FlowMon – Your Network Under Control!

B2B Workshop of ICT Companies, Tuesday, October 18, 2016

Flowmon
Driving Network Visibility

Hung Nguyen

Key Account Manager Benelux

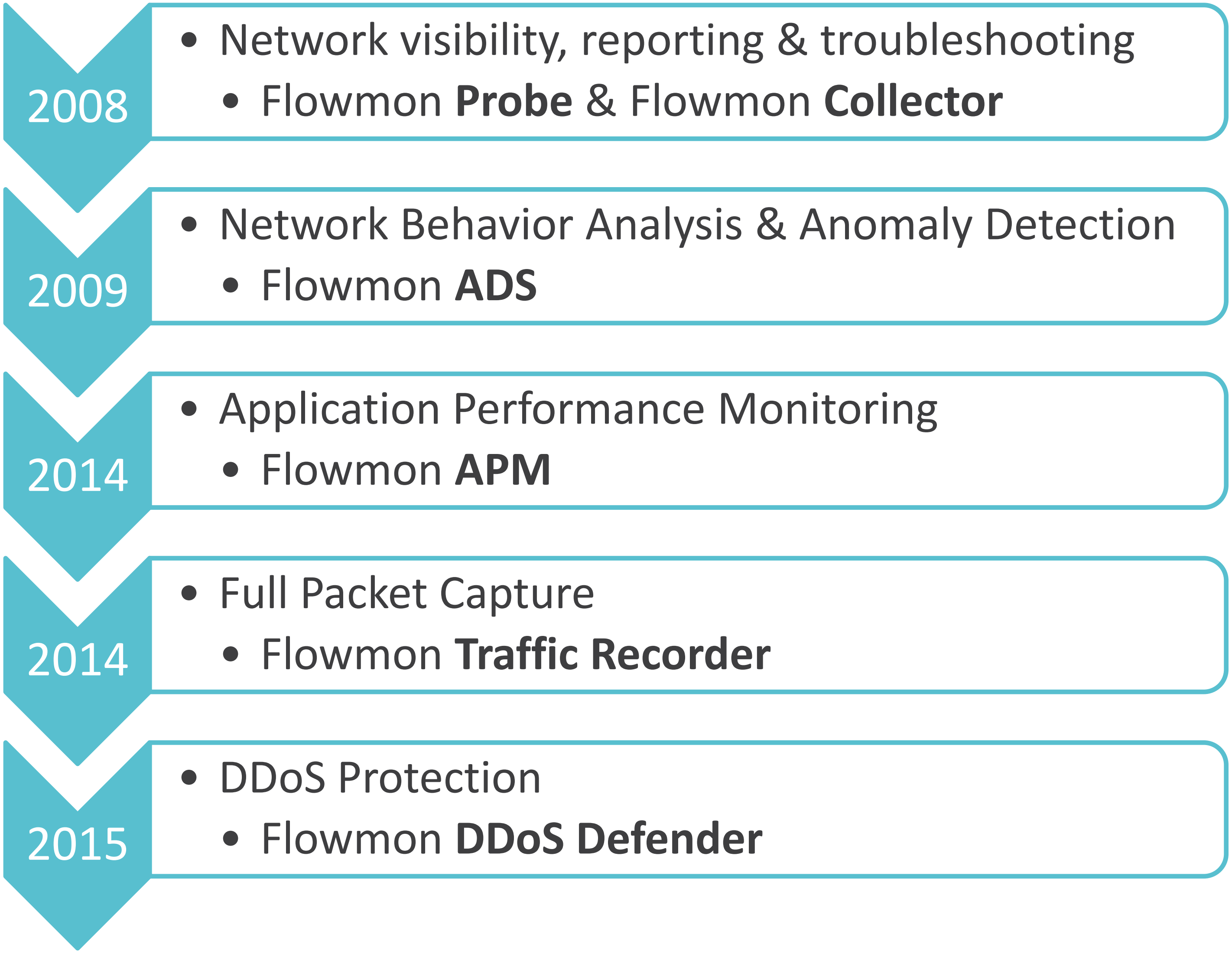
Hung.Nguyen@Flowmon.com

Company Overview

- International vendor devoted to innovative network traffic & performance & security monitoring
- Company facts
  - Founded in 2007, 50+ employees
  - Headquarters Brno, Czech Republic
  - Strong R&D background
- Achievements
  - Gartner recognized since 2010
  - Deloitte CE Technology Fast 50
  - Partnerships: Cisco, Check Point
  - 500+ customers worldwide

Flowmon Use Cases

Flowmon
Networks



2008

- Network visibility, reporting & troubleshooting
  - Flowmon **Probe** & Flowmon **Collector**

2009

- Network Behavior Analysis & Anomaly Detection
  - Flowmon **ADS**

2014

- Application Performance Monitoring
  - Flowmon **APM**

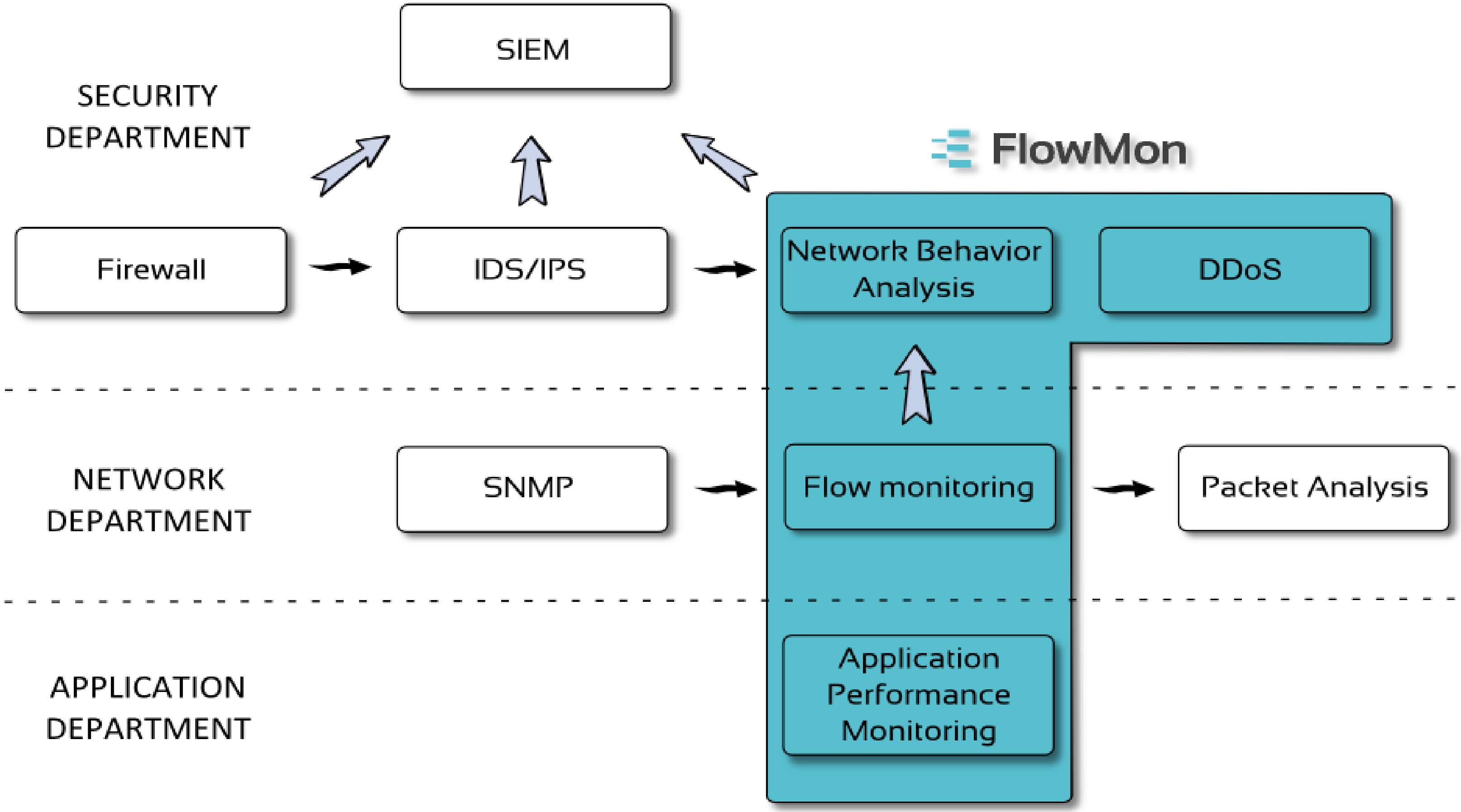
2014

- Full Packet Capture
  - Flowmon **Traffic Recorder**

2015

- DDoS Protection
  - Flowmon **DDoS Defender**

Technology Landscape



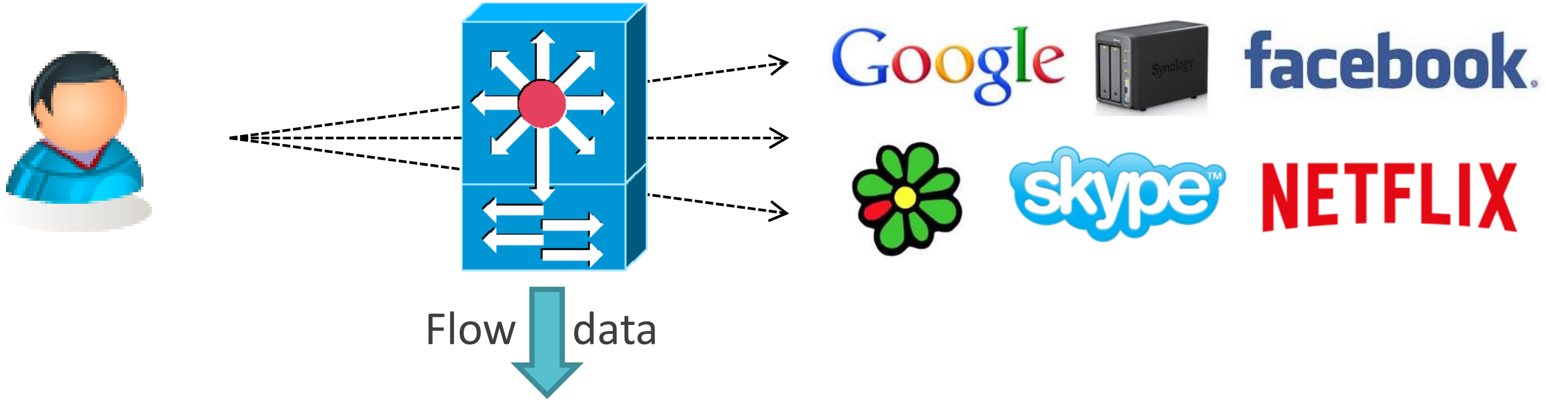
SECURITY DEPARTMENT

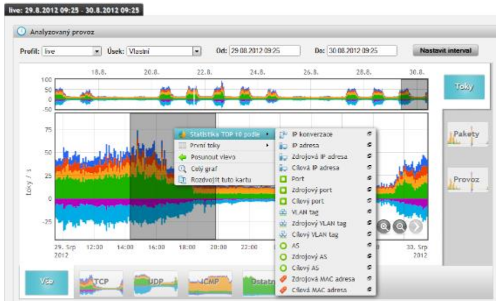
NETWORK DEPARTMENT

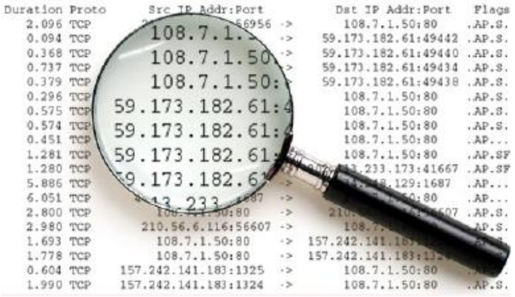
APPLICATION DEPARTMENT

What is Flow Data?

- Modern method for network monitoring – flow measurement
- Cisco standard **NetFlow v5/v9**, IETF standard **IPFIX**
- Focused on **L3/L4** information and volumetric parameters
- Real network traffic to flow statistics reduction ratio **500:1**







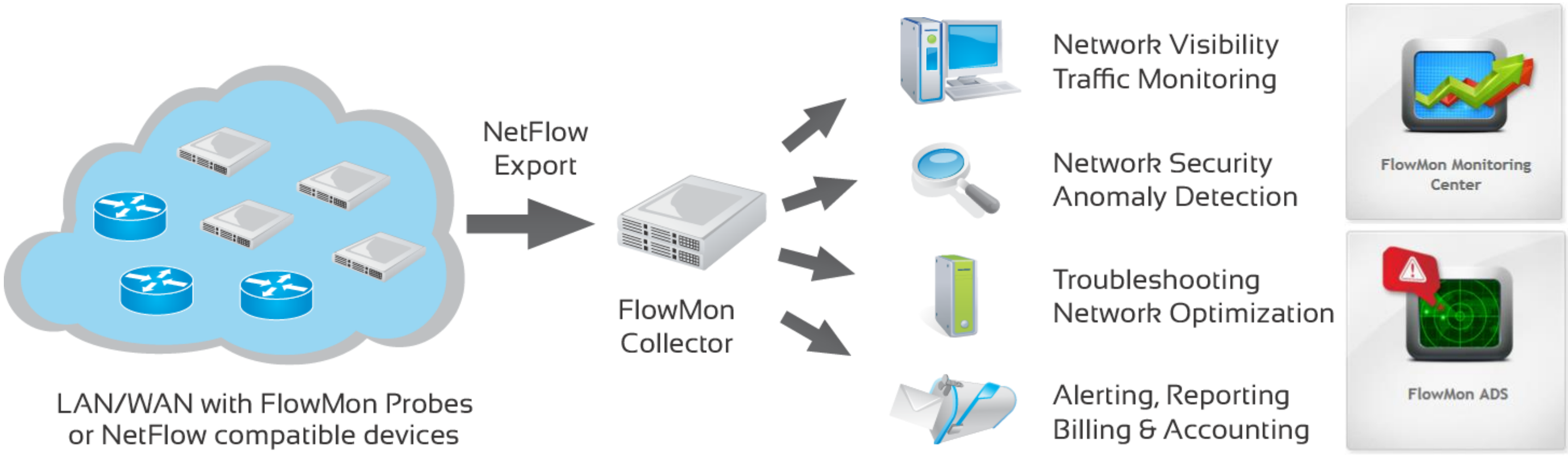
```
Duration Proto     Src IP Addr:Port            Dst IP Addr:Port   Flags
   2.096 TCP              :56956    ->      108.7.1.50:80       .AP.S.
   0.094 TCP        108.7.1.        ->  59.173.182.61:49442     .AP.S.
   0.368 TCP        108.7.1.50      ->  59.173.182.61:49440     .AP.S.
   0.737 TCP        108.7.1.50:     ->  59.173.182.61:49434     .AP.S.
   0.379 TCP        108.7.1.50:     ->  59.173.182.61:49438     .AP.S.
   0.296 TCP     59.173.182.61:4    ->      108.7.1.50:80       .AP.S.
   0.575 TCP     59.173.182.61:     ->      108.7.1.50:80       .AP.S.
   0.574 TCP     59.173.182.61:     ->      108.7.1.50:80       .AP.S.
   0.451 TCP     59.173.182.61      ->      108.7.1.50:80       .AP...
   1.281 TCP                        ->      108.7.1.50:80       .AP.SF
   1.280 TCP                        ->    .233.173:41667        .AP.SF
   5.886 TCP                        ->       .129:1687          .AP...
   6.051 TCP          .13.233.   687 ->           :80           .AP...
   2.800 TCP            108.    50:80 ->  210.         607      .AP.S.
   2.980 TCP   210.56.6.116:56607   ->      108.7.              .AP.S.
   1.693 TCP      108.7.1.50:80     -> 157.242.141.18
   1.778 TCP      108.7.1.50:80     -> 157.242.141.183:13
   0.604 TCP 157.242.141.183:1325   ->      108.7.1.50:80
   1.990 TCP 157.242.141.183:1324   ->      108.7.1.50:80       .AP.S.
```

Flowmon Components

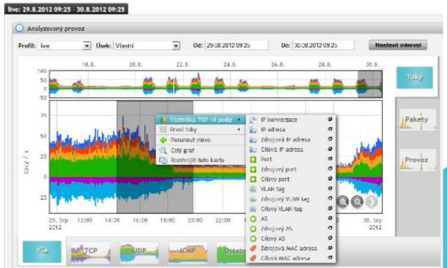
- Flowmon Probes
  - Passive source of NetFlow/IPFIX data
- Flowmon Collectors
  - Flow collection, reporting, analysis
- Flowmon modules (plugins)
  - ADS , APM, FTR, DDoS, DR

vmware

Microsoft Hyper-V



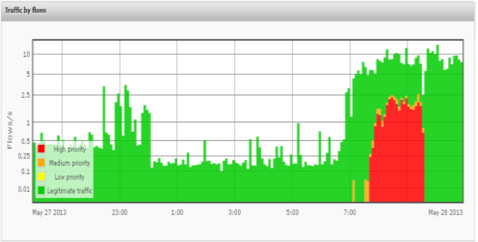
Product positioning

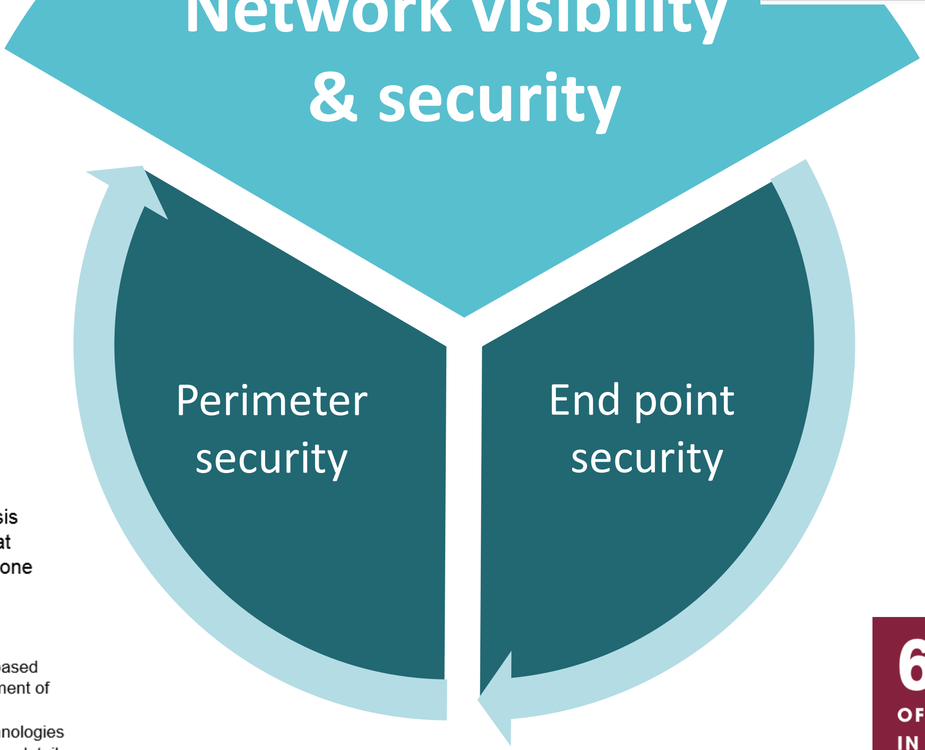


live: 29.8.2012 09:25 - 30.8.2012 09:25

Analyzovaný provoz

Profil: live   Úsek: Vlastní   Od: 29.08.2012 09:25   Do: 30.08.2012 09:25





Network visibility & security

Perimeter security

End point security

Gartner

Gartner last year stated that flow analysis should be done 80% of the time and that packet capture with probes should be done 20% of the time.

Recommendations

- Implement the use of advanced flow-based data sources to allow better measurement of the user experience.
- Implement flow-based monitoring technologies extensively, and leverage probes where detail is needed. Using a single platform for both makes management easier.

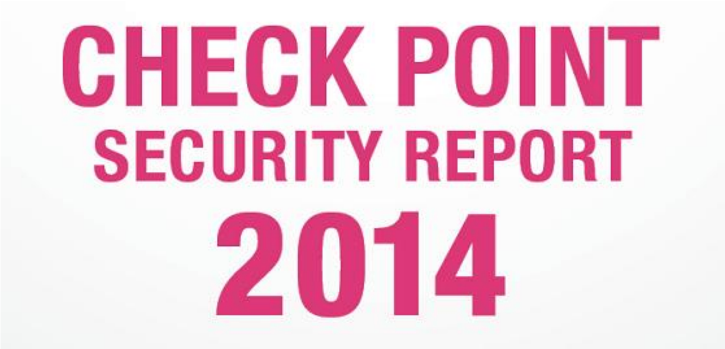
CHECK POINT 2013 SECURITY REPORT

63%

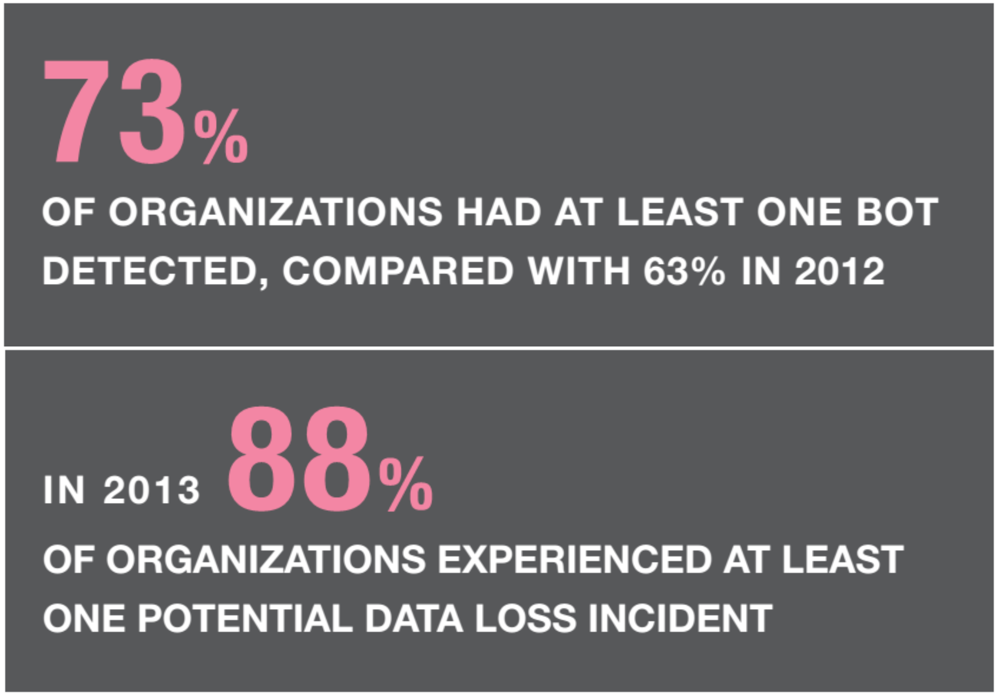
OF THE ORGANIZATIONS IN OUR RESEARCH ARE INFECTED WITH BOTS

Infected Corporate Networks

Flowmon
Networks



CHECK POINT
SECURITY REPORT
2014



73%

OF ORGANIZATIONS HAD AT LEAST ONE BOT DETECTED, COMPARED WITH 63% IN 2012

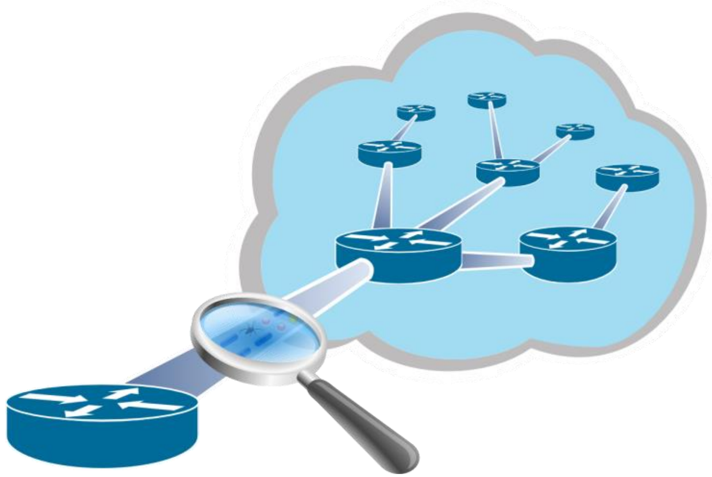
IN 2013 88%

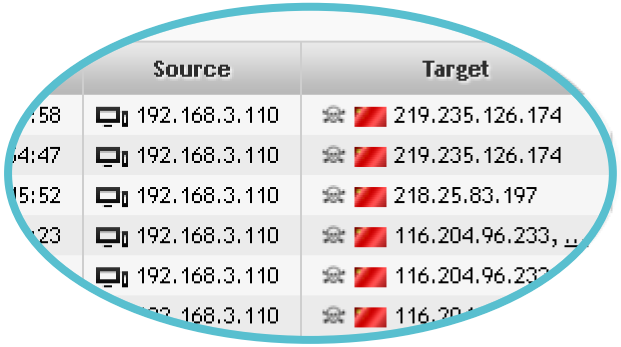
OF ORGANIZATIONS EXPERIENCED AT LEAST ONE POTENTIAL DATA LOSS INCIDENT

Prevention is not enough. You have to redefine your security strategy and incorporate tools to support **post-breach phase** by **early detection** and **remediation**.

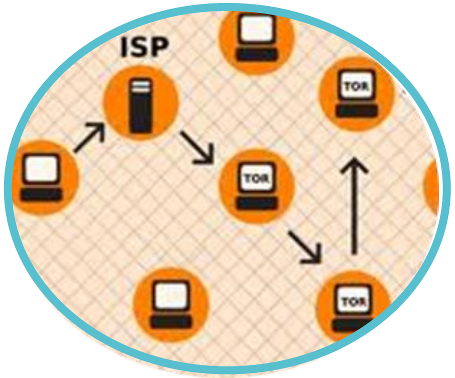
ADS Methods and Approach

- Signature-less technology
  - Advanced methods of artificial intelligence
    - Bidirectional flows (client/server identification)
    - Changes of network behavior in time
    - Machine learning methods and heuristics
    - Decision trees for monitoring of low & slow attacks
    - Algorithms for finding clusters and outliers



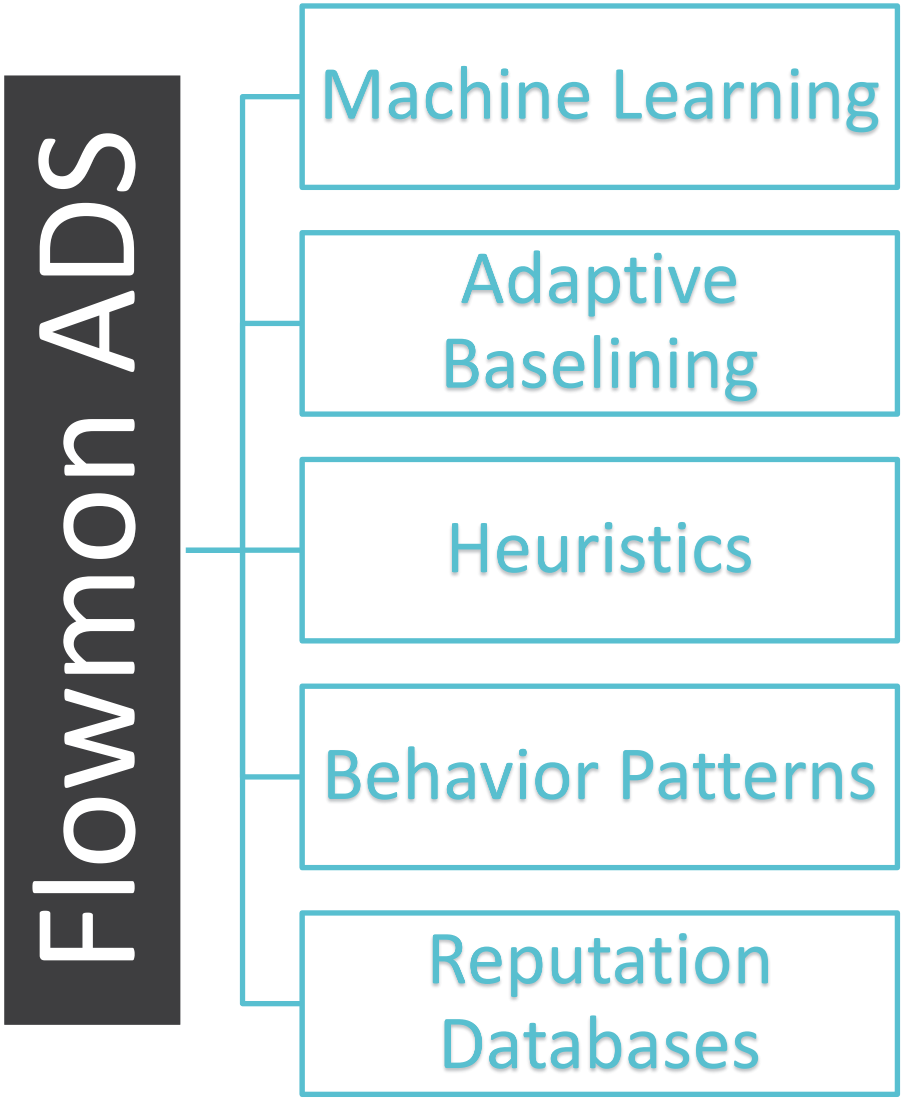


	Source	Target
:58	192.168.3.110	219.235.126.174
4:47	192.168.3.110	219.235.126.174
5:52	192.168.3.110	218.25.83.197
:23	192.168.3.110	116.204.96.233, ...
	192.168.3.110	116.204.96.23
	168.3.110	116.20



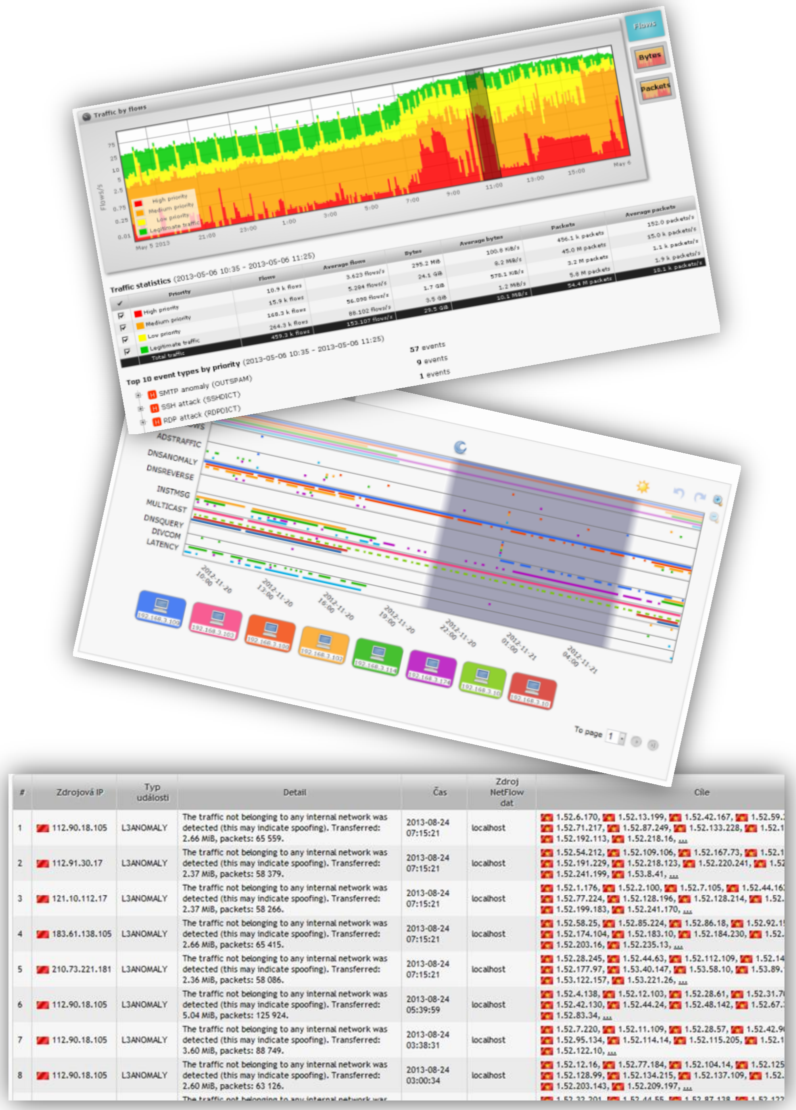
Flowmon ADS Principles

Flowmon Networks



Flowmon ADS

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



Traffic statistics (2013-05-06 10:35 - 2013-05-06 11:25)

✓	Priority	Flows	Average flows	Bytes	Average bytes	Packets	Average packets
☑	🟥 High priority	10.9 k flows	3.623 flows/s	295.2 MB	100.8 KiB/s	456.1 k packets	152.0 packets/s
☑	🟧 Medium priority	15.9 k flows	5.284 flows/s	24.1 GB	8.2 MiB/s	45.0 M packets	15.0 k packets/s
☑	🟨 Low priority	168.3 k flows	56.098 flows/s	1.7 GB	578.1 KiB/s	3.2 M packets	1.1 k packets/s
☑	🟩 Legitimate traffic	264.3 k flows	88.102 flows/s	3.5 GB	1.2 MiB/s	5.8 M packets	1.9 k packets/s
	Total traffic	459.3 k flows	153.107 flows/s	29.5 GB	10.1 MiB/s	54.4 M packets	18.1 k packets/s

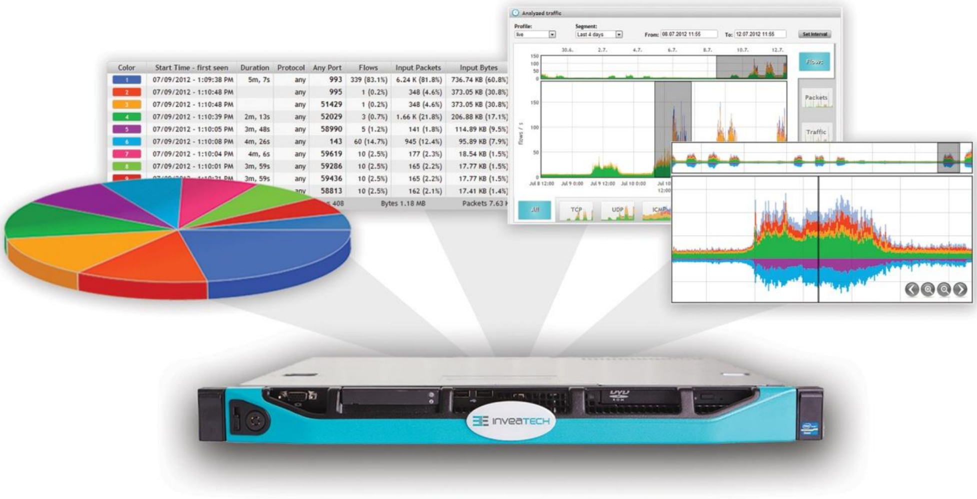
Top 10 event types by priority (2013-05-06 10:35 - 2013-05-06 11:25)

H SMTP anomaly (OUTSPAM)	57 events
H SSH attack (SSHDICT)	9 events
H RDP attack (RDPDICT)	1 events

#	Zdrojová IP	Typ události	Detail	Čas	Zdroj NetFlow dat	Cíle
1	112.90.18.105	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred: 2.66 MiB, packets: 65 559.	2013-08-24 07:15:21	localhost	1.52.6.170, 1.52.13.199, 1.52.42.167, 1.52.59. 1.52.71.217, 1.52.87.249, 1.52.133.228, 1.52.1 1.52.192.113, 1.52.218.16, ...
2	112.91.30.17	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred: 2.37 MiB, packets: 58 379.	2013-08-24 07:15:21	localhost	1.52.54.212, 1.52.109.106, 1.52.167.73, 1.52.1 1.52.191.229, 1.52.218.123, 1.52.220.241, 1.52 1.52.241.199, 1.53.8.41, ...
3	121.10.112.17	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred: 2.37 MiB, packets: 58 266.	2013-08-24 07:15:21	localhost	1.52.1.176, 1.52.2.100, 1.52.7.105, 1.52.44.16 1.52.77.224, 1.52.128.196, 1.52.128.214, 1.52. 1.52.199.183, 1.52.241.170, ...
4	183.61.138.105	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred: 2.66 MiB, packets: 65 415.	2013-08-24 07:15:21	localhost	1.52.58.25, 1.52.85.224, 1.52.86.18, 1.52.92.1 1.52.174.104, 1.52.183.10, 1.52.184.230, 1.52. 1.52.203.16, 1.52.235.13, ...
5	210.73.221.181	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred: 2.36 MiB, packets: 58 086.	2013-08-24 07:15:21	localhost	1.52.28.245, 1.52.44.63, 1.52.112.109, 1.52.14 1.52.177.97, 1.53.40.147, 1.53.58.10, 1.53.89. 1.53.122.157, 1.53.221.26, ...
6	112.90.18.105	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred: 5.04 MiB, packets: 125 924.	2013-08-24 05:39:59	localhost	1.52.4.138, 1.52.12.103, 1.52.28.61, 1.52.31.7 1.52.42.130, 1.52.44.24, 1.52.48.142, 1.52.67. 1.52.83.34, ...
7	112.90.18.105	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred: 3.60 MiB, packets: 88 749.	2013-08-24 03:38:31	localhost	1.52.7.220, 1.52.11.109, 1.52.28.57, 1.52.42.9 1.52.95.134, 1.52.114.14, 1.52.115.205, 1.52.1 1.52.122.10, ...
8	112.90.18.105	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred: 2.60 MiB, packets: 63 126.	2013-08-24 03:00:34	localhost	1.52.12.16, 1.52.77.184, 1.52.104.14, 1.52.125 1.52.128.99, 1.52.134.215, 1.52.137.109, 1.52. 1.52.203.143, 1.52.209.197, ...

FlowMon Family Overview

Flowmon
Networks

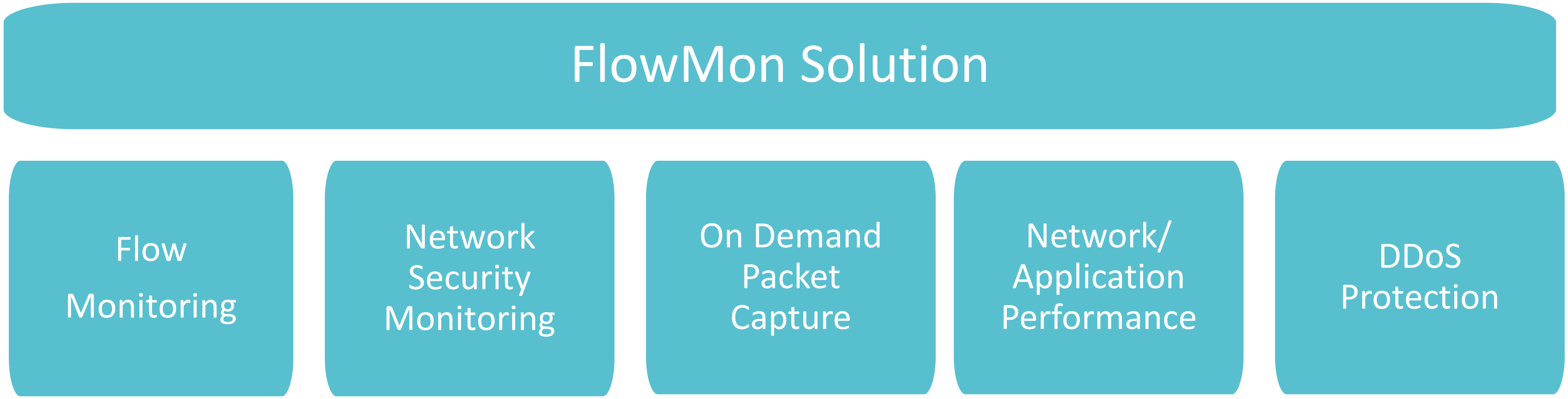


Color	Start Time - first seen	Duration	Protocol	Any Port	Flows	Input Packets	Input Bytes
1	07/09/2012 - 1:09:38 PM	5m, 7s	any	993	339 (83.1%)	6.24 K (81.8%)	736.74 KB (60.8%)
2	07/09/2012 - 1:10:48 PM		any	995	1 (0.2%)	348 (4.6%)	373.05 KB (30.8%)
3	07/09/2012 - 1:10:48 PM		any	51429	1 (0.2%)	348 (4.6%)	373.05 KB (30.8%)
4	07/09/2012 - 1:10:39 PM	2m, 13s	any	52029	3 (0.7%)	1.66 K (21.8%)	206.88 KB (17.1%)
5	07/09/2012 - 1:10:05 PM	3m, 48s	any	58990	5 (1.2%)	141 (1.8%)	114.89 KB (9.5%)
6	07/09/2012 - 1:10:08 PM	4m, 26s	any	143	60 (14.7%)	945 (12.4%)	95.89 KB (7.9%)
7	07/09/2012 - 1:10:04 PM	4m, 6s	any	59619	10 (2.5%)	177 (2.3%)	18.54 KB (1.5%)
8	07/09/2012 - 1:10:01 PM	3m, 59s	any	59286	10 (2.5%)	165 (2.2%)	17.77 KB (1.5%)
9	07/09/2012 - 1:10:21 PM	3m, 59s	any	59436	10 (2.5%)	165 (2.2%)	17.77 KB (1.5%)
			any	58813	10 (2.5%)	162 (2.1%)	17.41 KB (1.4%)

s 408 Bytes 1.18 MB Packets 7.63

Analyzed traffic

Profile: live
Segment: Last 4 days
From: 08.07.2012 11:55
To: 12.07.2012 11:55



FlowMon Solution

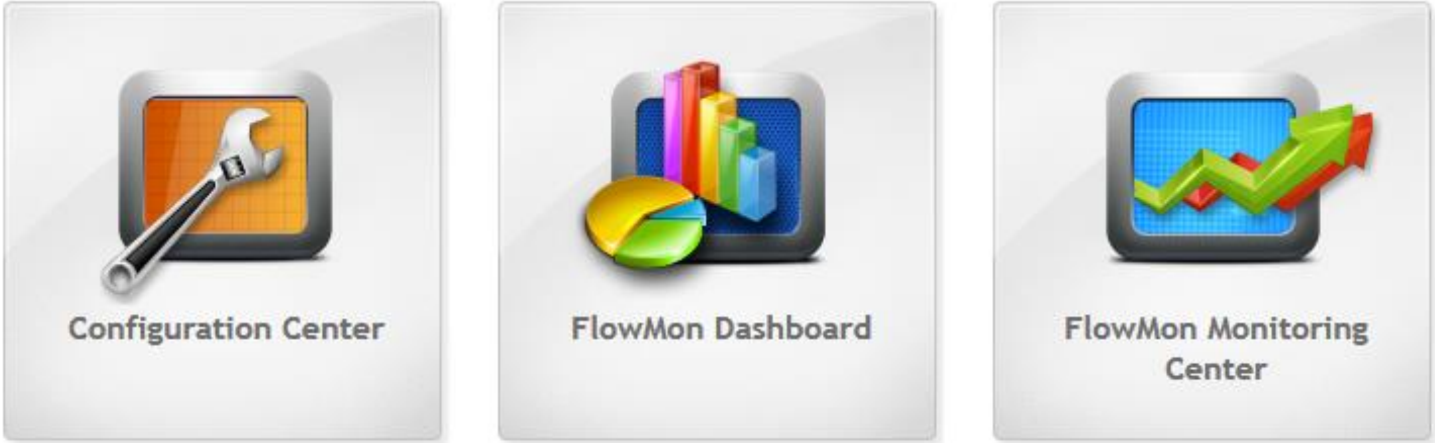
Flow Monitoring

Network Security Monitoring

On Demand Packet Capture

Network/ Application Performance

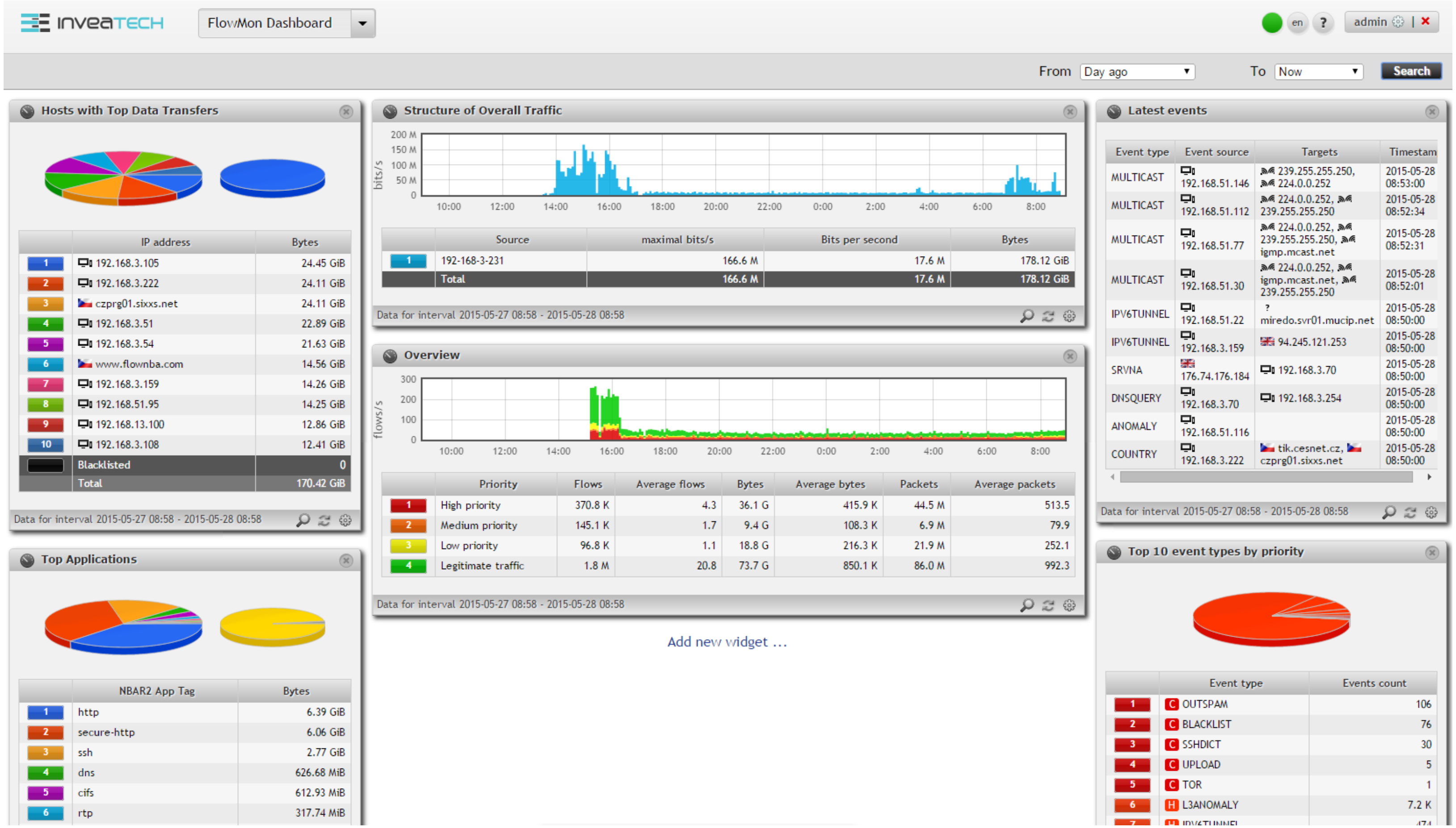
DDoS Protection



User Interface

FlowMon Dashboard (FMD)

- Combines widgets from different modules (plug-ins)



Hosts with Top Data Transfers

	IP address	Bytes
1	192.168.3.105	24.45 GiB
2	192.168.3.222	24.11 GiB
3	czprg01.sixxs.net	24.11 GiB
4	192.168.3.51	22.89 GiB
5	192.168.3.54	21.63 GiB
6	www.flownba.com	14.56 GiB
7	192.168.3.159	14.26 GiB
8	192.168.51.95	14.25 GiB
9	192.168.13.100	12.86 GiB
10	192.168.3.108	12.41 GiB
■	Blacklisted	0
	Total	170.42 GiB

Data for interval 2015-05-27 08:58 - 2015-05-28 08:58

Top Applications

	NBAR2 App Tag	Bytes
1	http	6.39 GiB
2	secure-http	6.06 GiB
3	ssh	2.77 GiB
4	dns	626.68 MiB
5	cifs	612.93 MiB
6	rtp	317.74 MiB

Structure of Overall Traffic

	Source	maximal bits/s	Bits per second	Bytes
1	192-168-3-231	166.6 M	17.6 M	178.12 GiB
	Total	166.6 M	17.6 M	178.12 GiB

Data for interval 2015-05-27 08:58 - 2015-05-28 08:58

Overview

	Priority	Flows	Average flows	Bytes	Average bytes	Packets	Average packets
1	High priority	370.8 K	4.3	36.1 G	415.9 K	44.5 M	513.5
2	Medium priority	145.1 K	1.7	9.4 G	108.3 K	6.9 M	79.9
3	Low priority	96.8 K	1.1	18.8 G	216.3 K	21.9 M	252.1
4	Legitimate traffic	1.8 M	20.8	73.7 G	850.1 K	86.0 M	992.3

Data for interval 2015-05-27 08:58 - 2015-05-28 08:58

Latest events

Event type	Event source	Targets	Timestam
MULTICAST	192.168.51.146	239.255.255.250, 224.0.0.252	2015-05-28 08:53:00
MULTICAST	192.168.51.112	224.0.0.252, 239.255.255.250	2015-05-28 08:52:34
MULTICAST	192.168.51.77	224.0.0.252, 239.255.255.250, igmp.mcast.net	2015-05-28 08:52:31
MULTICAST	192.168.51.30	224.0.0.252, igmp.mcast.net, 239.255.255.250	2015-05-28 08:52:01
IPV6TUNNEL	192.168.51.22	? miredo.svr01.mucip.net	2015-05-28 08:50:00
IPV6TUNNEL	192.168.3.159	94.245.121.253	2015-05-28 08:50:00
SRVNA	176.74.176.184	192.168.3.70	2015-05-28 08:50:00
DNSQUERY	192.168.3.70	192.168.3.254	2015-05-28 08:50:00
ANOMALY	192.168.51.116		2015-05-28 08:50:00
COUNTRY	192.168.3.222	tik.cesnet.cz, czprg01.sixxs.net	2015-05-28 08:50:00

Data for interval 2015-05-27 08:58 - 2015-05-28 08:58

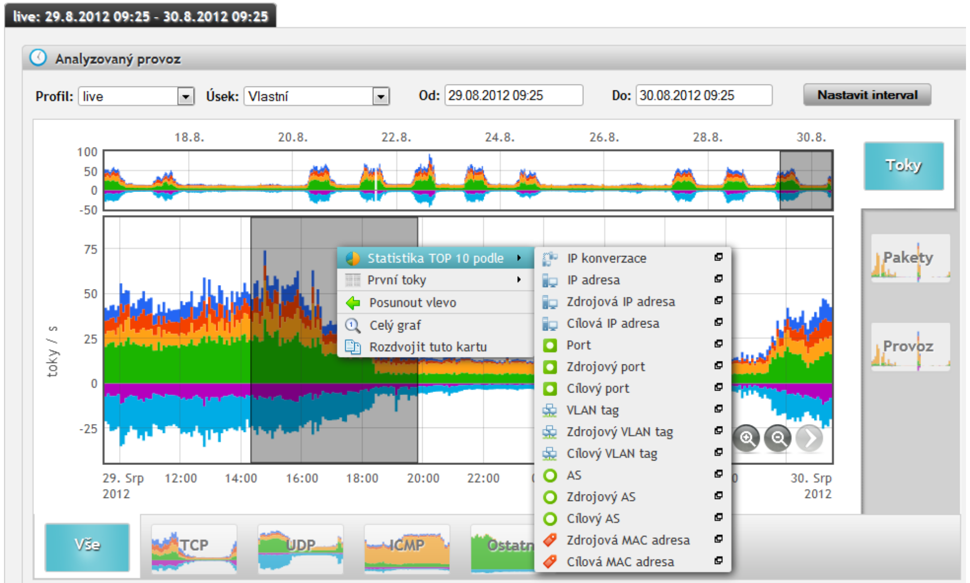
Top 10 event types by priority

	Event type	Events count
1	C OUTSPAM	106
2	C BLACKLIST	76
3	C SSHDICT	30
4	C UPLOAD	5
5	C TOR	1
6	H L3ANOMALY	7.2 K
7	H IPV6TUNNEL	474

Monitoring Center (FMC)

Flowmon Networks

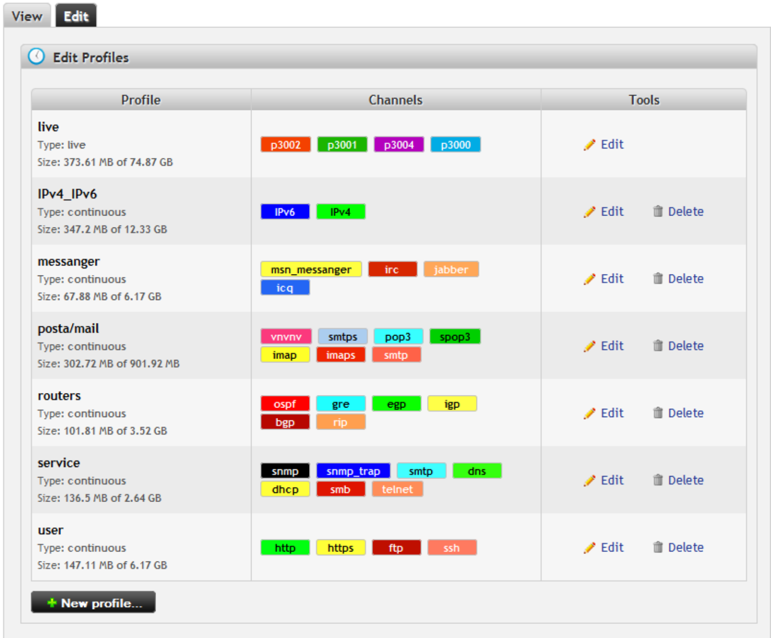
- Application for NetFlow data storage and visualization
- Graphs, tables and form for further data processing
- Top N statistics (users, sites, services)
- Predefined set of profiles (views) for standard protocols
- User defined profiles (based on IP address or ports)
- Alerts, thresholds



live: 29.8.2012 09:25 - 30.8.2012 09:25

Analyzovaný provoz

Profil: live Úsek: Vlastní Od: 29.08.2012 09:25 Do: 30.08.2012 09:25

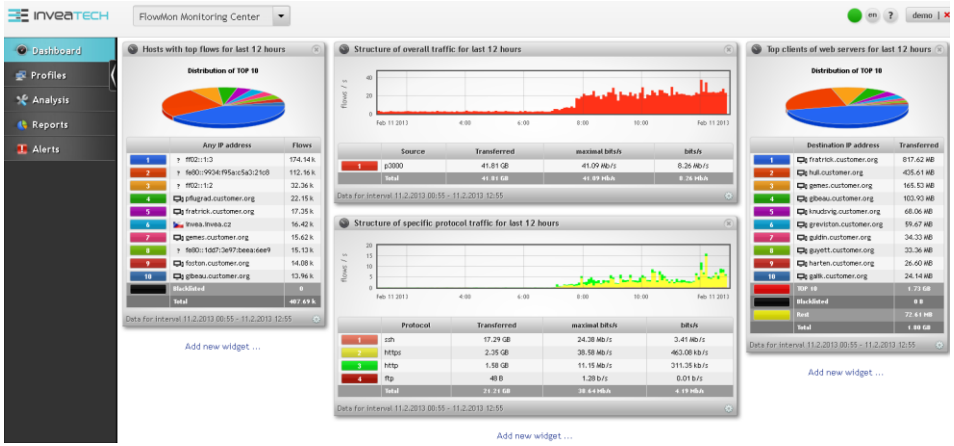


Edit Profiles

Profile	Channels	Tools
live Type: live Size: 373.61 MB of 74.87 GB	p3002 p3001 p3004 p3000	Edit
IPv4_IPv6 Type: continuous Size: 347.2 MB of 12.33 GB	IPv6 IPv4	Edit Delete
messanger Type: continuous Size: 67.88 MB of 6.17 GB	msn_messanger irc jabber icq	Edit Delete
posta/mail Type: continuous Size: 302.72 MB of 901.92 MB	vnvnv smtps pop3 spop3 imap imaps smtp	Edit Delete
routers Type: continuous Size: 101.81 MB of 3.52 GB	ospf gre egp igp bgp rip	Edit Delete
service Type: continuous Size: 136.5 MB of 2.64 GB	snmp snmp_trap smtp dns dhcp smb telnet	Edit Delete
user Type: continuous Size: 147.11 MB of 6.17 GB	http https ftp ssh	Edit Delete

Monitoring Center (FMC)

- Intelligent reporting tool, exports to pdf, csv



	Any IP address	Flows
1	? ff02::1:3	174.14 k
2	? fe80::9934:f95a:c5a3:21c8	112.16 k
3	? ff02::1:2	32.36 k
4	pflugrad.customer.org	22.15 k
5	fratrick.customer.org	17.35 k
6	invea.invea.cz	16.42 k
7	gemes.customer.org	15.62 k
8	? fe80::1dd7:3e97:beea:6ee9	15.13 k
9	foston.customer.org	14.08 k
10	gibeau.customer.org	13.96 k
	Blacklisted	0
	Total	407.69 k

Data for interval 11.2.2013 00:55 - 11.2.2013 12:55

	Source	Transferred	maximal bits/s	bits/s
1	p3000	41.81 GB	41.09 Mb/s	8.26 Mb/s
	Total	41.81 GB	41.09 Mb/s	8.26 Mb/s

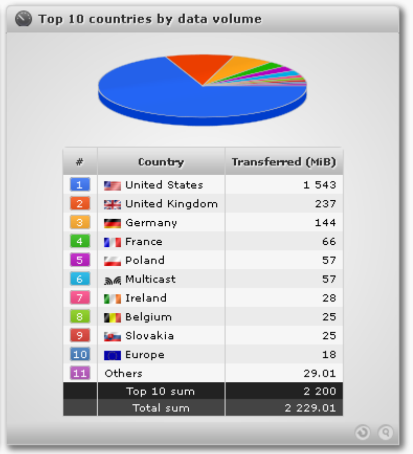
Data for interval 11.2.2013 00:55 - 11.2.2013 12:55

	Protocol	Transferred	maximal bits/s	bits/s
1	ssh	17.29 GB	24.38 Mb/s	3.41 Mb/s
2	https	2.35 GB	38.58 Mb/s	463.08 kb/s
3	http	1.58 GB	11.15 Mb/s	311.35 kb/s
4	ftp	48 B	1.28 b/s	0.01 b/s
	Total	21.21 GB	38.64 Mb/s	4.19 Mb/s

Data for interval 11.2.2013 00:55 - 11.2.2013 12:55

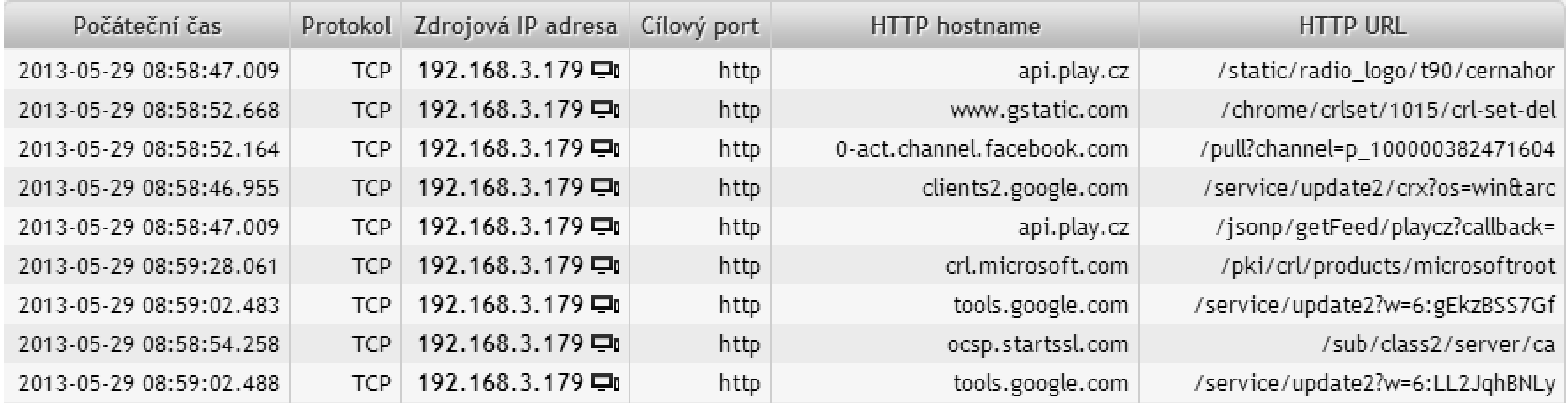
	Destination IP address	Transferred
1	fratrick.customer.org	817.62 MB
2	hull.customer.org	435.61 MB
3	gemes.customer.org	165.53 MB
4	gibeau.customer.org	103.93 MB
5	knudsvig.customer.org	68.06 MB
6	greviston.customer.org	59.67 MB
7	guidin.customer.org	34.33 MB
8	guyett.customer.org	33.36 MB
9	harten.customer.org	26.60 MB
10	galik.customer.org	24.14 MB
	TOP 10	1.73 GB
	Blacklisted	0 B
	Rest	72.61 MB
	Total	1.80 GB

Data for interval 11.2.2013 00:55 - 11.2.2013 12:55



#	Country	Transferred (MiB)
1	United States	1 543
2	United Kingdom	237
3	Germany	144
4	France	66
5	Poland	57
6	Multicast	57
7	Ireland	28
8	Belgium	25
9	Slovakia	25
10	Europe	18
11	Others	29.01
	Top 10 sum	2 200
	Total sum	2 229.01

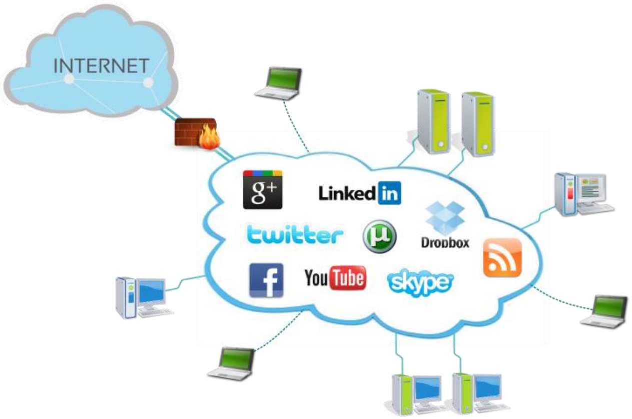
- Monitoring of HTTP traffic – analysis & detection



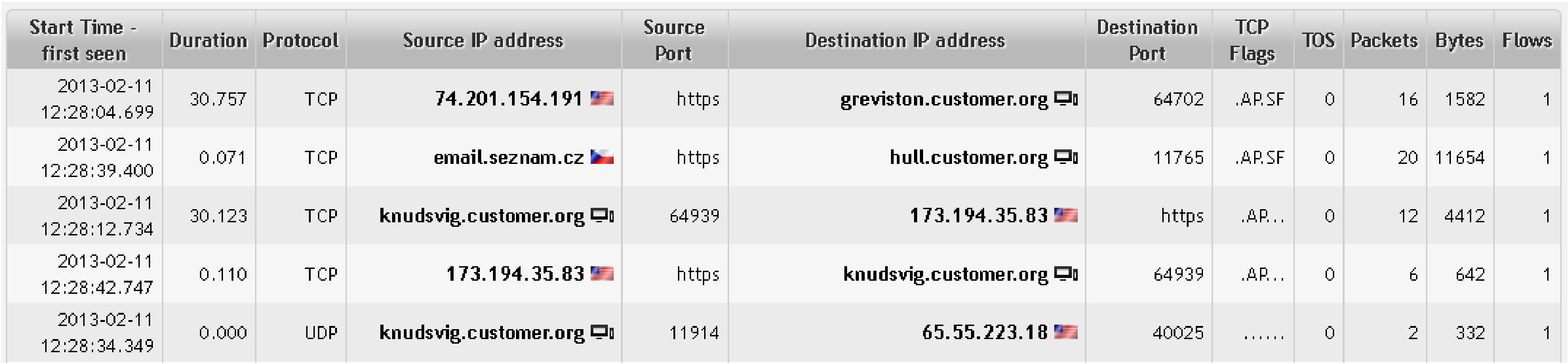
Počáteční čas	Protokol	Zdrojová IP adresa	Cílový port	HTTP hostname	HTTP URL
2013-05-29 08:58:47.009	TCP	192.168.3.179	http	api.play.cz	/static/radio_logo/t90/cernahor
2013-05-29 08:58:52.668	TCP	192.168.3.179	http	www.gstatic.com	/chrome/crlset/1015/crl-set-del
2013-05-29 08:58:52.164	TCP	192.168.3.179	http	0-act.channel.facebook.com	/pull?channel=p_100000382471604
2013-05-29 08:58:46.955	TCP	192.168.3.179	http	clients2.google.com	/service/update2/crx?os=win&arc
2013-05-29 08:58:47.009	TCP	192.168.3.179	http	api.play.cz	/jsonp/getFeed/playcz?callback=
2013-05-29 08:59:28.061	TCP	192.168.3.179	http	crl.microsoft.com	/pki/crl/products/microsoftroot
2013-05-29 08:59:02.483	TCP	192.168.3.179	http	tools.google.com	/service/update2?w=6:gEkzBSS7Gf
2013-05-29 08:58:54.258	TCP	192.168.3.179	http	ocsp.startssl.com	/sub/class2/server/ca
2013-05-29 08:59:02.488	TCP	192.168.3.179	http	tools.google.com	/service/update2?w=6:LL2JqhBNLy

Monitoring Center (FMC)

- Application recognition
  NBAR2 support



- Geolocation
  - Automatically available in FMC and ADS
  - IP address location shown by flag
  - Integrated database – geolocation is available also offline



Start Time - first seen	Duration	Protocol	Source IP address	Source Port	Destination IP address	Destination Port	TCP Flags	TOS	Packets	Bytes	Flows
2013-02-11 12:28:04.699	30.757	TCP	74.201.154.191 🇺🇸	https	greviston.customer.org 🖥	64702	.AP.SF	0	16	1582	1
2013-02-11 12:28:39.400	0.071	TCP	email.seznam.cz 🇨🇿	https	hull.customer.org 🖥	11765	.AP.SF	0	20	11654	1
2013-02-11 12:28:12.734	30.123	TCP	knudsvig.customer.org 🖥	64939	173.194.35.83 🇺🇸	https	.AP...	0	12	4412	1
2013-02-11 12:28:42.747	0.110	TCP	173.194.35.83 🇺🇸	https	knudsvig.customer.org 🖥	64939	.AP...	0	6	642	1
2013-02-11 12:28:34.349	0.000	UDP	knudsvig.customer.org 🖥	11914	65.55.223.18 🇺🇸	40025	......	0	2	332	1

Questions?

High-Speed Networking Technology Partner

Hung Nguyen
Hung.Nguyen@Flowmon.com
+31624914056

Flowmon Networks a.s.
U Vodárny 2965/2
616 00 Brno, Czech Republic
www.invea.com