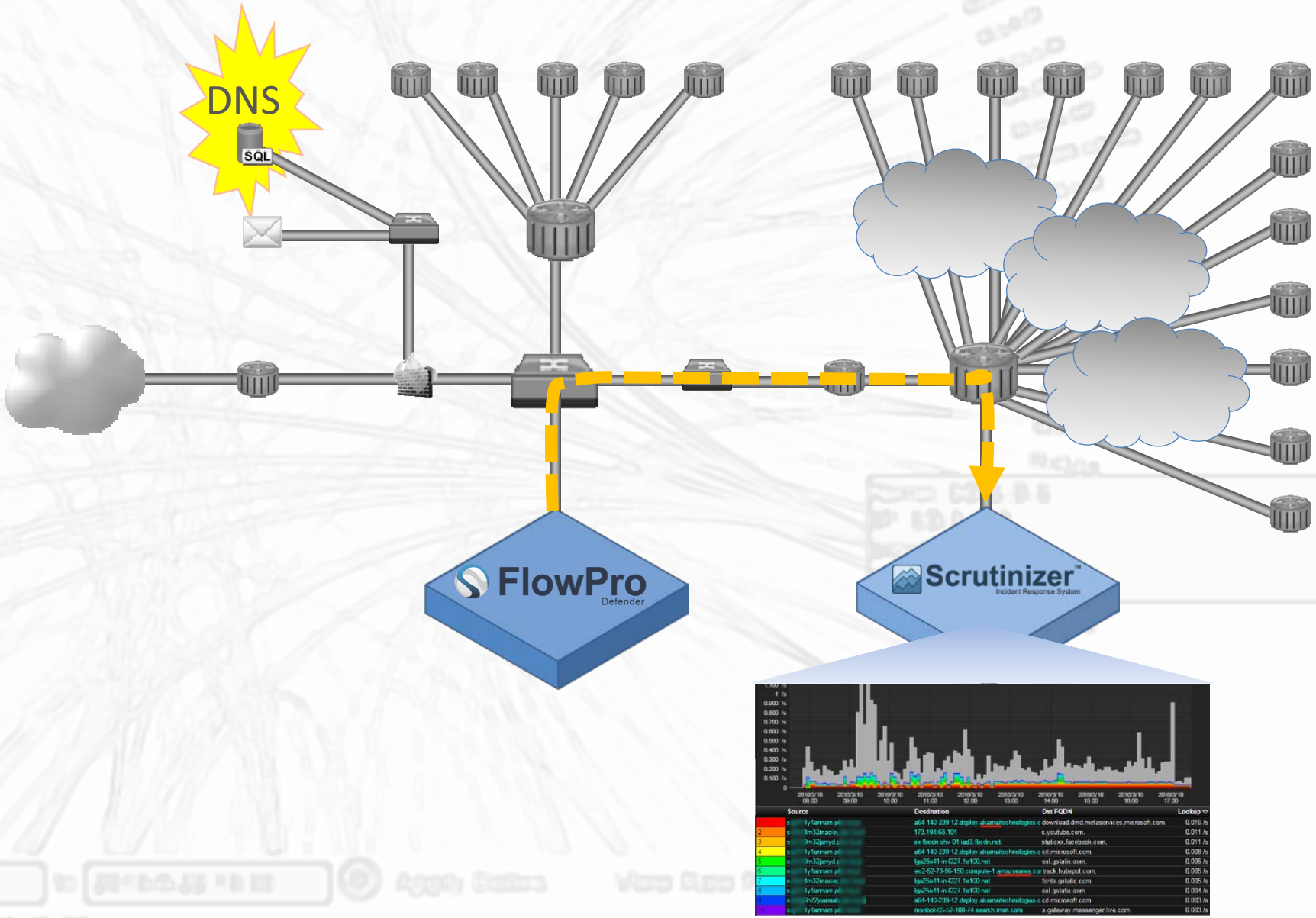
Visibility Challenge

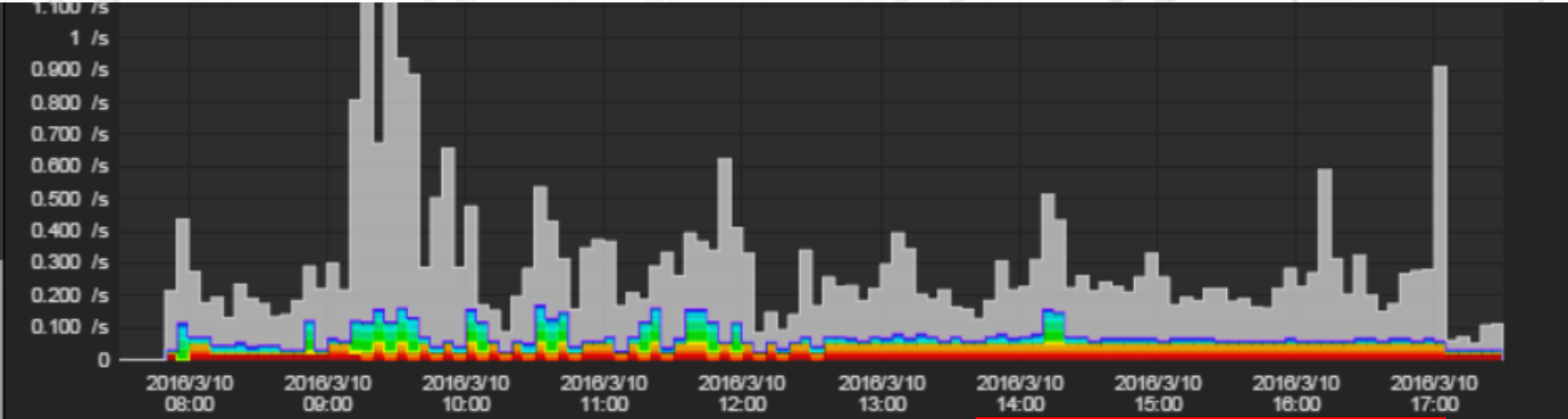


- Cloud, Virtualization, & Encryption make it difficult to collect flow data directly from all source devices.
- Visibility suffers as a result!



	Source	Destination	Lookup
1	s ly1annam.p	a64-140-239-12.deploy.akamaitechnologies.c	0.016 /s
2	s 4m32maciej.	173.194.68.101	0.011 /s
3	s 9m32jarryd.p	xx-fbcdn-shv-01-iad3.fbcdn.net	0.011 /s
4	s ly1annam.p	a64-140-239-12.deploy.akamaitechnologies.c	0.008 /s
5	s 9m32jarryd.p	lga25s41-in-f227.1e100.net	0.006 /s
6	s ly1annam.p	ec2-52-73-56-150.compute-1.amazonaws.co	0.005 /s
7	s 4m32maciej.	lga25s41-in-f227.1e100.net	0.005 /s
8	s ly1annam.p	lga25s41-in-f227.1e100.net	0.004 /s
9	s 6h72joannab	a64-140-239-12.deploy.akamaitechnologies.c	0.003 /s
10	s ly1annam.p	msnbot-65-52-108-74.search.msn.com	0.003 /s

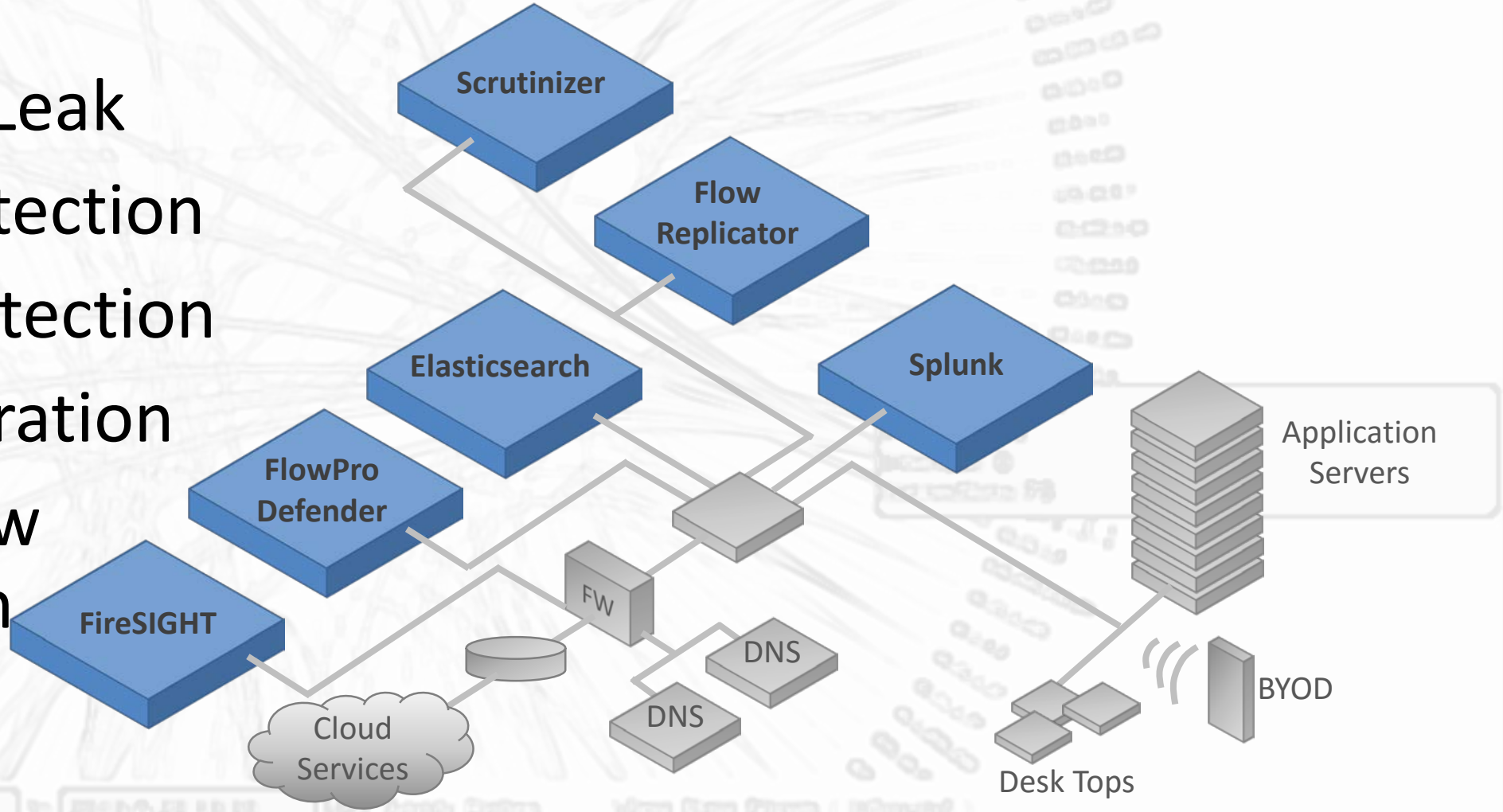

DNS
SQL
FlowPro
Defender
Scrutinizer
Incident Response System



	Source	Destination	Lookup
1	s ly1annam.p	a64-140-239-12.deploy.akamaitechnologies.	0.016 /s
2	s 4m32maciej.	173.194.68.101	0.011 /s
3	s 9m32jarryd.p	xx-fbcdn-shv-01-iad3.fbcdn.net	0.011 /s
4	s ly1annam.p	a64-140-239-12.deploy.akamaitechnologies.	0.008 /s
5	s 9m32jarryd.p	lga25s41-in-f227.1e100.net	0.006 /s
6	s ly1annam.p	ec2-52-73-56-150.compute-1.amazonaws.co	0.005 /s
7	s 4m32maciej.	lga25s41-in-f227.1e100.net	0.005 /s
8	s ly1annam.p	lga25s41-in-f227.1e100.net	0.004 /s
9	s 6h72joannab	a64-140-239-12.deploy.akamaitechnologies.	0.003 /s
10	s ly1annam.p	msnbot-65-52-108-74.search.msn.com	0.003 /s

FlowPro Defender

- DNS Data Leak
- Botnet Detection
- DNS C2 detection
- Data exfiltration
- DNS to flow correlation



Policy	Board Name	Violations	Events	TI	HI
Flow Analytics: DNS Server Detection [Edit] [FA]	Security Events	376	5285	450	42
Flow Analytics: DNS Data Leak [Edit] [FA]	Security Events	1	1	10	1
Flow Analytics: DNS Command and Control Detection [Edit] [FA]	Security Events	1	74	10	1
Flow Analytics: Indicator Correlation Event [Edit] [FA]	Security Events	1	166	10	1
Domain Reputation > Malicious Command & Control Domains [Edit] [FA]	Indicators of Compromise	1	1	10	1
Flow Analytics: Denied Flows [Edit] [FA]	Indicators of Compromise	9	46	5	1
Data Leak [Edit] [FA]	Security Events	5	5	5	1
Flow Analytics: SYN Scan [Edit] [FA]	Indicators of Compromise	1	1	3	1
Flow Analytics: BotNet Detection [Edit] [FA]	Security Events	2	5	2	2
Scrutinizer: Interface Exceeded Threshold [Edit]	Thresholds	26	26	0	1
Scrutinizer Thresh: Exceeded 5 MB in 5 [Edit]	Thresholds	868	868	0	75

DNS Data Leak and Exfiltration

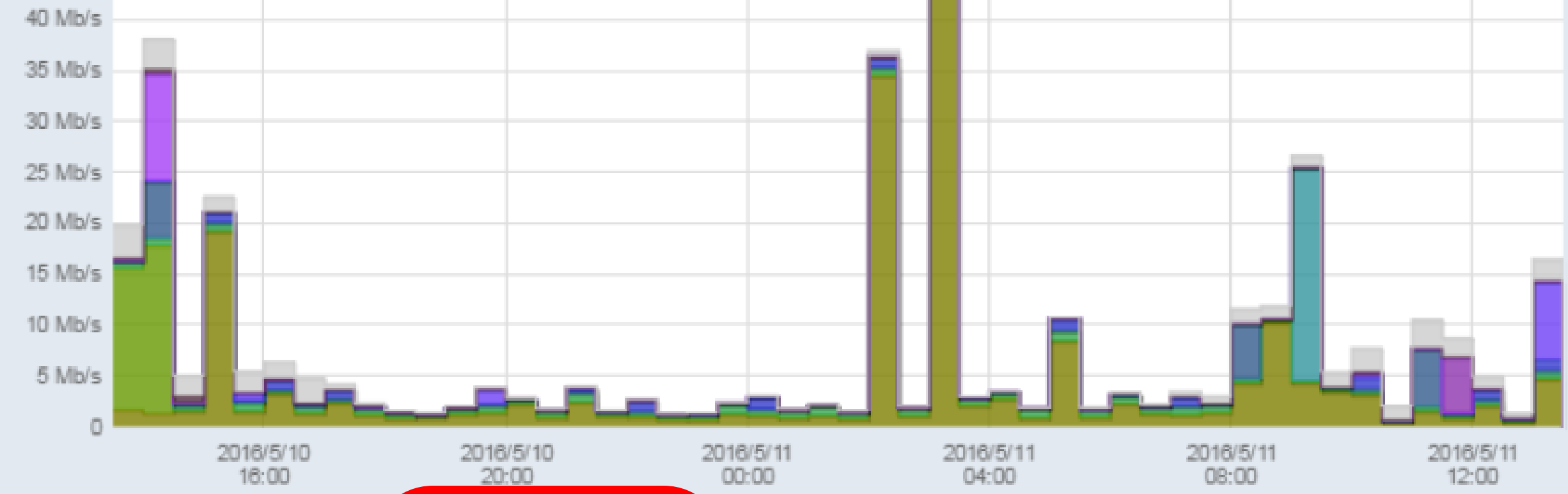
Trusted Vendors are sneaking past your firewall.

c-0.b3000081.50083.15e0.1e2a.36d4.210.0.mfunhzl9whredkfbfe2qvdhiti.**avts.mcafee.com**

1009050090202.000001000.0010101010101010.110100123.dc1a8ae28a4a4ea8938842445c903a91.6b4c217548c84de99d42b0262debd80d.11000.h.00.**mac.sophosxl.net**

Violator Address	Host	Users	Alarm Time	Recent Activity	Duration	Events	Board Name	Message
10.50.3.213	N/A	-	2016-07-05 21:56	N/A	N/A	1	Security Events	<174>DATAEXFIL[2132]: 10.50.3.213,216.58.219.208, Total Byte Exfil: gcs-us-00001.content-storage-download.googleapis.com. gcs-us-00002.content-storage-download.googleapis.com.
10.50.3.199	N/A	-	2016-07-05 21:56	N/A	N/A	1	Security Events	<174>DATAEXFIL[2132]: 10.50.3.199,54.231.32.1, Total Byte Exfil: 174 s3-w-a.us-east-1.amazonaws.com.
10.1.255.251	N/A	-	2016-07-05 21:56	N/A	N/A	1	Security Events	DATAEXFIL[2132]: 10.1.255.251,172.16.2.7, Total Byte Exfil: 797.580000000001
plxrdc01.plxr.local	N/A	-	2016-07-05 21:56	N/A	N/A	1	Security Events	DATAEXFIL[2132]: 10.1.5.1,192.168.5.25, Total Byte Exfil: 831.1
appassure.plxr.local	N/A	-	2016-07-05 21:56	N/A	N/A	1	Security Events	DATAEXFIL[2132]: 10.1.4.144,198.73.18.20, Total Byte Exfil: 53997.6


Identity Services Engine
Version : 1.1.0.912
Username
admin
Password
Login
Remember username
Problem logging in?



	Source	User Name(s)	Packets	Percent	Bits
1	10.1.5.2	plxr/ipfixify	408.301 p/s	51.44 %	4 Mb/s
2	10.1.15.136	plxr/pauld,plxr/pauld-dc	79.867 p/s	8.25 %	641.631 kb/s
3	10.1.4.200	plxr/jakeb,plxr/scottr,plxr...	119.397 p/s	7.67 %	596.535 kb/s
4	10.60.1.139	plxr/mpatters	46.594 p/s	5.80 %	451.121 kb/s
5	10.1.15.170	plxr/austinb	63.770 p/s	4.94 %	384.406 kb/s
6	10.1.4.5	plxr/appassure,plxr/wug	45.385 p/s	3.67 %	285.367 kb/s
7	10.1.4.235	plxr/bugzillaldap,plxr/marc	22.046 p/s	3.12 %	242.626 kb/s
8	10.1.15.233	plxr/ryans	21.720 p/s	2.87 %	223.079 kb/s
9	10.1.15.148	plxr/joanneg	13.456 p/s	1.50 %	116.940 kb/s
10	10.60.1.18	plxr/jarrydb	15.097 p/s	0.63 %	48.832 kb/s

Report:

UNSAVED

Templates Used: 2

Devices Used: 1

Update when filters change

Filters

Where

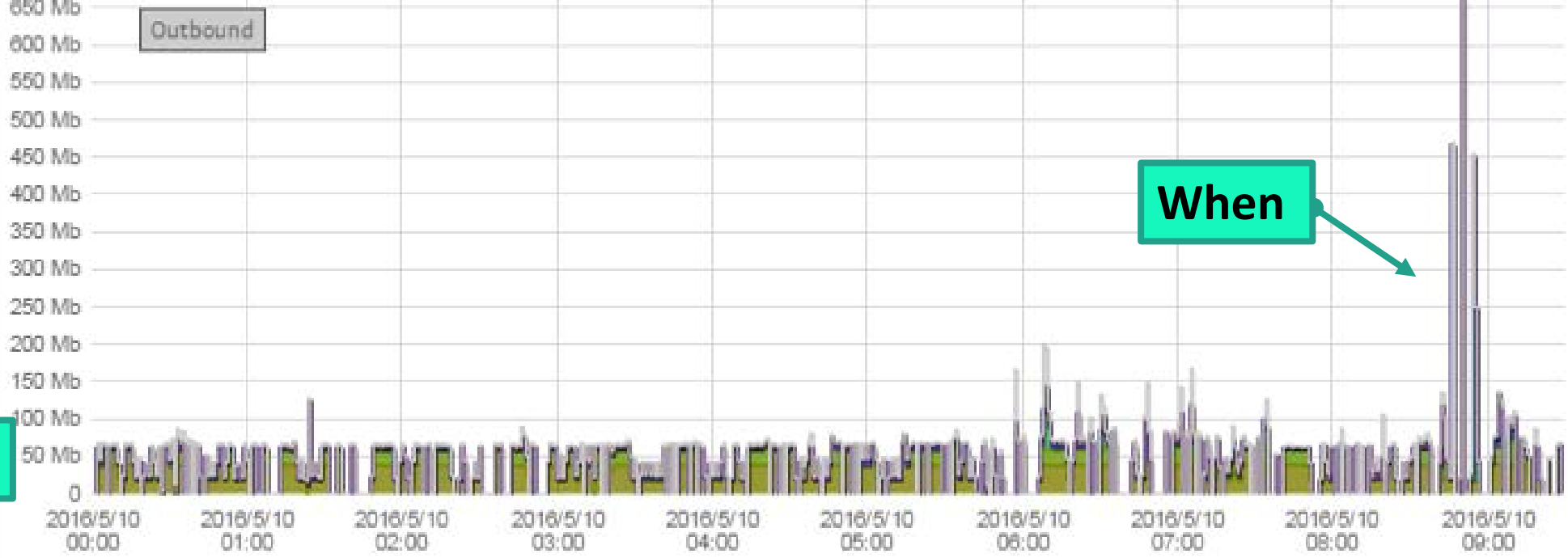
Device/Interface edit x

Device: asa.plxr.local

Interface: 4

Threshold

Add



Outbound Results, speed: 1 Mb/s

	Source	Application	Destination	Bits
1	replicator.plxr.local	HTTP (80 - TCP)	10.2.1.93	19.410 Gb
2	64.140.243.149	HTTPS (443 - UDP)	cpe-184-153-132-96.main..	11.164 Gb
3	64.140.243.149	ipsec-nat-t (4500 - UDP)	107-205-155-52.lightspee...	1.999 Gb
4	devapps.plxr.local	HTTPS (443 - TCP)	192.168.6.6	1.682 Gb
5	64.14	43 - UDP)	c-65-96-245-93.hsd1.nh.	578.960 Mb
6	10.1.225.225	(5901 TCP)	10.2.1.93	488.795 Mb
7	64.140.243.149	ipsec-nat-t (4500 - UDP)	70-127-24-22.res.bhn.net	452.429 Mb
8	10.1.15.49	undefined (19399 TCP)	10.2.1.95	314.981 Mb
9	64.140.243.149	ipsec-nat-t (4500 - UDP)	95.15.227.192.dynamic.tt...	295.837 Mb

Who

What

How much

Thank You for Attending!

Thomas Pore
Director of IT & Services
thomas.pore@plixer.com

www.plixer.com/unc