It’s Flow Time!

The Role and Importance of Flow Monitoring in Network Operations and Security

Jiri Knapek, Presales Engineer

RONOG 5, 23 October 2018

Flowmon
Driving Network Visibility

Your customers depend on your services more than ever before

You need proper set of tools to ensure reliability and service continuity

There is an opportunity to transform from ISP to MSP or MSSP

Flowmon
Driving Network Visibility

“85% of Enterprise customers expect their ISP to offer more comprehensive DDoS protection-as-a-service.

Source: DDoS Impact and Opportunity in the Service Provider Environment by FierceMarkets

Flowmon
Driving Network Visibility

Flowmon
Networks

is an international vendor devoted to innovative network traffic & performance & security monitoring

700+ customers
30+ countries

First 100G probes
in the world

Strong R&D
background

European
origin

Customer references

SEGA · AVG · KBC

KONICA MINOLTA · vodafone · TDK

ORIFLAME SWEDEN · SIEMENS · SLOVENSKÁ sporiteľňa

Volkswagen · orange · Telefonica

Allianz · hp · T··Mobile·

GÉANT Networks • Services • People · KIA · upc

Raiffeisen BANK · e·on

Technology partner of premium vendors

cisco

vmware

Check Point
SOFTWARE TECHNOLOGIES LTD.

IBM

ixia

Gigamon

radware

f5

The only vendor recognized in both NetFlow related Gartner reports – network visibility & security

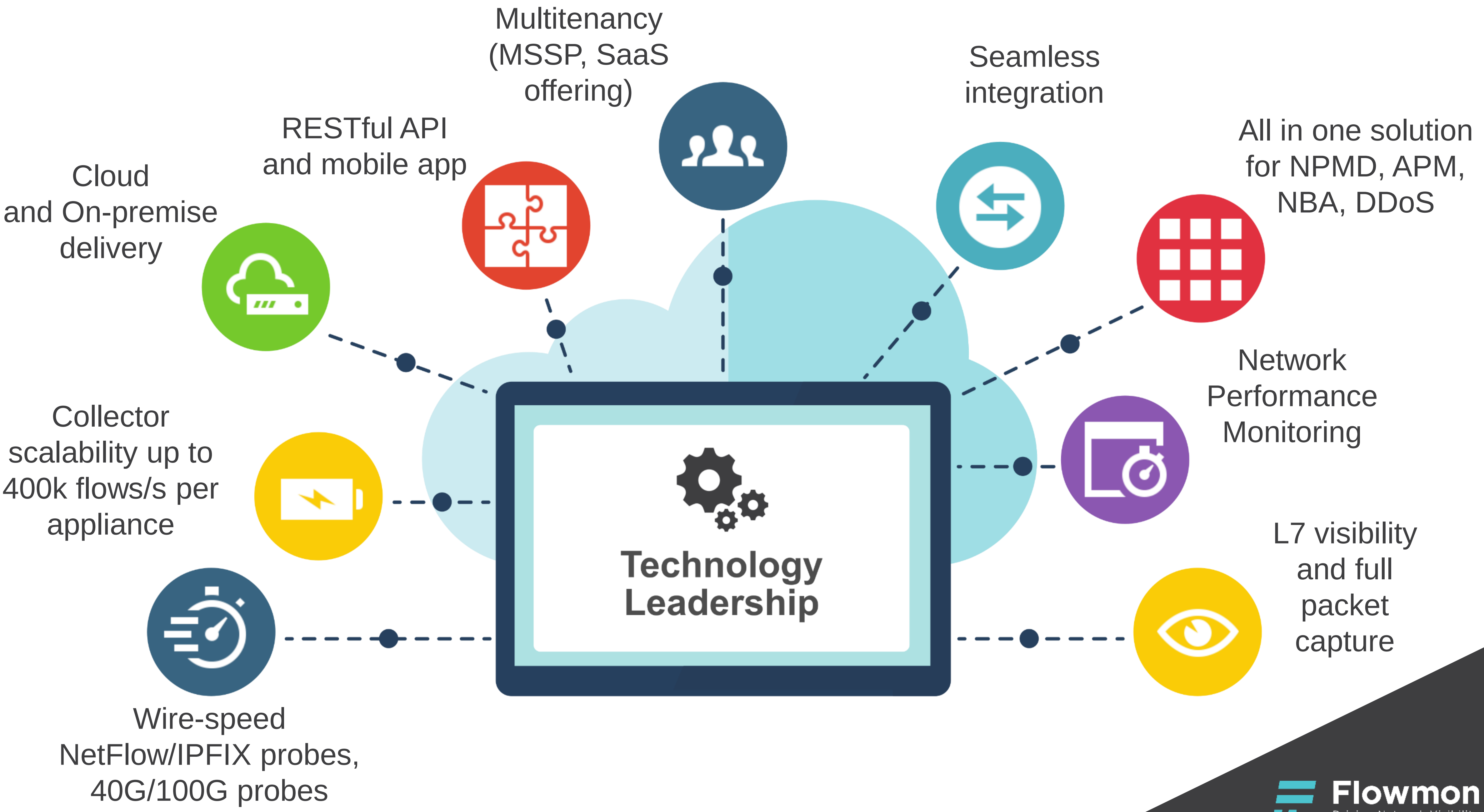
Gartner

MAGIC QUADRANT

50™ Technology Fast 50
Deloitte.

RED HERRING
WINNER 100
EUROPE

Flowmon
Driving Network Visibility



Technology Leadership

Cloud and On-premise delivery

RESTful API and mobile app

Multitenancy (MSSP, SaaS offering)

Seamless integration

All in one solution for NPMD, APM, NBA, DDoS

Network Performance Monitoring

L7 visibility and full packet capture

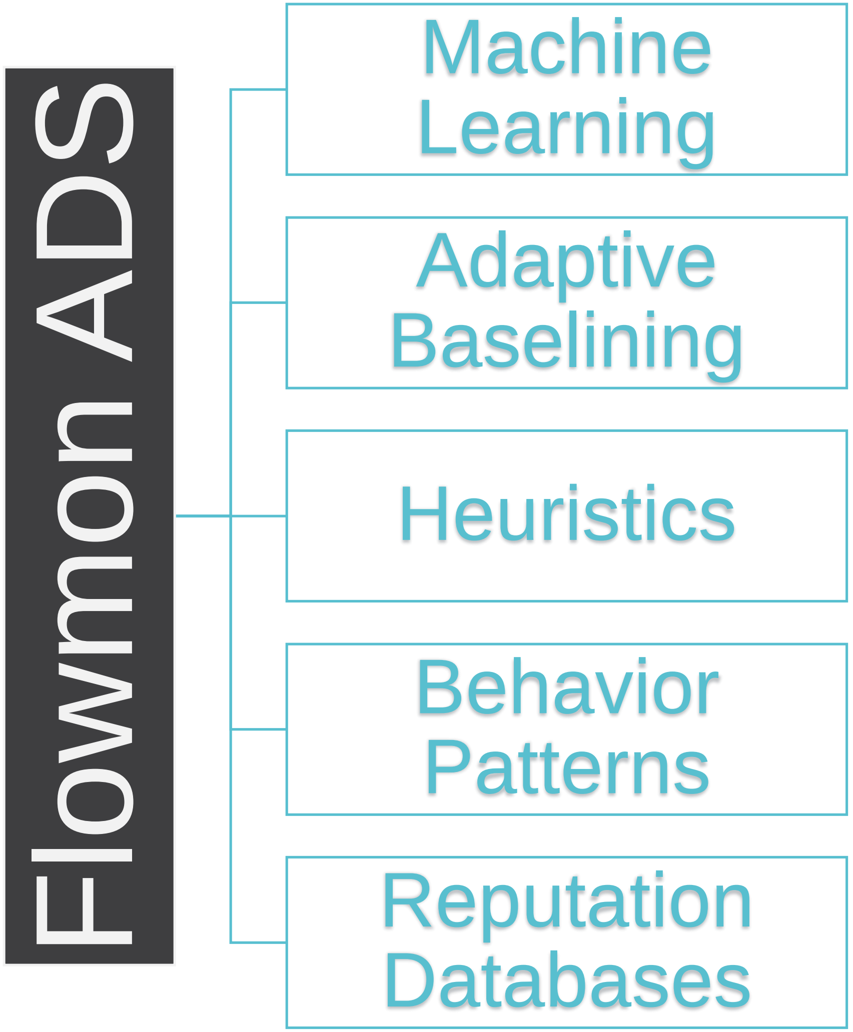
Wire-speed NetFlow/IPFIX probes, 40G/100G probes

Collector scalability up to 400k flows/s per appliance

How L3/L4 Data Helps Security?

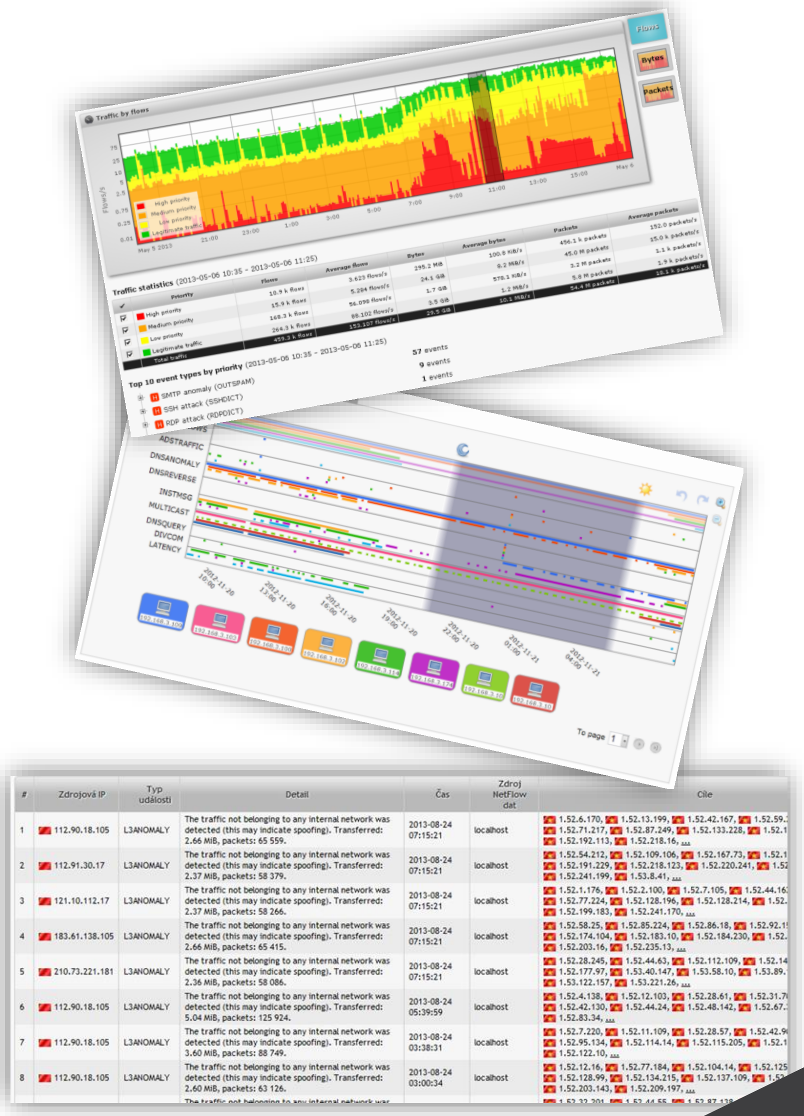
- Myth 1: **Flow is sampled and highly inaccurate.**
  - This is true for sFlow and NetFlow Lite
  - For NetFlow/IPFIX this depends on flow source
  - Probes and new network equipment do just fine
- Myth 2: **Flow is limited to L3/L4 visibility.**
  - This is the original design but today’s flow data come with L2 and L7 extensions (usually using IPFIX)
- Myth 3: **You need continuous packet capture.**
  - Flows with L7 visibility + on-demand or triggered packet capture is cost efficient option

Flowmon ADS Principles



Flowmon ADS

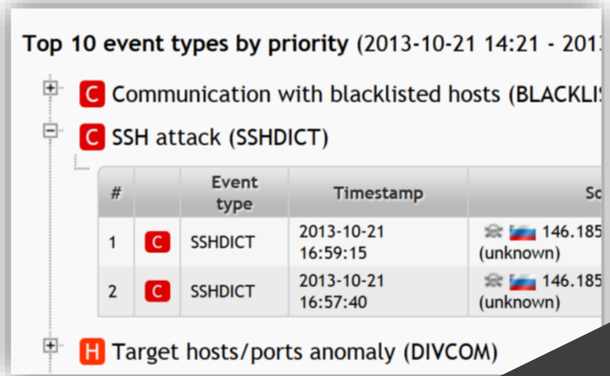
- Machine Learning
- Adaptive Baselining
- Heuristics
- Behavior Patterns
- Reputation Databases



#	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, ...
			The traffic not belonging to any internal network was			1.52.32.201, 1.52.44.55, 1.52.87.138

Traffic Analysis (Using Flows)

- Bridges the gap left by endpoint and perimeter security solutions
- Behavior based Anomaly Detection (NBA)
- Detection of security and operational issues
  - Attacks on network services, network reconnaissance
  - Infected devices and botnet C&C communication
  - Anomalies of network protocols (DNS, DHCP, …)
  - P2P traffic, TOR, on-line messengers, …
  - DDoS attacks and vulnerable services
  - Configuration issues



Top 10 event types by priority (2013-10-21 14:21 - 201

⊞ C Communication with blacklisted hosts (BLACKLI

⊟ C SSH attack (SSHDICT)

#		Event type	Timestamp	Sc
1	C	SSHDICT	2013-10-21 16:59:15	146.185 (unknown)
2	C	SSHDICT	2013-10-21 16:57:40	146.185 (unknown)

⊞ H Target hosts/ports anomaly (DIVCOM)

Use Case: DDoS Protection

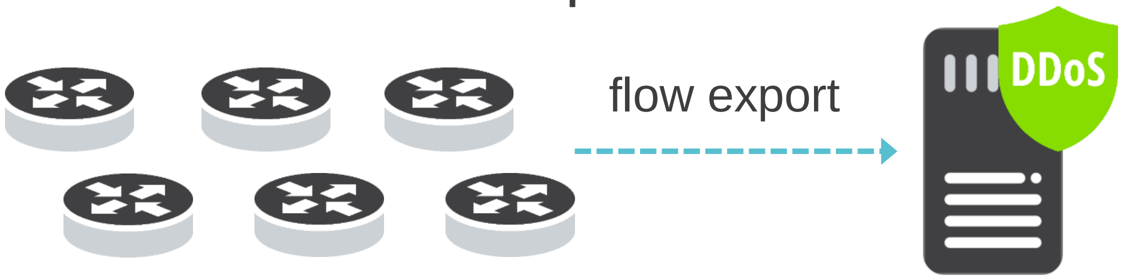
Volumetric DDoS Detection

Traffic Redirection and Mitigation Control

Flowmon
Driving Network Visibility

Backbone Protection Strategy

- Backbone perimeter specifics
  - Multiple peering points – routers & uplinks
  - Large transport capacity – tens of gigabits easily
  - In-line protection is close to impossible!



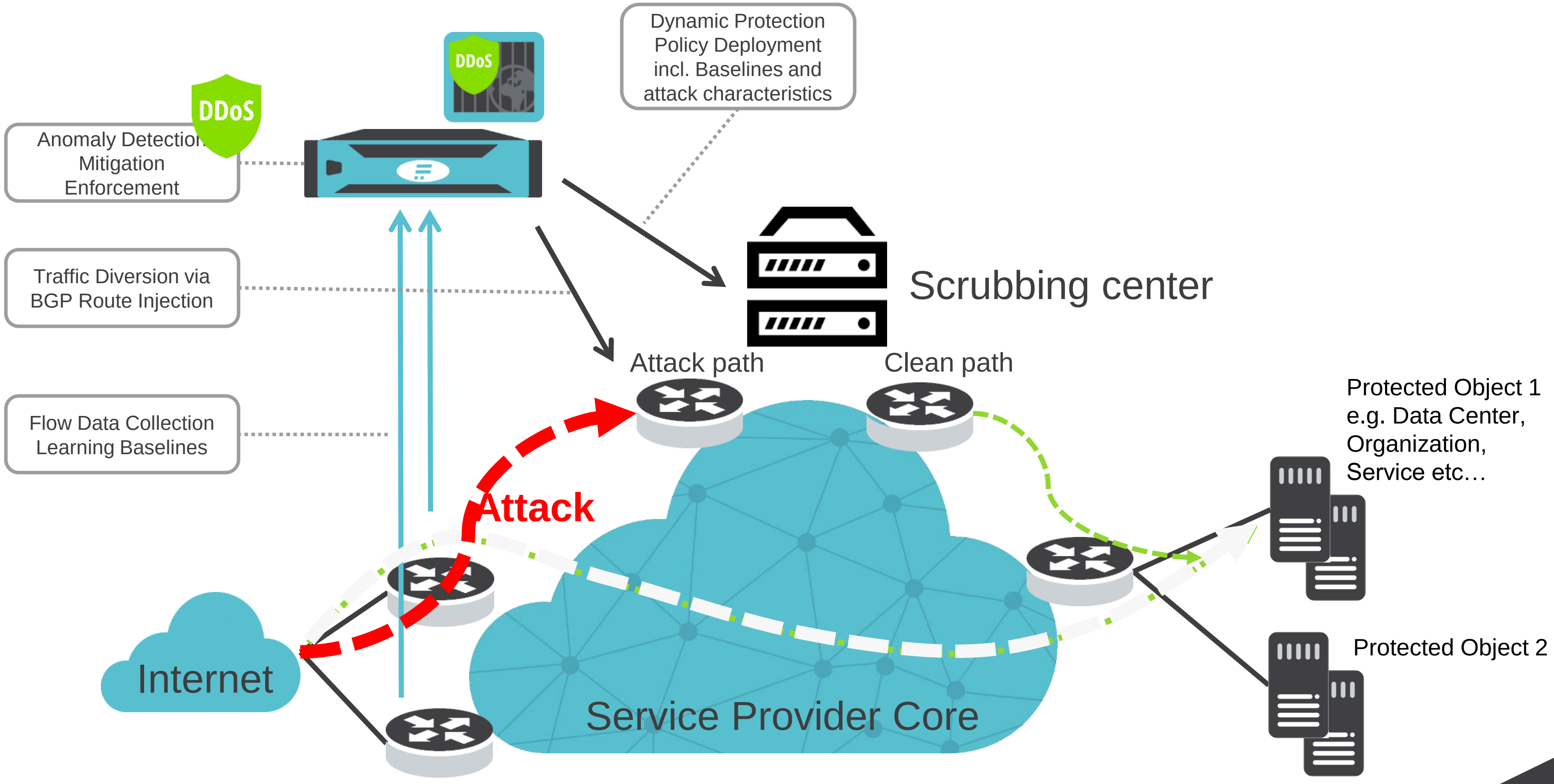
1. Flow collection
2. DDoS detection
3. Routing control
4. Mitigation control

- Flow-based detection and out-of-path mitigation
  - Easy and cost efficient to deploy in backbone/ISP
  - Prevents volumetric DDoS to reach enterprise perimeter

Flow-Based DDoS Protection

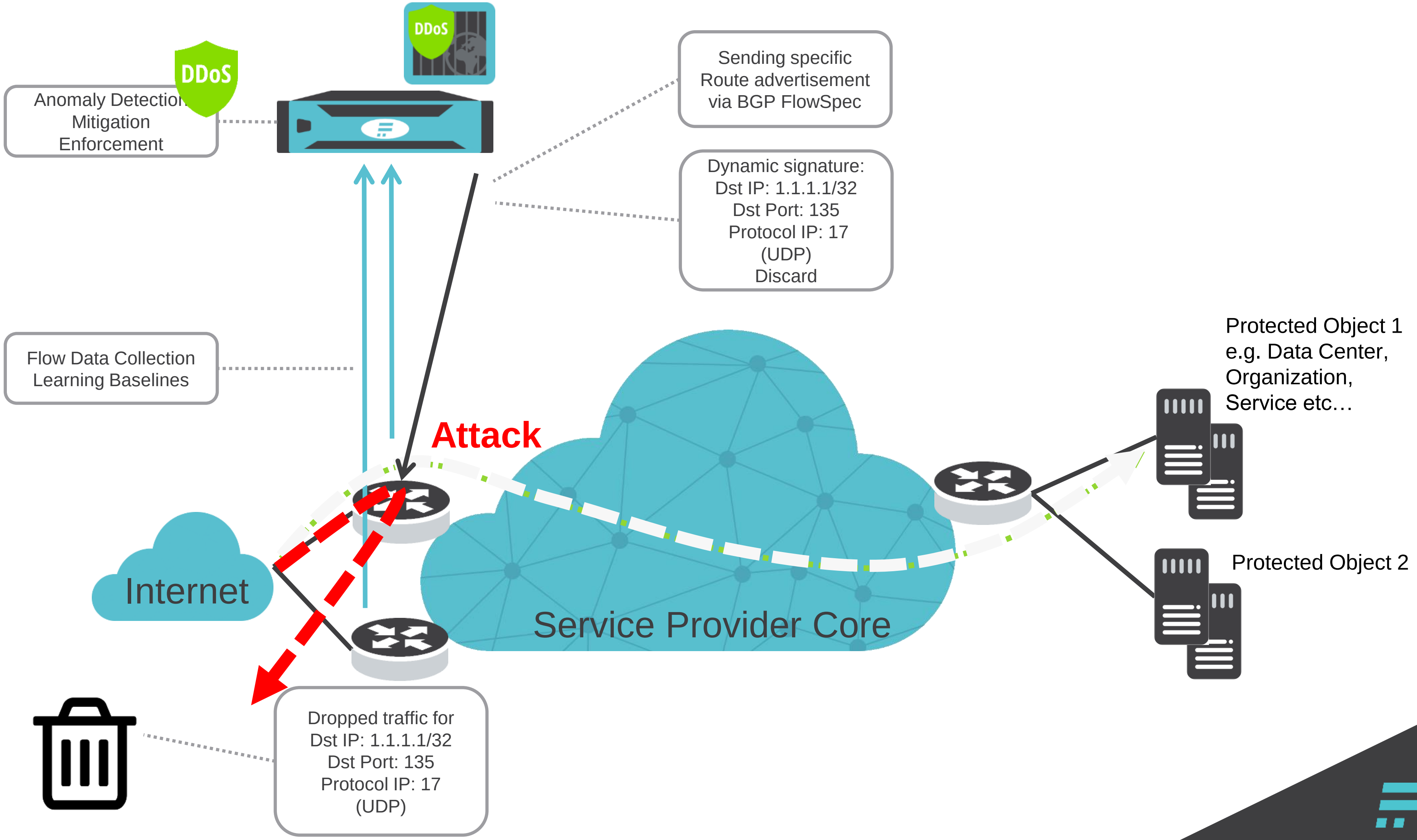
1. Definition of Customers = protected segments
   - Usually by network subnets (simple)
2. Configuration of rules for DDoS detection
   - Multiple types of baselines per protected segment
3. Alerts setup
   - Notify about attacks (humans & systems)
4. Configuration of traffic diversion = changes in routing
   - Divert traffic for mitigation of DDoS attack
5. Configuration of mitigation control = scrubbing
   - Integration with scrubbing equipment or services

Out-of-Band Mitigation Scenario



Flowmon
Driving Network Visibility

BGP Flowspec Scenario



Anomaly Detection
Mitigation
Enforcement

Sending specific
Route advertisement
via BGP FlowSpec

Dynamic signature:
Dst IP: 1.1.1.1/32
Dst Port: 135
Protocol IP: 17
(UDP)
Discard

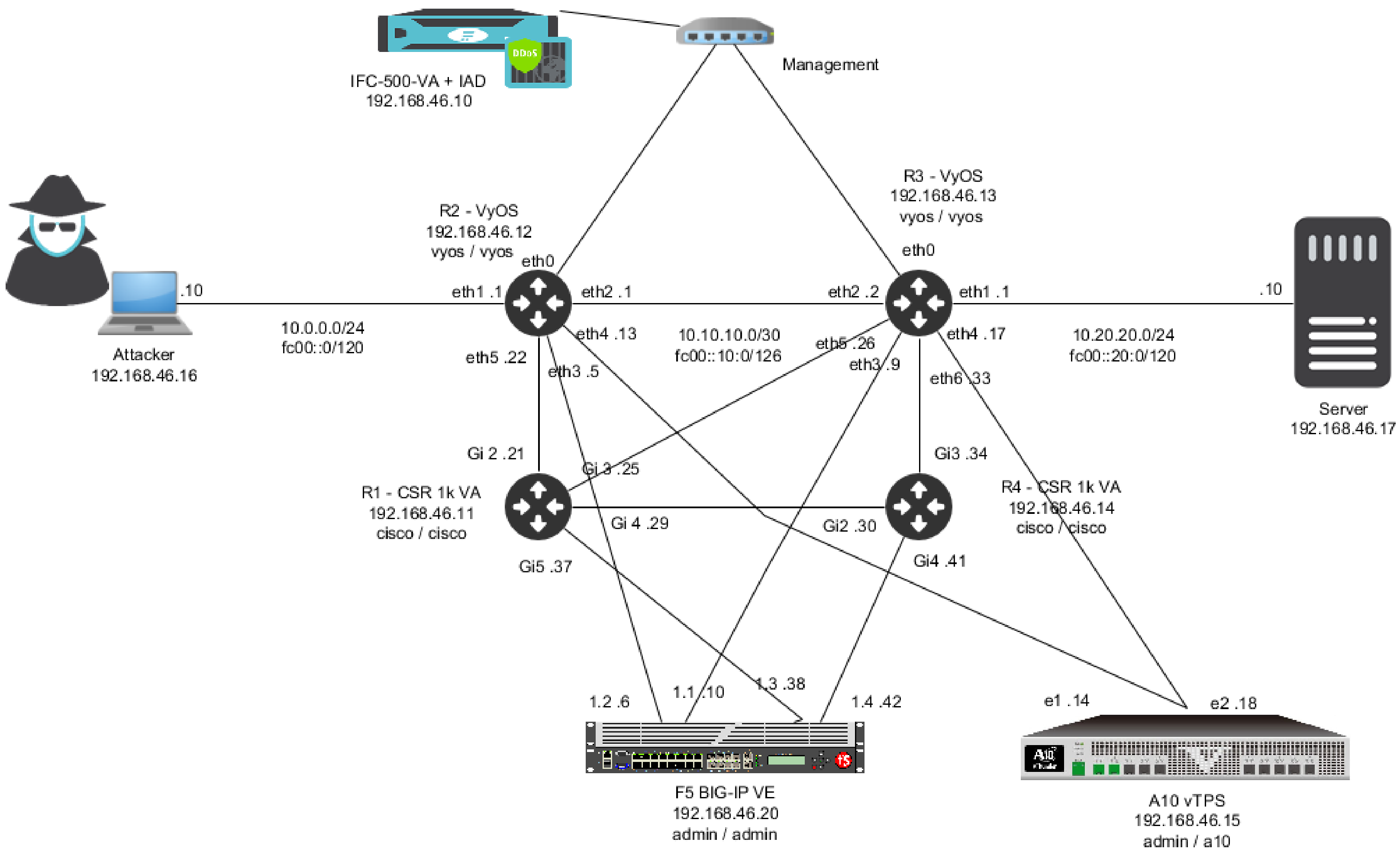
Flow Data Collection
Learning Baselines

Protected Object 1
e.g. Data Center,
Organization,
Service etc…

Protected Object 2

Dropped traffic for
Dst IP: 1.1.1.1/32
Dst Port: 135
Protocol IP: 17
(UDP)

Demonstration



Use Case: Malware Activity

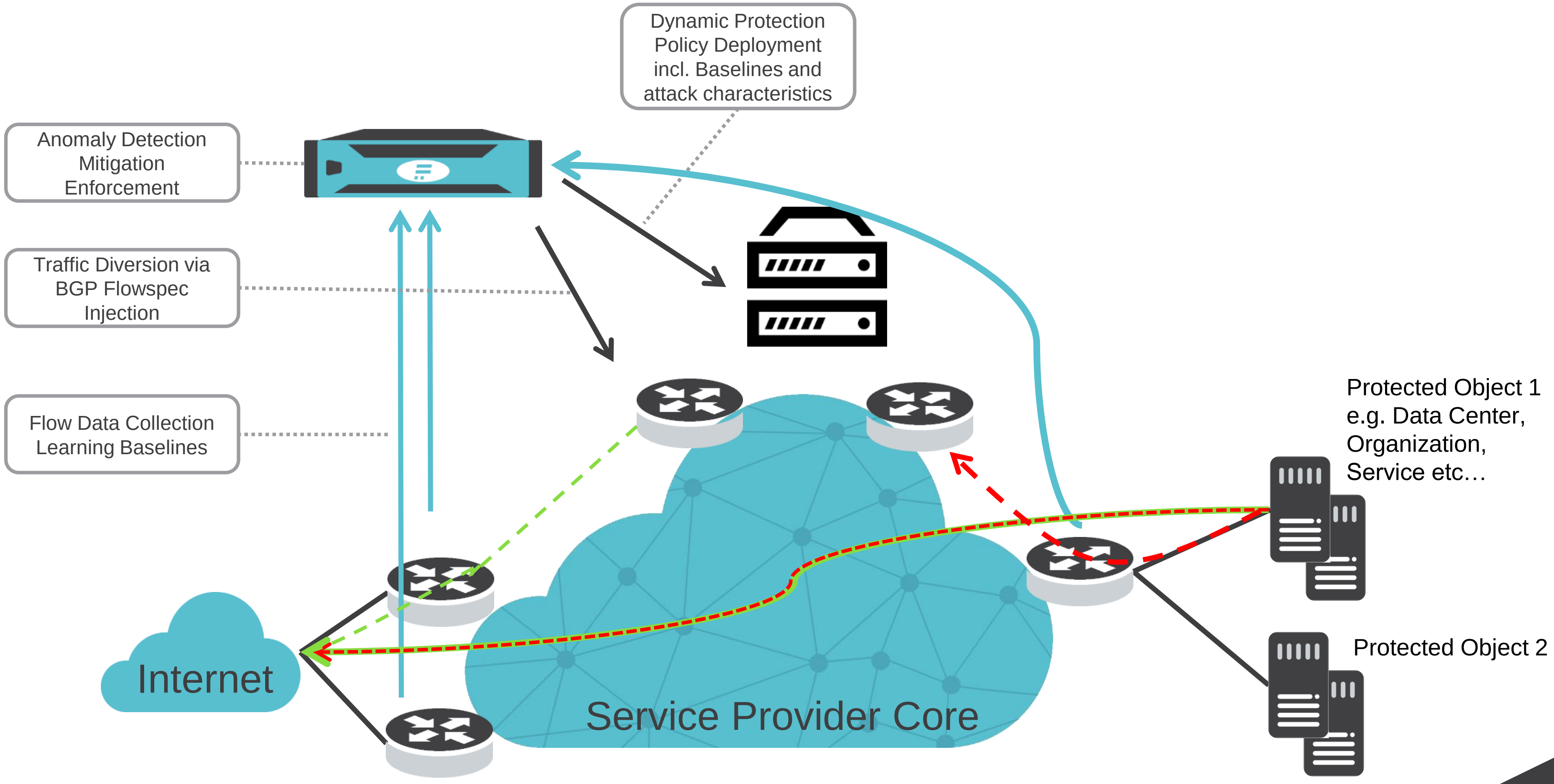
Flowmon ADS

Flowmon
Driving Network Visibility

Visibility Improves Security

- Information from both direction flow helps us to detect threats inside of your network
- In time detection could stop the problem to spread in your network and mitigate problem before it would create impact to the network
- Scripting capability can help to integrate with other tools used for the analysis
- You can resolve such issues before someone complain about them

Inside Traffic Monitoring and Mitigation



Dynamic Protection Policy Deployment incl. Baselines and attack characteristics

Anomaly Detection
Mitigation
Enforcement

Traffic Diversion via BGP Flowspec Injection

Flow Data Collection
Learning Baselines

Protected Object 1
e.g. Data Center,
Organization,
Service etc…

Protected Object 2

Thank you

Single solution for network visibility and security for your network

Jiri Knapek, Presales Engineer

Jiri.Knapek@flowmon.com

Flowmon Networks a.s.
Sochorova 3232/34
616 00 Brno, Czech Republic
www.flowmon.com

Flowmon
Driving Network Visibility