Flowmon Networks

Modern ways of analyzing traffic in core of your network

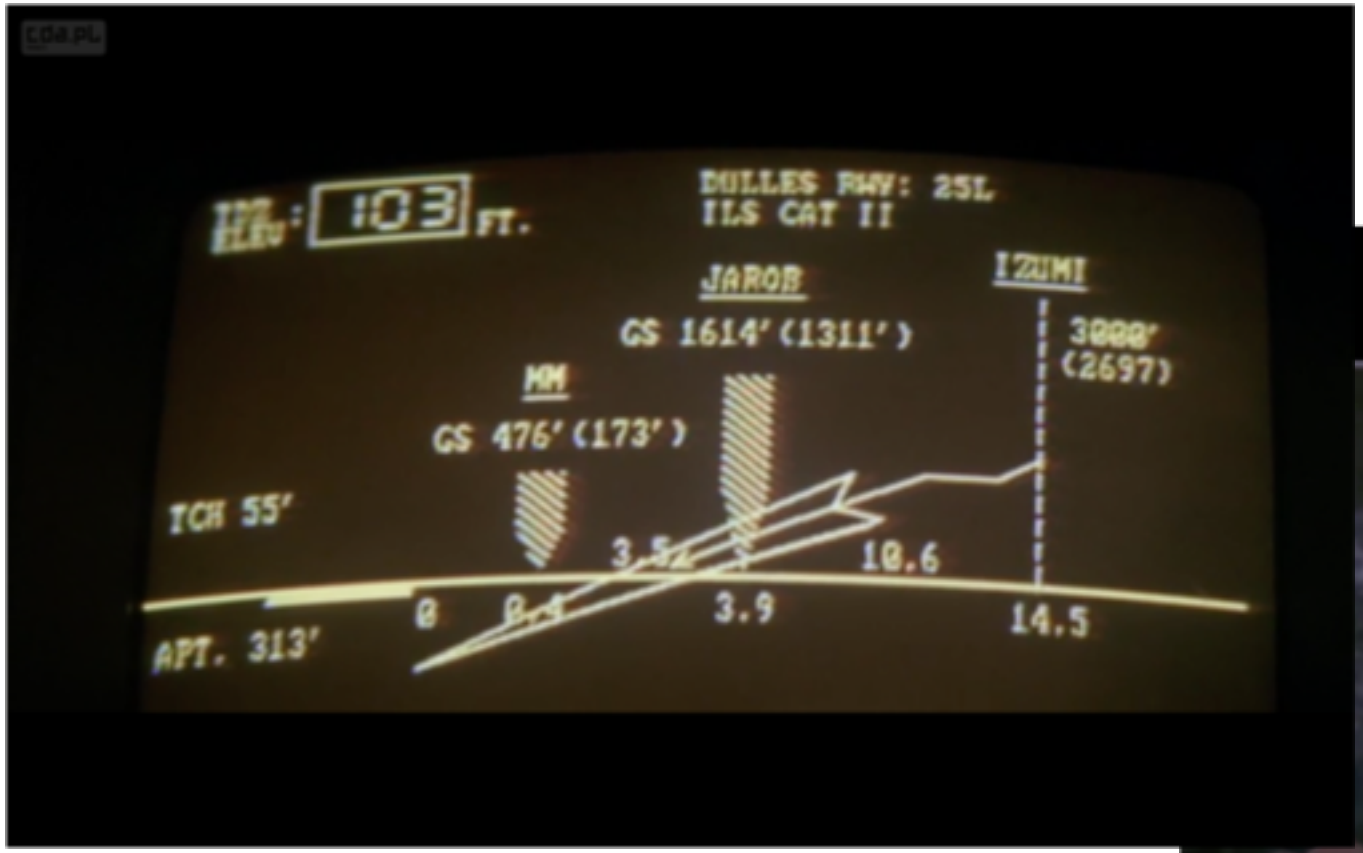
Piotr Tkaczyk
Senior Security Consultant, CLICO

CLICO

CLICO in Europe

- Poland: HQ Kraków, Offices: Katowice, Rzeszów, and Warsaw
- Bulgaria: Sofia
- Croatia: Zagreb
- Czech, Slovakia: Praha
- Romania: Bucharest
- Slovenia: Ljubljana
- Serbia: Belgrade
- Hungary: Budapest
- Strong presence (VAR) in Baltics

First known airport attack



Bad monitoring = totally blindness

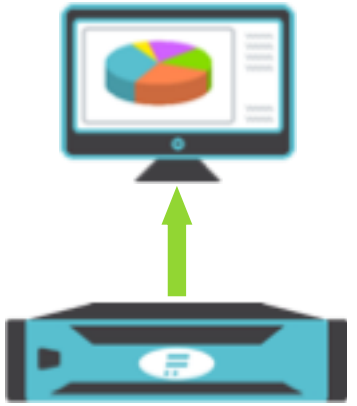
You can’t prevent attack when you’re blind

Flowmon ADS

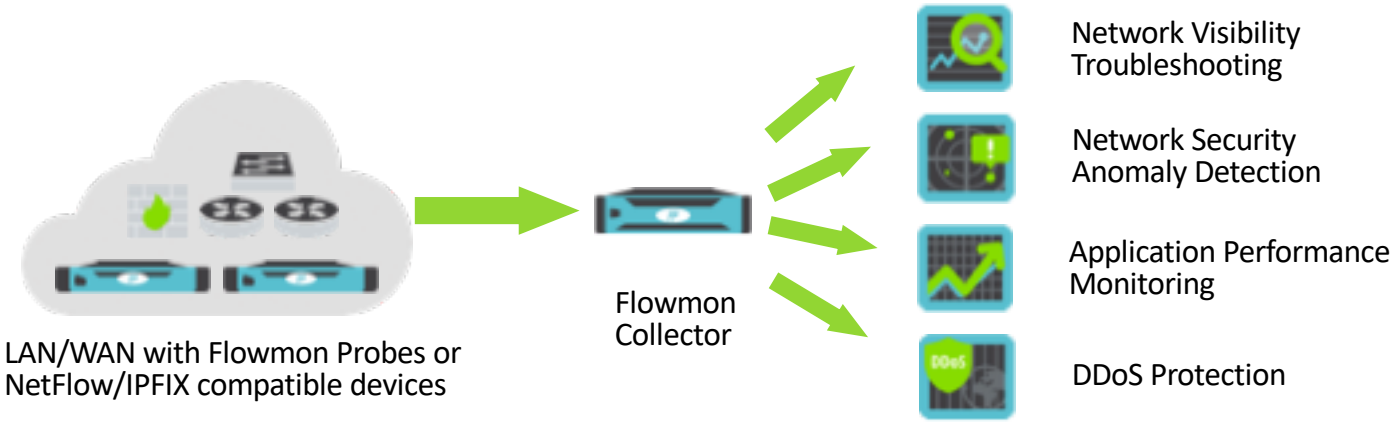
Security Intelligence based on
Network Behavior Analysis

Flowmon Solution

Flowmon Networks



- Real-time network traffic insight
- Flexible drill-down
- Months of history without aggregation
- Thousands of flow sources
- High performance (up to 400k fps per appliance)



Flowmon Solution

Network Traffic Monitoring

Flowmon Probes

- Stand-alone passive sources of network statistics (NetFlow / IPFIX)

Flowmon Collector

- Storing, visualization and analysis of network statistics

Flowmon Modules

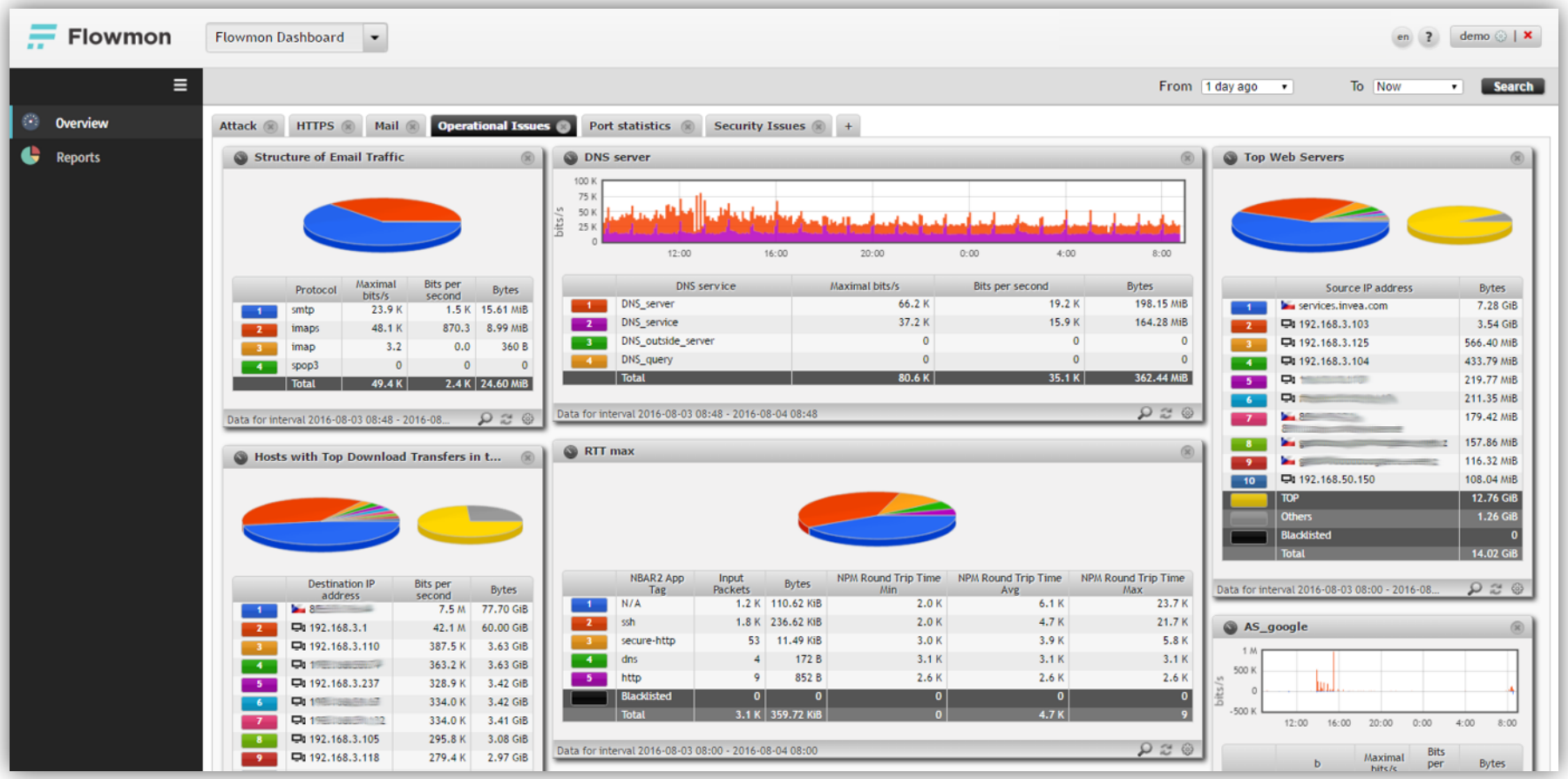
- Anomaly detection, traffic capture, Application Performance Monitoring, DDoS attacks detection and mitigation

Flowmon Web GUI

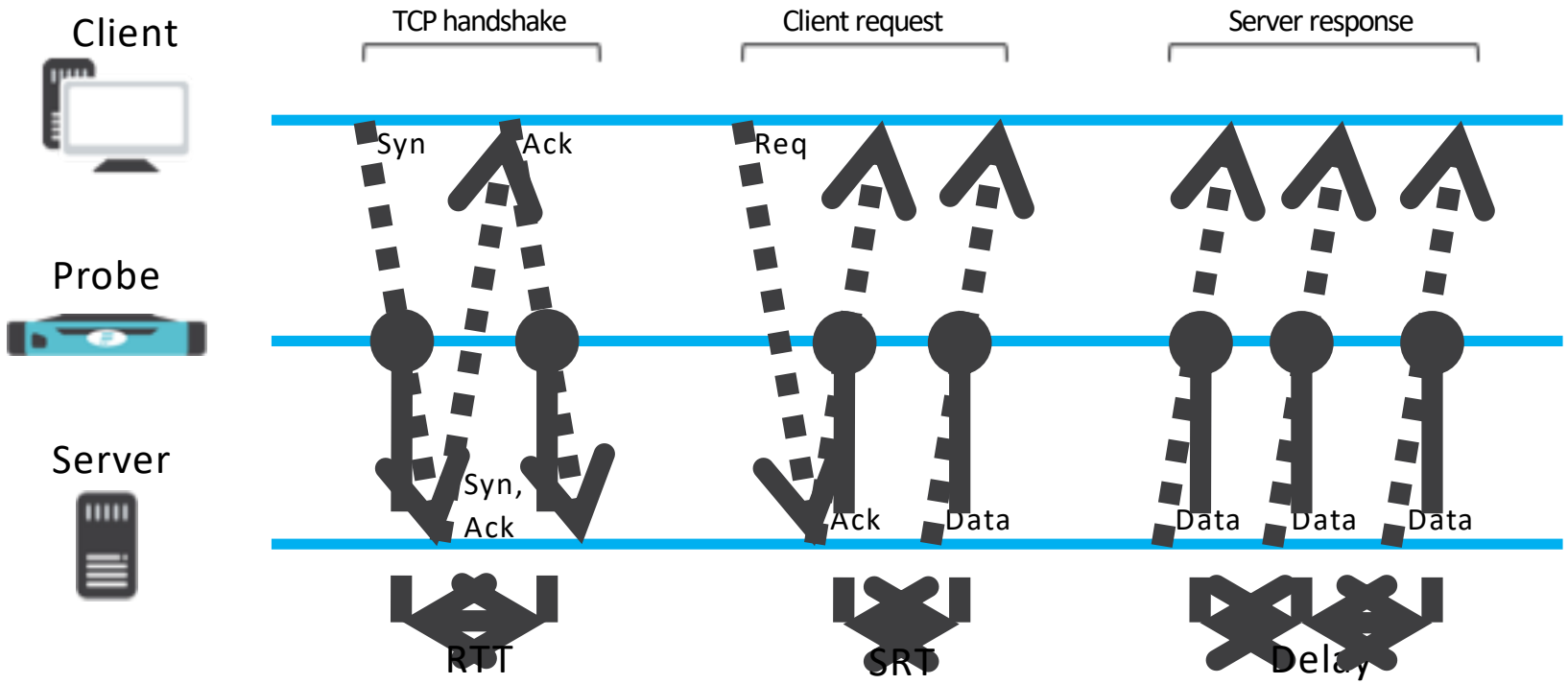
- User-friendly web interface with secure access (HTTPS)
- Probe/Collector parameters settings – FCC
- Visualization of statistics on built-in collector – FMC
- Central dashboard – FMD

Flowmon Dashboard (FMD)

- Combines widgets and reports from different modules
  - In current version supports FMC, ADS



Performance Monitoring



Round Trip Time – **delay introduced by network**

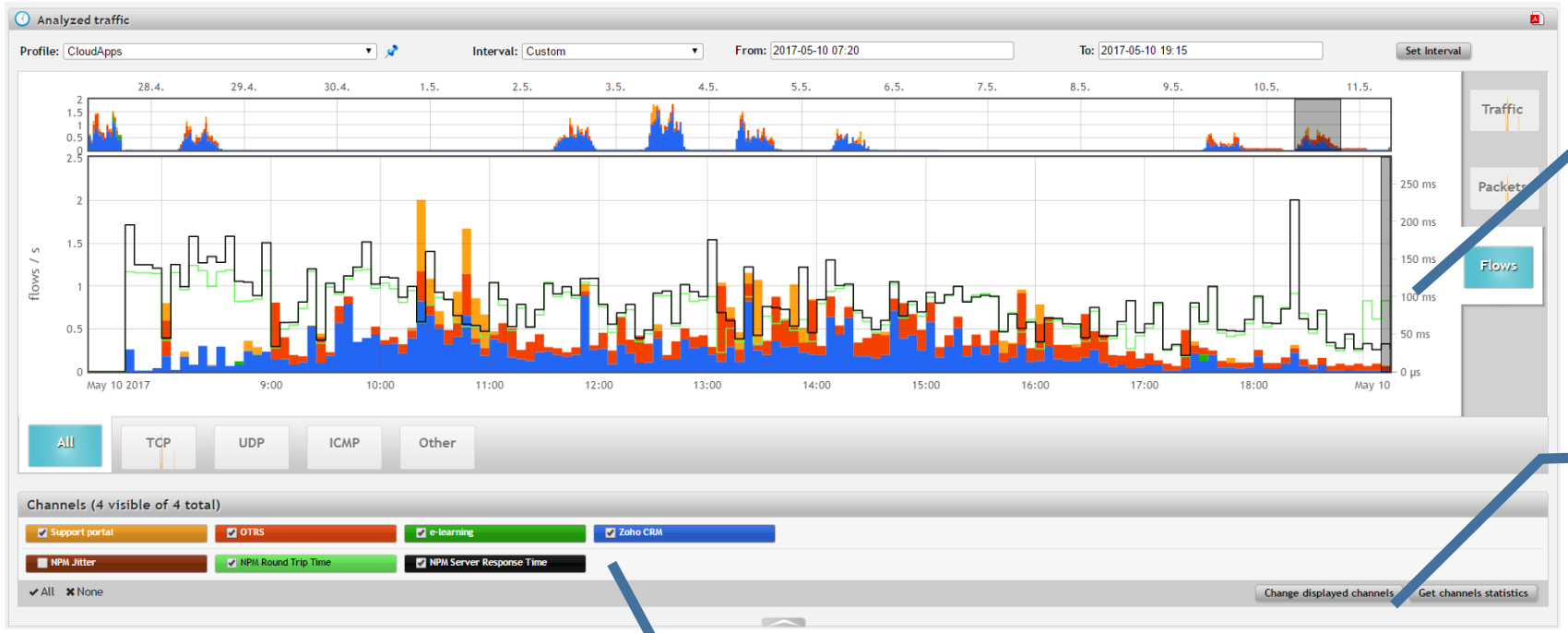
Server Response Time – **delay introduced by server/application**

Delay (min, max, avg, deviation) – **delays between packets**

Jitter (min, max, avg, deviation) – **variance of delays between packets**

Network Performance Visualization

- Visualize network performance metrics over time frame
  - RTT, SRT, Jitter per profile/channel



Y axis on the right side of traffic chart

Change of displayed channels

Selection of current view

Monitoring of Cloud applications

- Identify individual cloud applications
  - Detailed visibility into HTTP, both traffic directions (request, response)

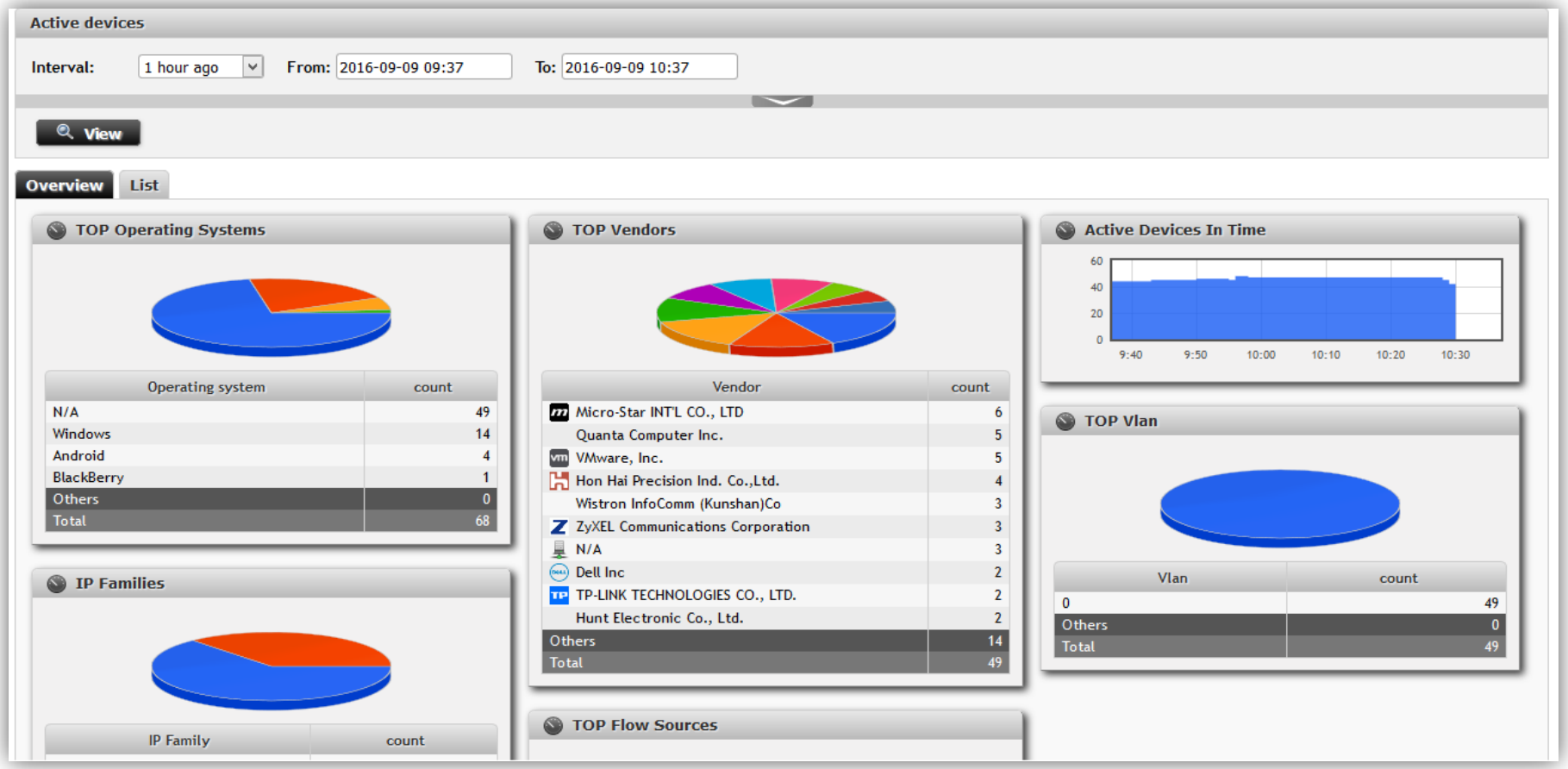
Start Time - first seen	Duration	Source IP address	Destination IP address	Hostname	Source port	Destination port	Packets	Bytes	HTTP method	HTTP result code	Source AS	Destination AS
2017-05-10 13:15:34.060	4 m, 59.998 s	8.40.222.57	192.168.70.78	wms0.zoho.com	https	58122	11	1023	SSL	0	ZOHO	0
2017-05-10 13:15:34.254	4 m, 59.672 s	192.168.70.78	8.40.222.57	wms0.zoho.com	58122	https	20	1330	SSL	0	0	ZOHO
2017-05-10 13:15:42.175	4 m, 30.357 s	192.168.70.76	8.40.222.57	wms1.zoho.com	53311	https	20	1330	SSL	0	0	ZOHO
2017-05-10 13:15:42.292	4 m, 59.945 s	192.168.70.76	8.40.222.57	wms4.zoho.com	62545	https	21	1423	SSL	0	0	ZOHO
2017-05-10 13:15:42.307	4 m, 30.155 s	8.40.222.57	192.168.70.76	wms1.zoho.com	https	53311	10	930	SSL	0	ZOHO	0
2017-05-10 13:15:42.425	4 m, 30.020 s	8.40.222.57	192.168.70.76	wms4.zoho.com	https	62545	10	930	SSL	0	ZOHO	0
2017-05-10 13:15:50.273	4 m, 30.223 s	192.168.70.207	8.40.222.57	wms8.zoho.com	52756	https	20	1330	SSL	0	0	ZOHO
2017-05-10 13:15:50.278	4 m, 30.217 s	192.168.70.207	8.40.222.57	wms.zoho.com	52754	https	20	1330	SSL	0	0	ZOHO
2017-05-10 13:15:50.408	4 m, 30.036 s	8.40.222.57	192.168.70.207	wms8.zoho.com	https	52756	10	930	SSL	0	ZOHO	0
2017-05-10 13:15:50.414	4 m, 30.029 s	8.40.222.57	192.168.70.207	wms.zoho.com	https	52754	10	930	SSL	0	ZOHO	0
2017-05-10 13:16:04.141	4 m, 30.187 s	192.168.70.24	8.40.222.57	wms1.zoho.com	53330	https	20	1330	SSL	0	0	ZOHO
2017-05-10 13:16:04.275	4 m, 30.002 s	8.40.222.57	192.168.70.24	wms1.zoho.com	https	53330	10	930	SSL	0	ZOHO	0
2017-05-10 13:16:20.262	4 m, 59.995 s	8.40.222.57	192.168.70.25	wms3.zoho.com	https	52575	11	1023	SSL	0	ZOHO	0
2017-05-10 13:16:20.399	4 m, 59.727 s	192.168.70.25	8.40.222.57	wms3.zoho.com	52575	https	20	1330	SSL	0	0	ZOHO
2017-05-10 13:16:34.796	4 m, 30.185 s	192.168.70.13	8.40.222.57	wms.zoho.com	63328	https	20	1330	SSL	0	0	ZOHO
2017-05-10 13:16:34.929	4 m, 30.003 s	8.40.222.57	192.168.70.13	wms.zoho.com	https	63328	10	930	SSL	0	ZOHO	0
2017-05-10 13:16:53.318	4 m, 59.973 s	192.168.90.30	8.40.222.57	wms.zoho.com	56720	https	21	1423	SSL	0	0	ZOHO
2017-05-10 13:16:53.450	4 m, 29.977 s	8.40.222.57	192.168.90.30	wms.zoho.com	https	56720	10	930	SSL	0	ZOHO	0
2017-05-10 13:17:04.794	4 m, 30.188 s	192.168.70.13	8.40.222.57	wms0.zoho.com	63405	https	20	1330	SSL	0	0	ZOHO
2017-05-10 13:17:04.928	4 m, 30.003 s	8.40.222.57	192.168.70.13	wms0.zoho.com	https	63405	10	930	SSL	0	ZOHO	0
										Flows 246	Bytes 2.6 M	Packets 4.33 K

Information included in both traffic directions

Visibility into HTTP & HTTPS (SNI)

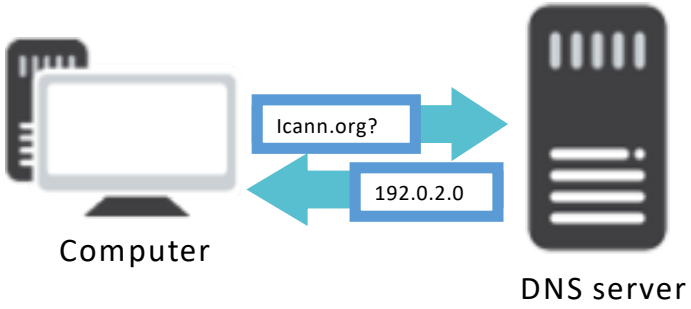
Active Devices

- IP versus MAC mapping including history
  - VLAN, Host OS, User ID, Vendor identification



Analysis of DNS traffic

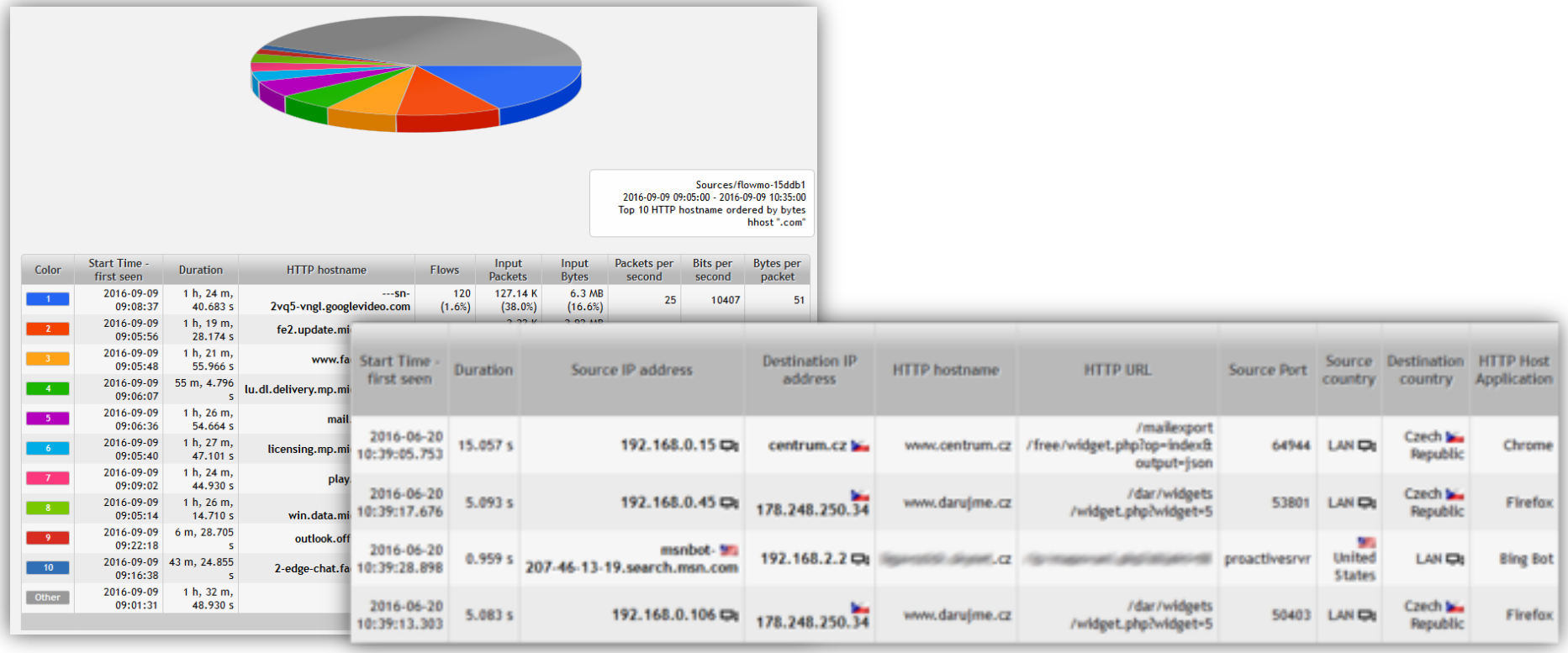
- DNS (Domain Name System)
  - Full visibility into DNS queries and replies
    - domain, type of query, return value
  - Various use cases
    - Malware and botnet detection
    - Spoofed IPs and domains
    - Troubleshooting



Start Time - first seen	Source IP address	Destination IP address	DNS Query/Response	DNS Question type	DNS Question name	DNS Response name	DNS Response type	DNS Response code	DNS Response data
2015-09-06 14:04:21.010	192.168.222.42	192.168.222.1	Query	A	xpu.samsungelectronics.com		N/A	NoError	
2015-09-06 14:04:21.029	192.168.222.1	192.168.222.42	Response	A	xpu.samsungelectronics.com	xpu.samsungelectronics.com	A	NoError	54.235.219.101
2015-09-06 14:04:29.116	192.168.222.47	192.168.222.1	Query	A	meteor.androworks.org		N/A	NoError	
2015-09-06 14:04:29.136	192.168.222.1	192.168.222.47	Response	A	meteor.androworks.org	meteor.androworks.org	A	NoError	62.109.133.45
2015-09-06 14:04:37.060	192.168.222.37	192.168.222.1	Query	A	invea.invea.cz		N/A	NoError	
2015-09-06 14:04:37.063	192.168.222.1	192.168.222.37	Response	A	invea.invea.cz	invea.invea.cz	A	NoError	89.185.252.10
2015-09-06 14:05:45.085	192.168.222.37	192.168.222.1	Query	A	clients4.google.com		N/A	NoError	
2015-09-06 14:05:45.088	192.168.222.1	192.168.222.37	Response	A	clients4.google.com	clients4.google.com	CNAME	NoError	clients.l.google.com

Analysis of HTTP traffic

- HTTP and HTTPS L7 visibility
  - User Agent analysis (OS, HTTP APP)
  - Server name indication even for HTTPS (SNI)

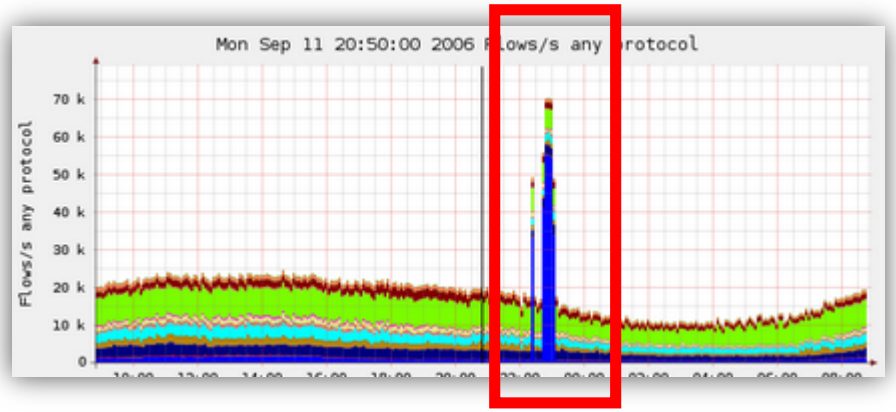


Color	Start Time - first seen	Duration	HTTP hostname	Flows	Input Packets	Input Bytes	Packets per second	Bits per second	Bytes per packet
1	2016-09-09 09:08:37	1 h, 24 m, 40.683 s	---sn-2vq5-vngl.googlevideo.com	120 (1.6%)	127.14 K (38.0%)	6.3 MB (16.6%)	25	10407	51
2	2016-09-09 09:05:56	1 h, 19 m, 28.174 s	fe2.update.mi						
3	2016-09-09 09:05:48	1 h, 21 m, 55.966 s	www.fa						
4	2016-09-09 09:06:07	55 m, 4.796 s	lu.dl.delivery.mp.mi						
5	2016-09-09 09:06:36	1 h, 26 m, 54.664 s	mail						
6	2016-09-09 09:05:40	1 h, 27 m, 47.101 s	licensing.mp.mi						
7	2016-09-09 09:09:02	1 h, 24 m, 44.930 s	play						
8	2016-09-09 09:05:14	1 h, 26 m, 14.710 s	win.data.mi						
9	2016-09-09 09:22:18	6 m, 28.705 s	outlook.off						
10	2016-09-09 09:16:38	43 m, 24.855 s	2-edge-chat.fa						
Other	2016-09-09 09:01:31	1 h, 32 m, 48.930 s							

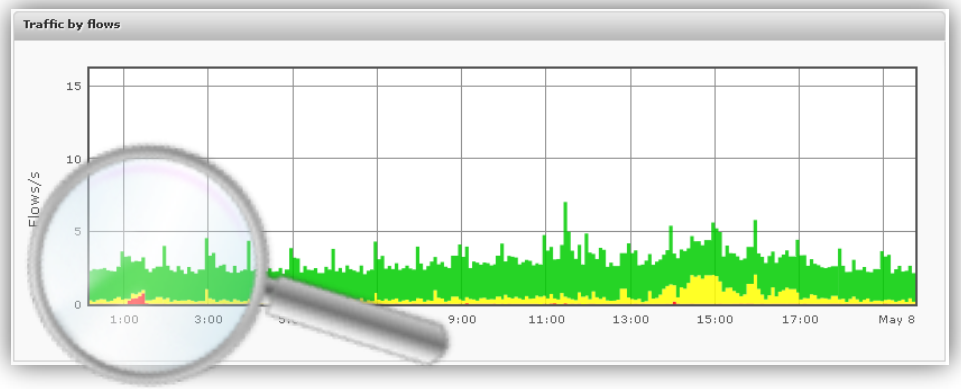
Start Time - first seen	Duration	Source IP address	Destination IP address	HTTP hostname	HTTP URL	Source Port	Source country	Destination country	HTTP Host Application
2016-06-20 10:39:05.753	15.057 s	192.168.0.15	centrum.cz	www.centrum.cz	/mailexport /free/widget.php?op=index&output=json	64944	LAN	Czech Republic	Chrome
2016-06-20 10:39:17.676	5.093 s	192.168.0.45	178.248.250.34	www.darujme.cz	/dar/widgets /widget.php?widget=5	53801	LAN	Czech Republic	Firefox
2016-06-20 10:39:28.898	0.959 s	msnbot-207-46-13-19.search.msn.com	192.168.2.2	[redacted]	[redacted]	proactivesrvr	United States	LAN	Bing Bot
2016-06-20 10:39:13.303	5.083 s	192.168.0.106	178.248.250.34	www.darujme.cz	/dar/widgets /widget.php?widget=5	50403	LAN	Czech Republic	Firefox

Anomaly Detection

- How is Flowmon different from other tools?



Common tools use statistical methods to detect traffic spikes and deviations



Flowmon analyzes each flow and goes beyond the traditional statistical algorithms

Flowmon ADS Principles

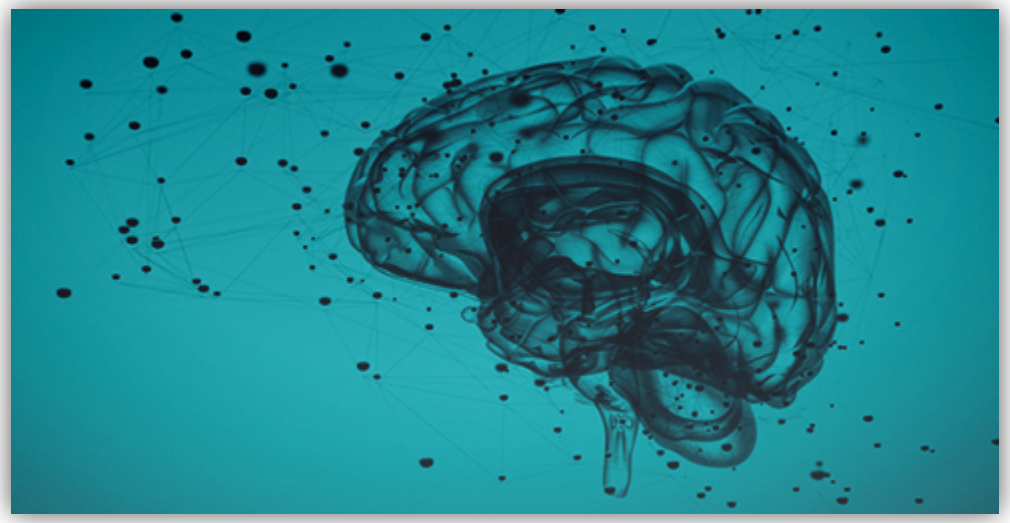
Flowmon Networks

Flowmon ADS

- Machine Learning
- Adaptive Baselining
- Heuristics
- Behavior Patterns
- Reputation Databases

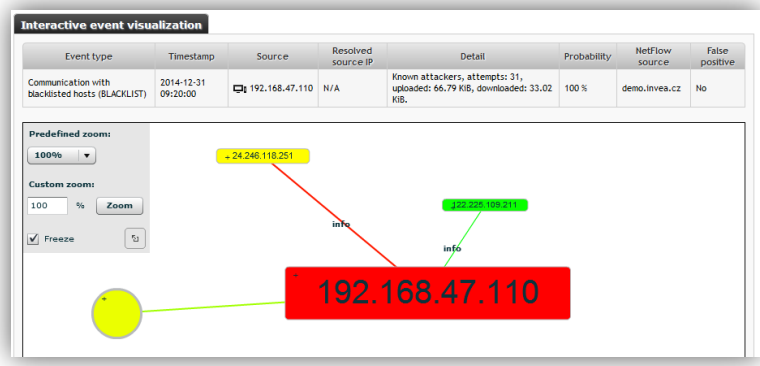
Flowmon Threat Intelligence

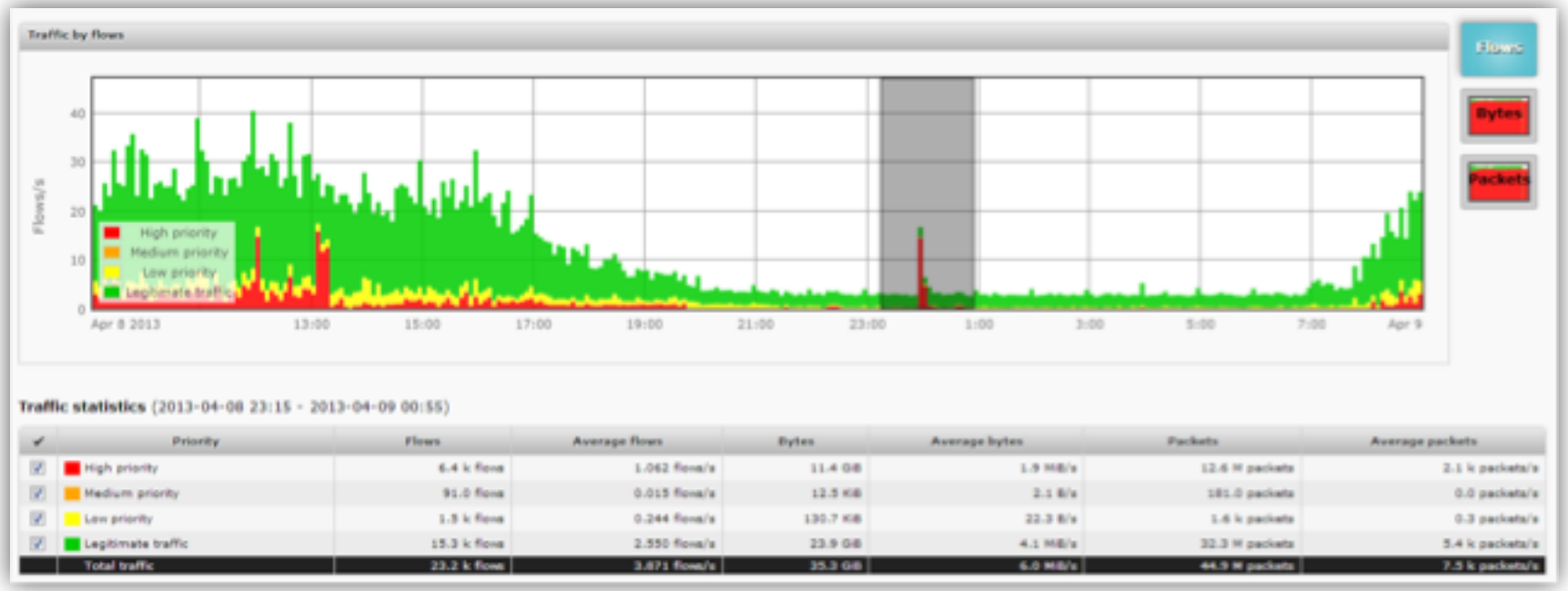
- IP and host-based reputation feeds
- Detection of C&C domains, P2P botnets, phishing
  - IP addresses (available)
  - HTTP host names (available, probe needed)
  - Domain names (probe needed)



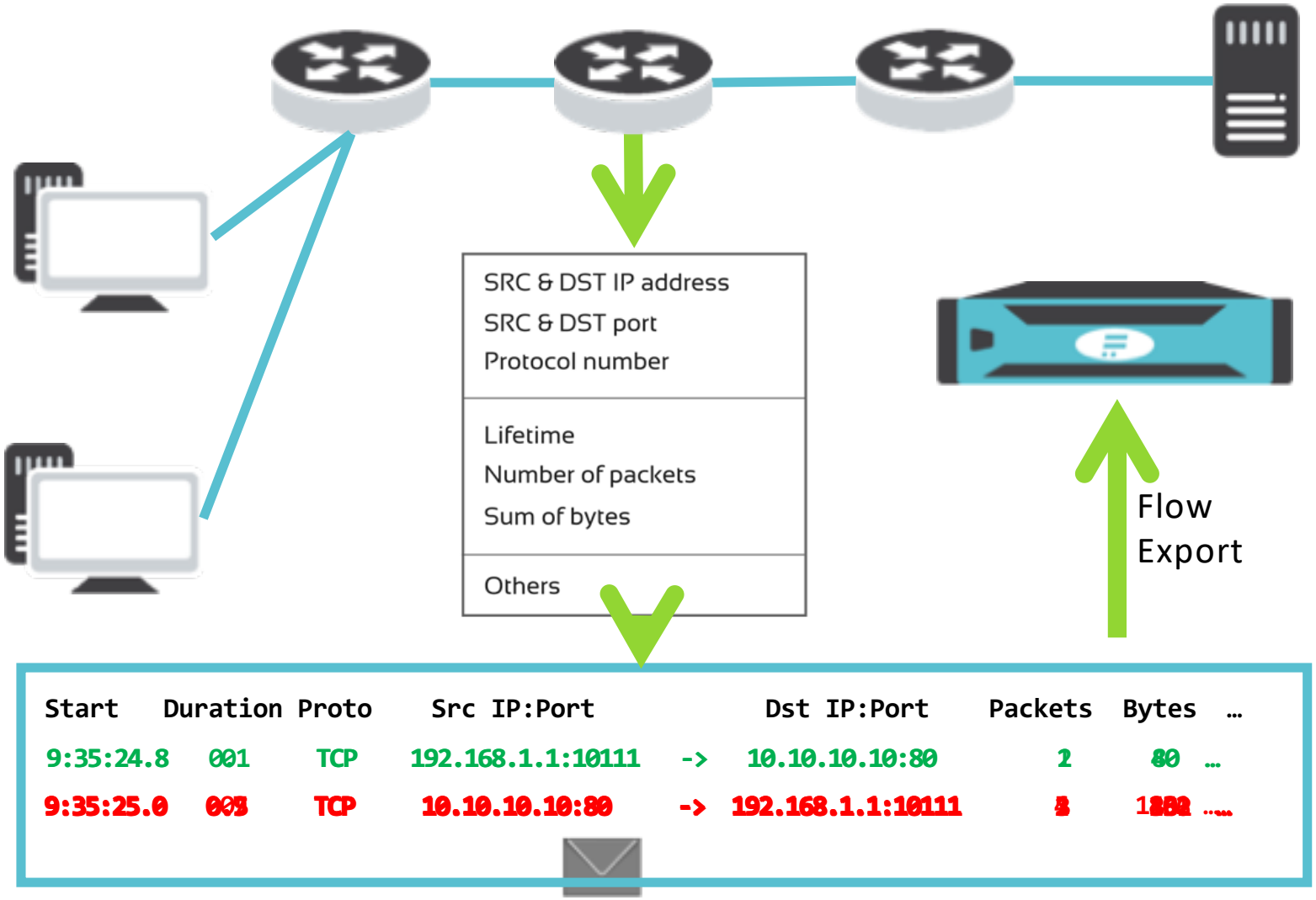
Incident Evidence Visualization

- Insight and visual analytics
  - Dashboards and reports
  - Interactive visualization

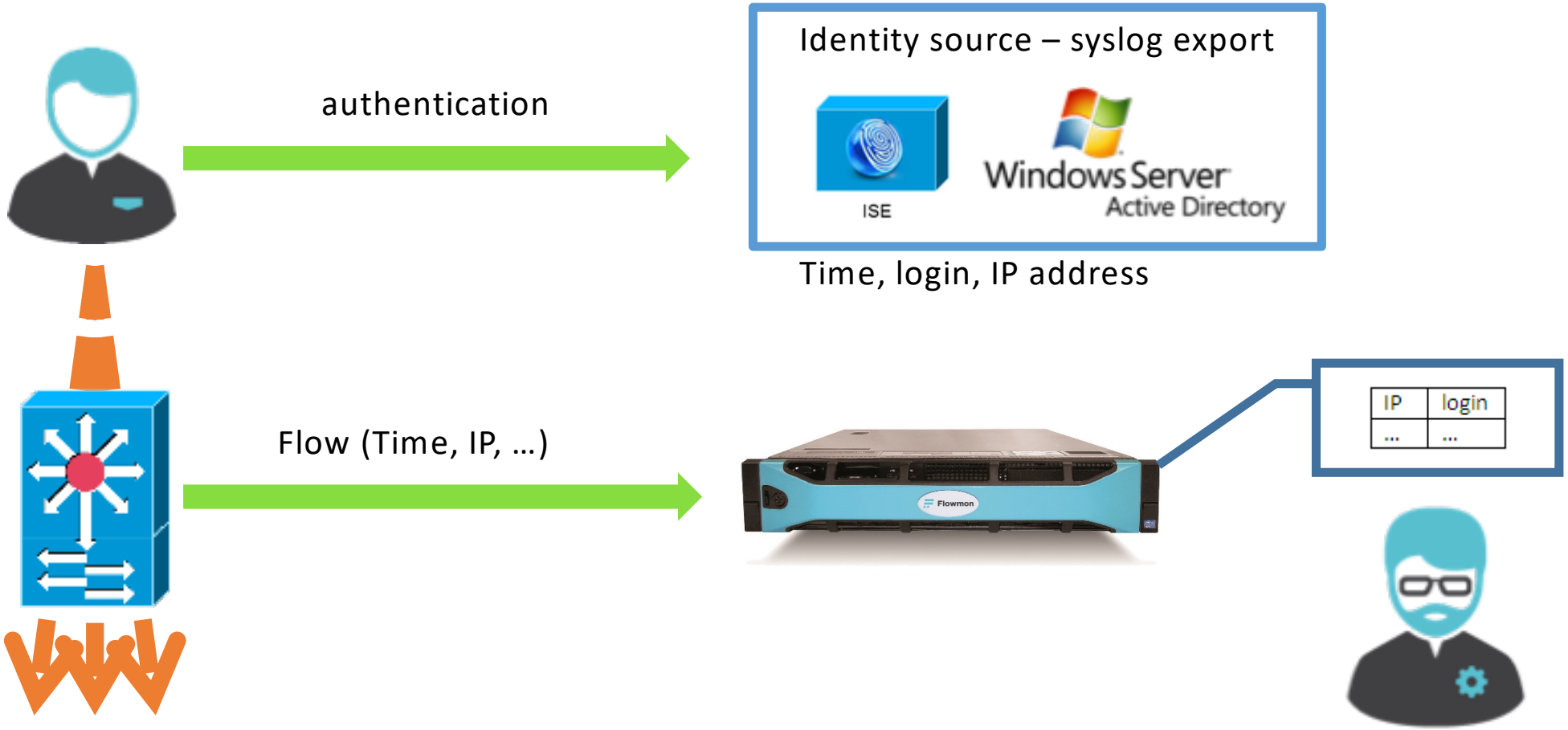




Detect incidents in Network Access Layer



User Identity Awareness



Evidence for Network Forensic

Flowmon Networks

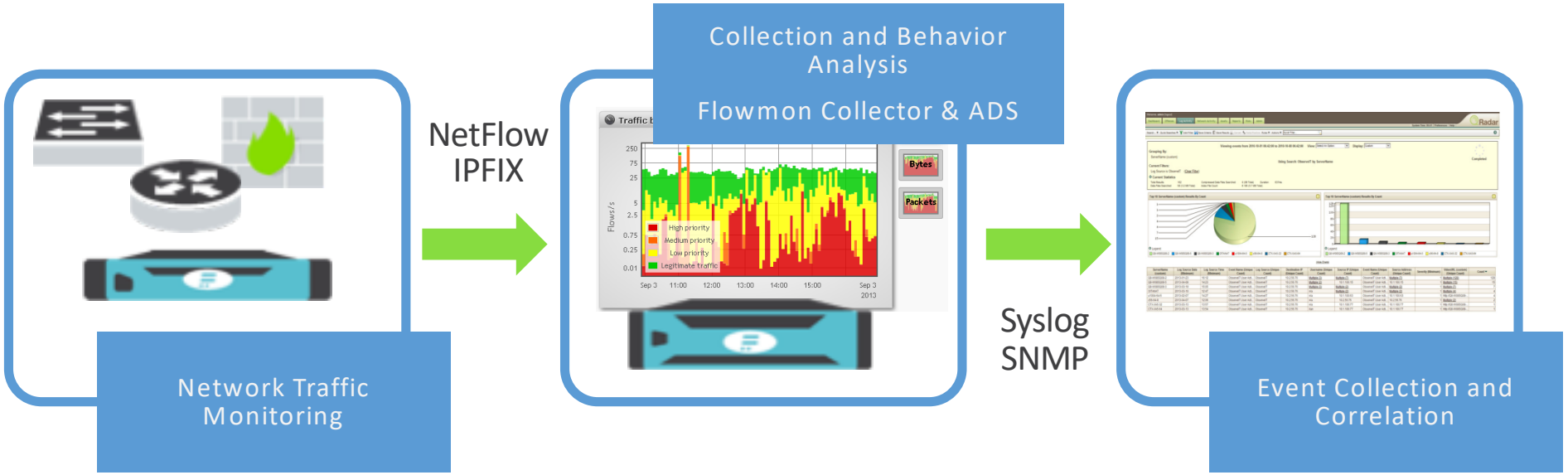
Flow monitoring including L7
Network Behavior Analysis

Full packet capture
Triggered by detection

Collected evidence
of system compromise

Integration with third-party solutions

- Event exporting (syslog based)



- Links Flowmon <-> Log Management

Incident detection with ADS

ALERTS!

- Transfer of data
- New protocol in the network
- Anomaly in network behavior
- Port scanning (TCP, UDP)
- Network scanning (ICMP, TCP, UDP)
- DNS tunneling
- Unknown DNS requests
- Dangerous access attempts (Threat Intelligence)

Summary

- Detailed information about network and applications and users
- Effective troubleshooting
- Detection of misconfigurations
- Optimization and capacity planning
- Monitoring and analysis of network and application performance
- Prevention of overload and network down-time