Bezpečnost sítě založena na NetFlow/IPFIX

Monitorování výkonu, viditelnost a bezpečnost s jediným řešením

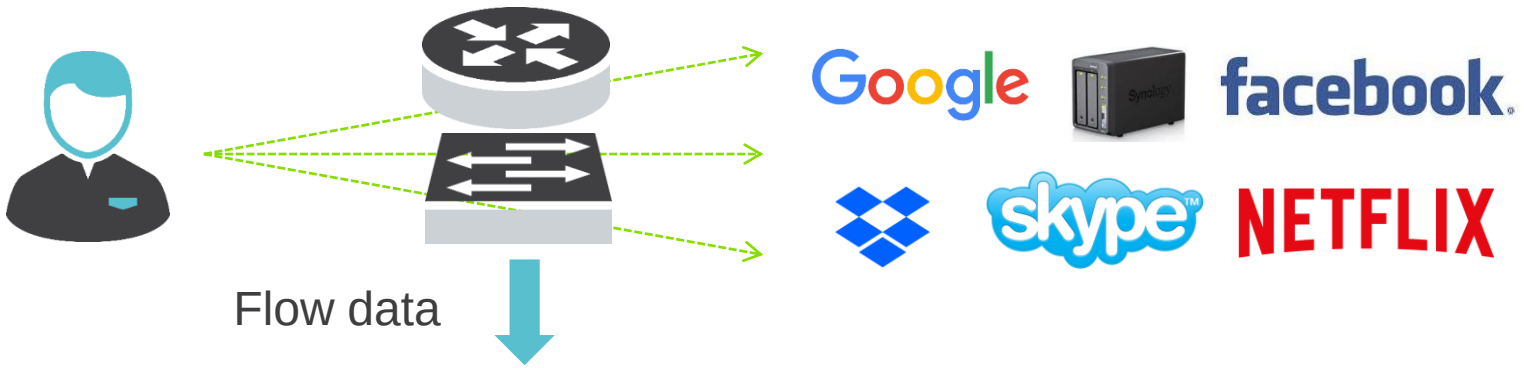
Ing. Lukáš Rauscher, Business Development Manager

lukas.rauscher@flowmon.com + 420 777 236 274

Flowmon
Driving Network Visibility

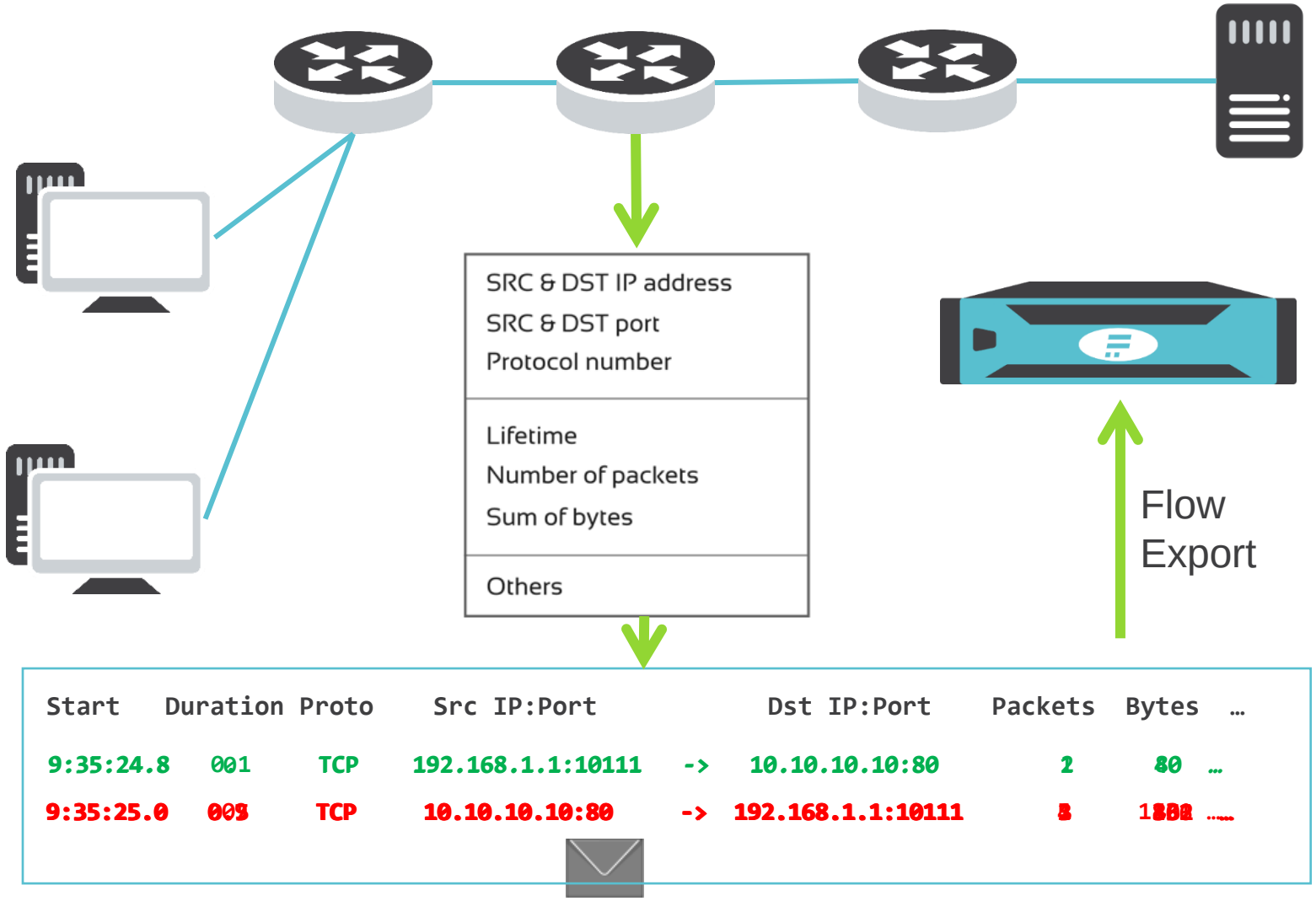
Co to jsou flow data?

- Moderní metoda pro síťový monitoring – měření flow dat
- Cisco standard NetFlow v5/v9, IETF standard IPFIX
- Zaměřeno na L3/L4 informace a volumetrické parametry
- Skutečný síťový provoz flow statistik snížený v poměru 500:1



Flowmon
Driving Network Visibility

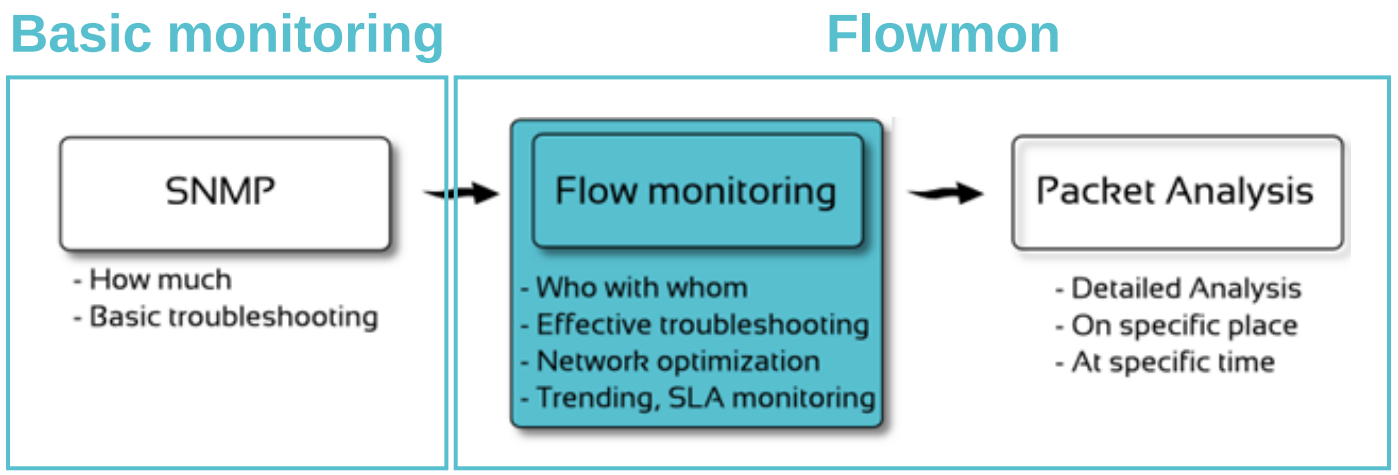
Flow Monitoring Principle



Flowmon
Driving Network Visibility

Úrovně viditelnosti

- SNMP monitoring
  - Množství přenesených dat, počet paketů, nedostatečné
- Flow monitoring založený na IP flows
  - Viditelnost do složení provozu, detekce anomálií a reporting
- Analýza paketů
  - Forenzní analýza a řešení specifických problémů



Flow data vs. Analýza paketů

	Analýza paketů	Slabé stránky
Flow data	• Pracuje ve vysokorychlostních sítích • Odolný vůči šifrované komunikaci • Viditelnost a podávání zpráv • Analýza chování sítě	• Chybí datová vrstva aplikace • Někdy nedostatek detailů • Samplování (směrovače, přepínače)
Analýza paketů	• Plný provoz v síti • Dostatek podrobností k řešení problému • Podpora forenzní analýzy • Podpisově založená detekce	• Neužitečná pro šifrovanou komunikaci • Obvykle příliš mnoho detailů • Velmi náročný zdroj

- Řešení?
  - Využití silných stránek v jednom řešení
  - Univerzální a flexibilní sondy s viditelností do všech vrstev sítě – **dlouhodobá strategie Flowmon**

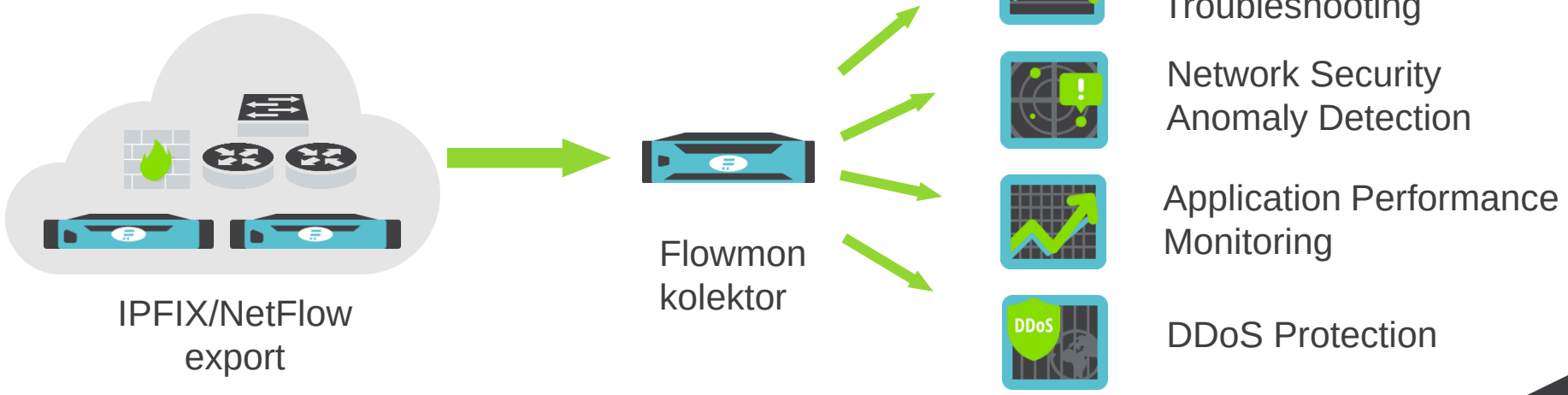
Flowmon
Driving Network Visibility

Architektura řešení Flowmon

- Flowmon sondy
  - Pasivní zdroj NetFlow/IPFIX dat
- Flowmon kolektory
  - Sběr flow dat, report, analýza
- Flowmon moduly

vmware® Microsoft Hyper-V KVM

CLOUD



Flowmon
Driving Network Visibility

Flowmon sondy

- Všestranný a flexibilní exportér flow dat
  - V porovnání s tradičními exportéry sonda obohacuje tradiční flow statistiky, díky tomu získáváme podrobnější přehled o síťovém provozu
  - Nevzorkovaný export v NetFlow v5/v9 nebo IPFIX
  - Wire-speed, L2-L7 viditelnost, Záchyt paketů dle potřeby

L2	L3/L4	L7	
• MAC • VLAN • MPLS • GRE tunnel • OTV	• Standardní položky • NPM metriky • RTT, SRT, … • TTL, SYN velikost, … • ASN • Geolokace	• NBAR2 • HTTP • SNI • DNS • DHCP	• SMB/CIFS • VoIP (SIP) • Email • SQL

Flowmon
Driving Network Visibility

Flowmon

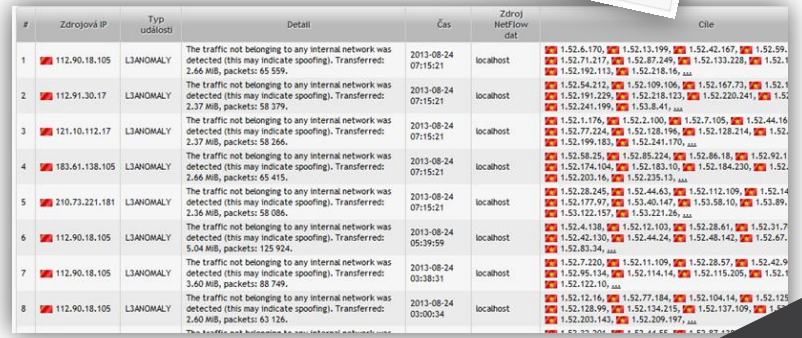
Behaviorální analýza

Flowmon
Driving Network Visibility

Technologie Flowmon ADS

Flowmon ADS

- Strojové učení
- Adaptivní baselining
- Heuristika
- Vzory chování
- Reputační databáze

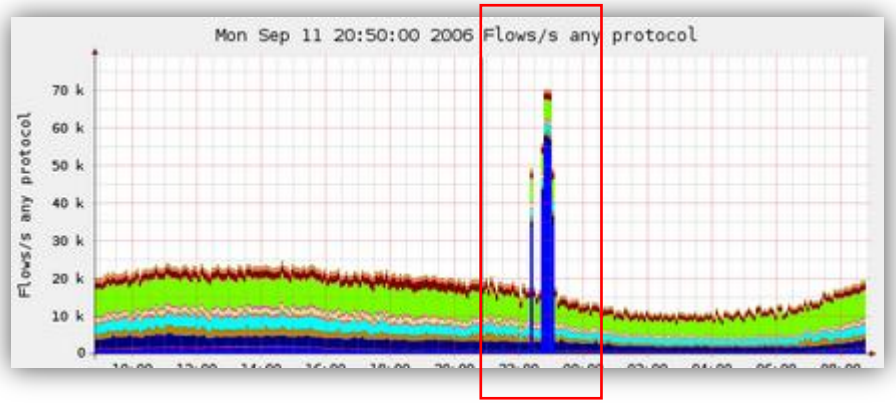


#	Zdrojová IP	Typ události	Detail	Čas	Zdroj NetFlow dat	Cíle
1	112.90.18.105	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred: 2.66 MiB, packets: 65 559.	2013-08-24 07:15:21	localhost	1.52.6.170, 1.52.13.199, 1.52.42.167, 1.52.59. 1.52.71.217, 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, ...

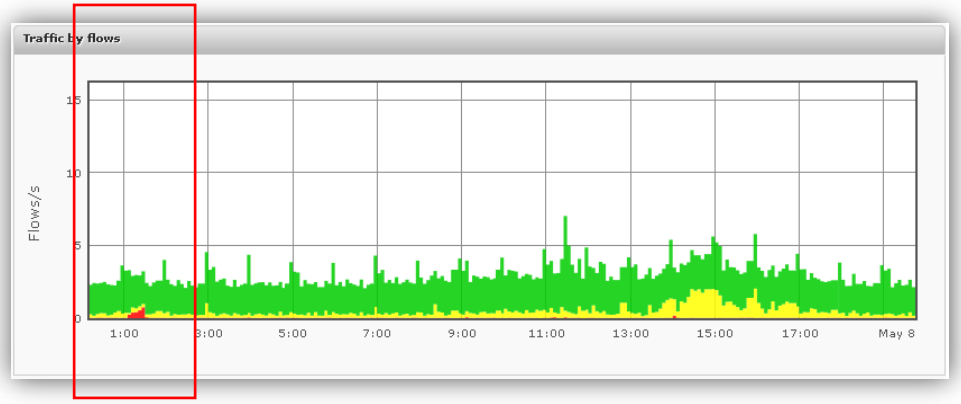
Flowmon
Driving Network Visibility

Analýza provozu z flow dat

- Koncept sítě jako sensor a nástroj pro dynamickou konfiguraci
- Doplňuje se s metodami založenými na signaturách
- Klíčová technologie pro odezvu na incident
- Navrženo pro práci v nejrychlejších sítích



Statistická analýza
Detekce volumetrických anomálií

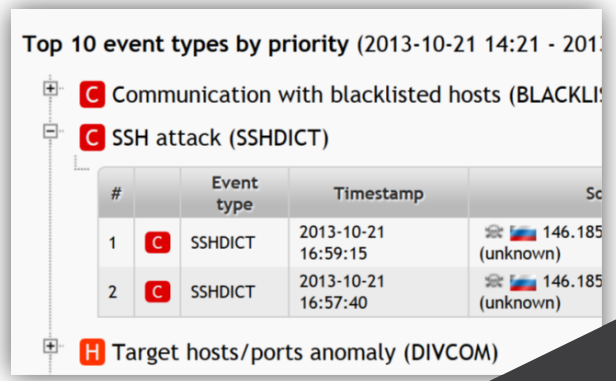


Pokročilé algoritmy pro datovou analýzu
Detekce nevolumetrických anomálií

Flowmon
Driving Network Visibility

Hrozby

- Detekce bezpečnostních a provozních problémů
  - Útoky na síťové služby, skenování sítě
  - Infikované zařízení a komunikace botnetu s C&C
  - Anomálie síťových protokolů (DNS, DHCP, …)
  - P2P provoz, TOR, vysoký upload, …
  - DDoS útoky a zranitelnosti služeb
  - Špatně nakonfigurované služby
  - Prolamování hesel
  - Scenování portů



Flowmon
Driving Network Visibility

Shrnutí

- Neexistuje jediné univerzální řešení
- Bezpečnost je záležitost vyrovnané kombinace
  - Technologií, lidí a procesů
  - Posunem monitoringu infrastruktury na další úroveň
  - Síťovou viditelností, inženýrstvím a troubleshootingem
  - Analýzou výkonu a reportingem
  - Vyplněním mezery zanechané produkty založenými na signaturách
  - Detekcí a řízením mitigace volumetrických DDoS útoků
  - Odezvou na incidenty a plným záchytem paketů na vyžádání

Partnerství s předními technologickými společnostmi

Jediný výrobce uznaný společností Gartner zároveň v oblastech síťová viditelnost a bezpečnost

Gartner MAGIC QUADRANT

50 Technology Fast 50 Deloitte.

RED HERRING EUROPE WINNER 100

Flowmon Driving Network Visibility

Flowmon Networks

Výrobce inovativního řešení pro monitorování provozu, výkonnosti a bezpečnosti sítí

1000+ zákazníků ve více než 40 zemích

První 100G sondy na světě

Silné R&D zázemí

Evropský původ

Zákaznické reference

SEGA, AVG, KBC, Konica Minolta, Vodafone, TDK, Oriflame Sweden, Siemens, Slovenská sporiteľňa, Volkswagen, orange, Telefónica, Allianz, hp, T-Mobile, GÉANT, KIA, upc, Raiffeisen Bank, e·on

Flowmon
Driving Network Visibility

Děkuji za pozornost

Monitorování výkonu, viditelnost a bezpečnost s jediným řešením

Ing. Lukáš Rauscher, Business Development Manager

lukas.rauscher@flowmon.com + 420 777 236 274

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

Flowmon
Driving Network Visibility