Bezpečnost sítě založená na NetFlow/IPFIX

Patricie Baroňová, Business Development Manager

patricie.baronova@flowmon.com 606 677 700

Flowmon

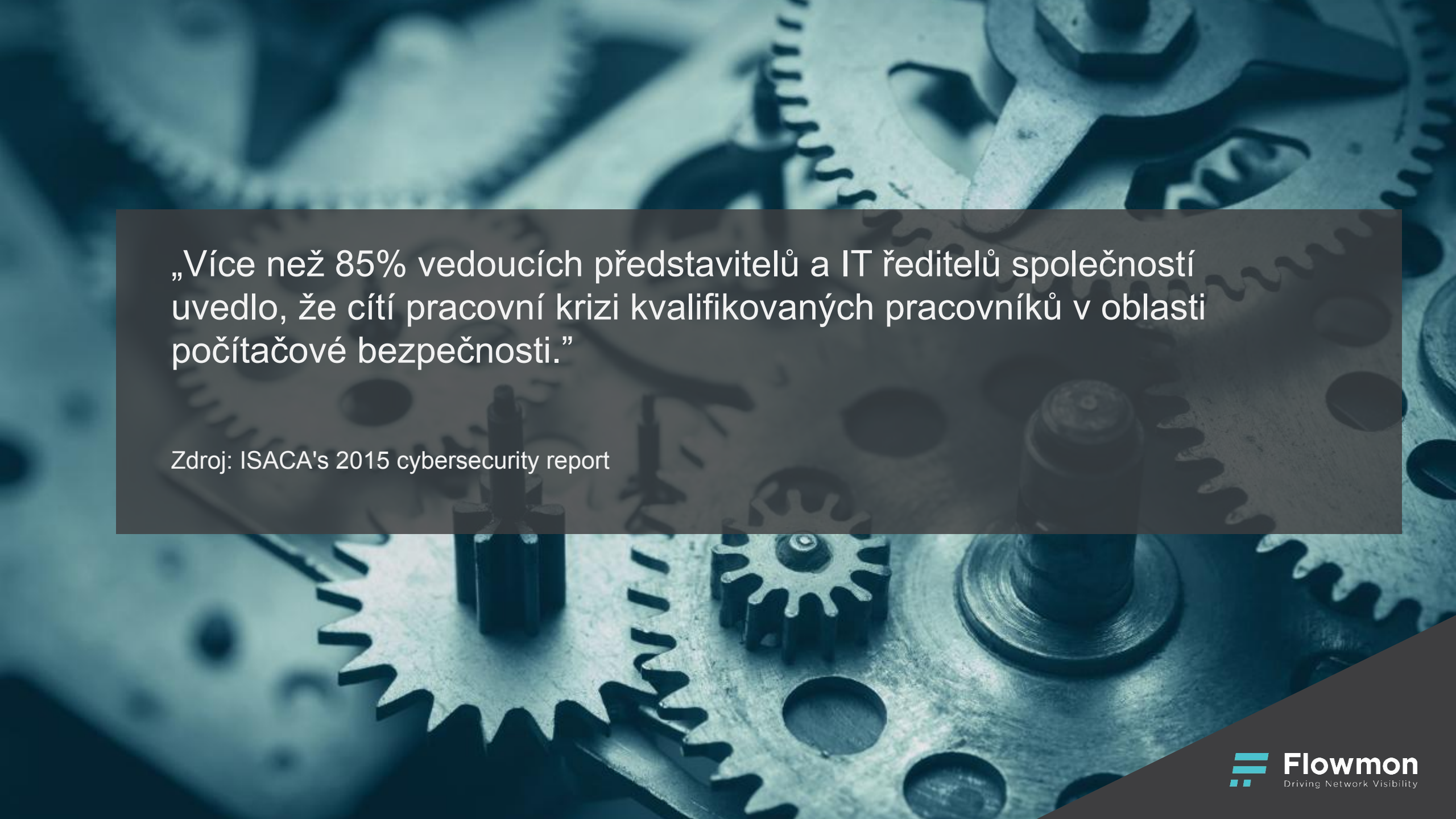
Driving Network Visibility

Nikdy jsme nebyli na počítačové síti závislejší

Sítě jsou příliš komplikované na správu

Zkušených expertů je nedostatek

Flowmon
Driving Network Visibility



„Více než 85% vedoucích představitelů a IT ředitelů společností uvedlo, že cítí pracovní krizi kvalifikovaných pracovníků v oblasti počítačové bezpečnosti.”

Zdroj: ISACA's 2015 cybersecurity report

Flowmon
Driving Network Visibility

Perimetrová vs. interní bezpečnost

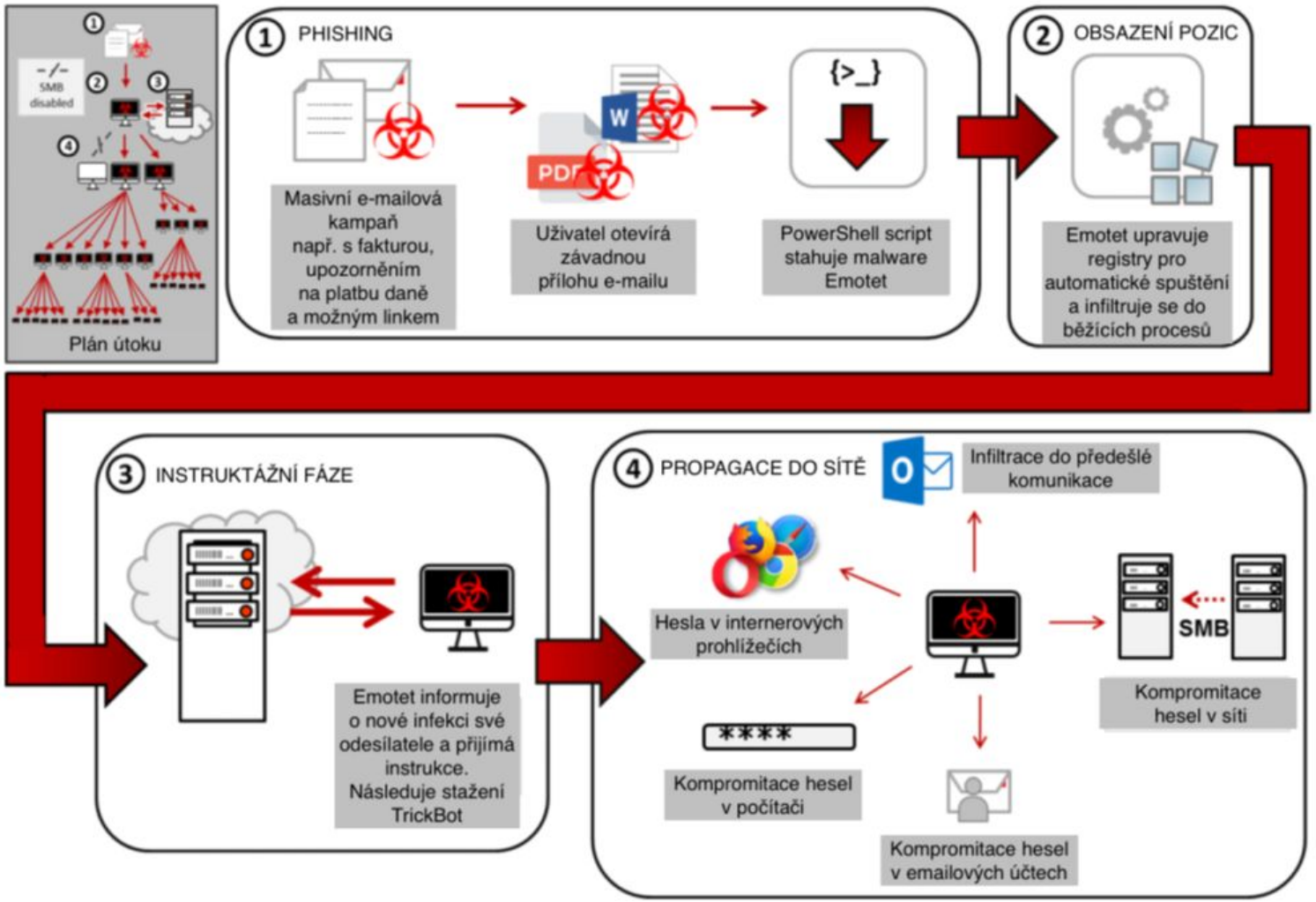
90% rozpočtu na bezpečnost utrácíme na perimetr, ale jen 25% sem cílí.

Flowmon
Driving Network Visibility

Stav infrastruktury před incidentem

- FW - výkonnostně nedostačuje
- Antivirus na koncových stanicích i serverech
- Většina serverů běží na starém virtualizačním prostředí
- Nedostatečná segmentace sítě
- Stanice mix OS od Win XP po Win 10
- „Black box“ - zařízení pro specializovaná vyšetření (rentgen, ultrazvuk, CT)
- Neomezený přístup na internet všem
- Otevřené RDP do internetu

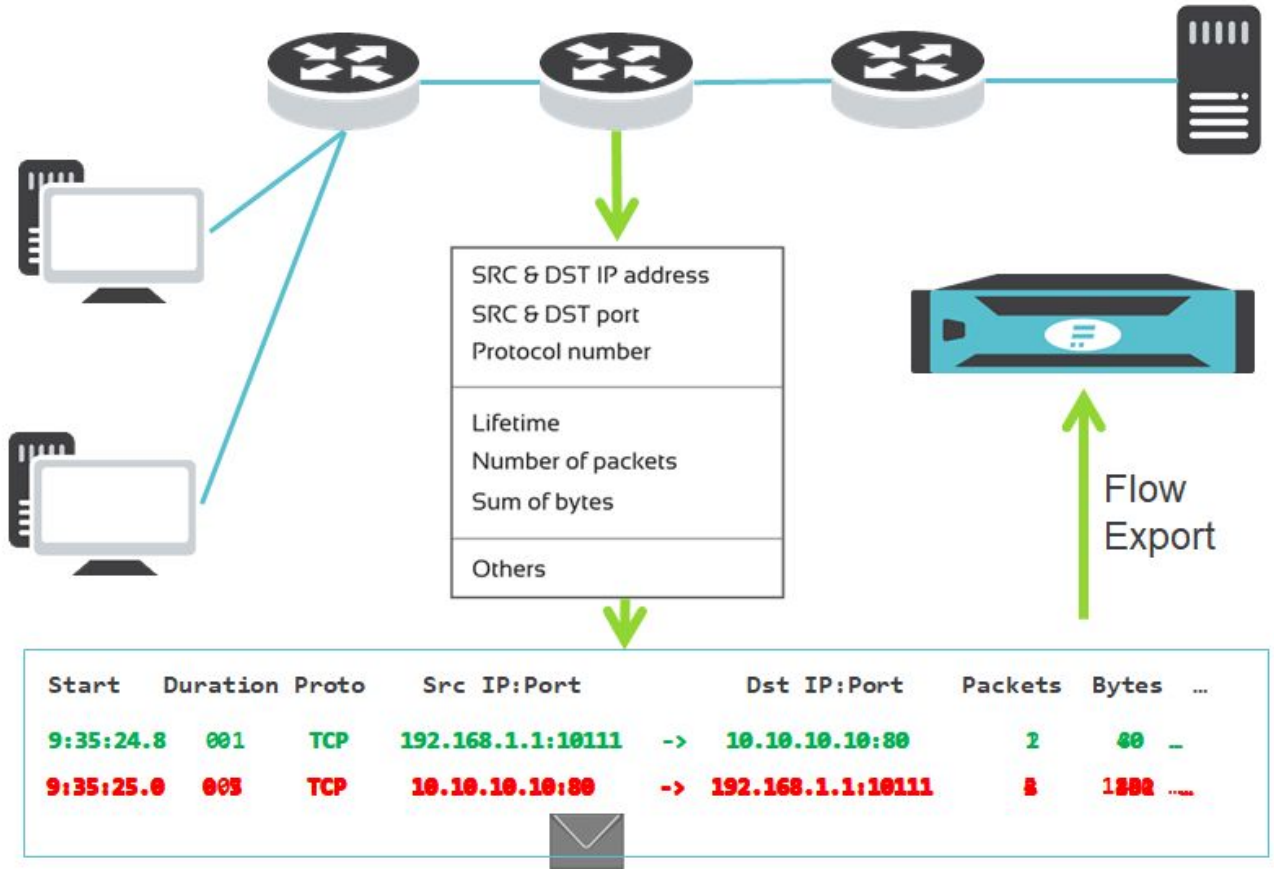
Jakmile jednou proběhne infekce zařízení uvnitř sítě, perimetrová ochrana a prevence jsou k ničemu.



- Necílená phishingová kampaň
- Otevření závadné přílohy
- Instalace malware **Emotet**
- Scan systémů a následné stažení trojan **TrickBot**
- Scan účtů, prolomení hesel administrátorů
- Rozšíření po síti
- Stažení ransomware **RYUK** - šifrování systémů

Flowmon
Driving Network Visibility

Flow Monitoring Principle



Flowmon
Driving Network Visibility

Úrovně viditelnosti

SNMP monitoring

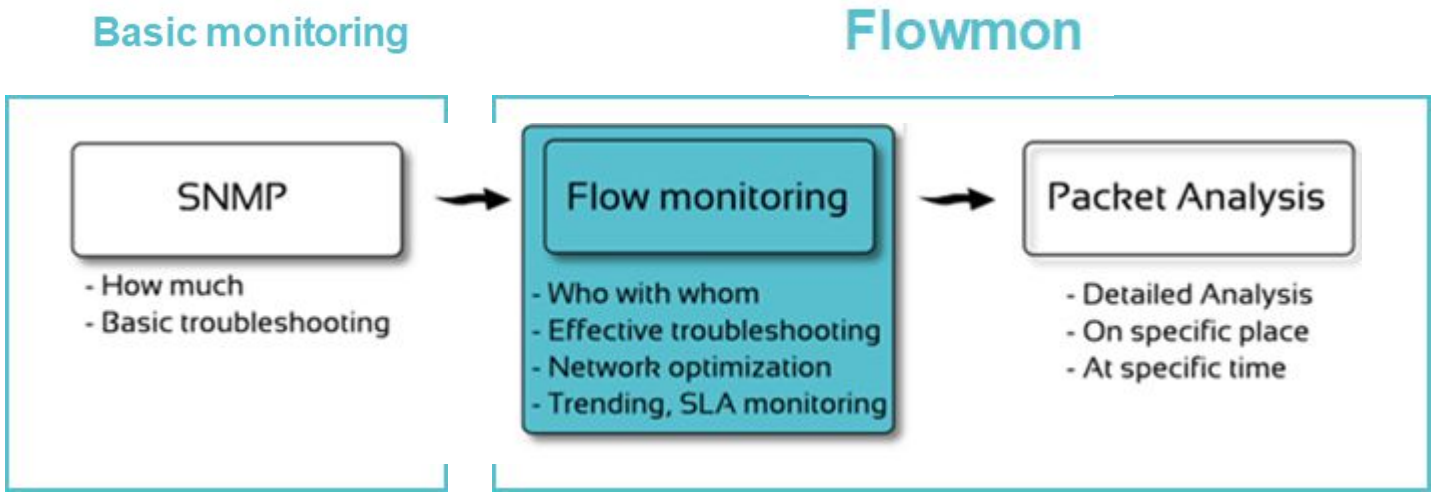
- Množství přenesených dat, počet paketů, nedostatečné

Flow monitoring založený na IP flows

- Viditelnost do složení provozu, detekce anomálií a reporting

Analýza paketů

- Forenzní analýza a řešení specifických problémů



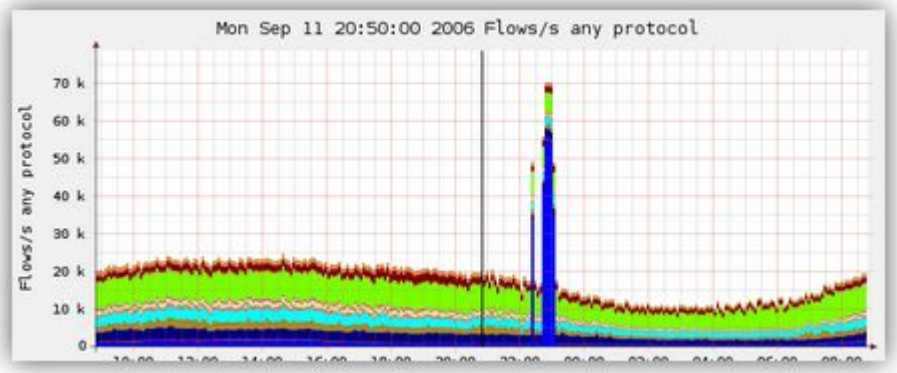
Analýza provozu z flow dat

Koncept sítě jako sensor a nástroj pro dynamickou konfiguraci

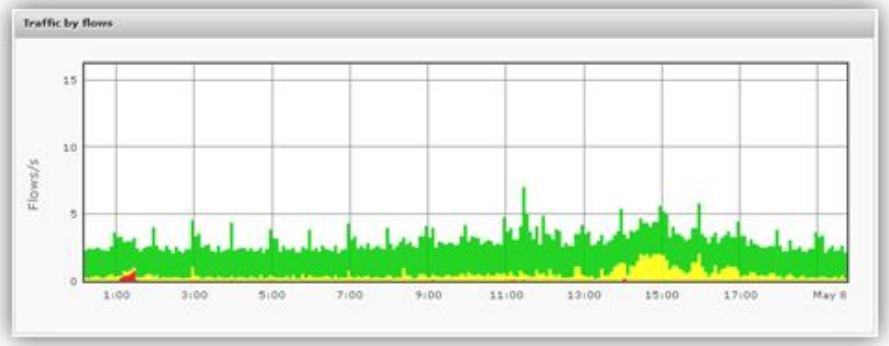
Doplňuje se s metodami založenými na signaturách

Klíčová technologie pro odezvu na incident

Navrženo pro práci v nejrychlejších sítích



Statistická analýza
Detekce volumetrických anomálií

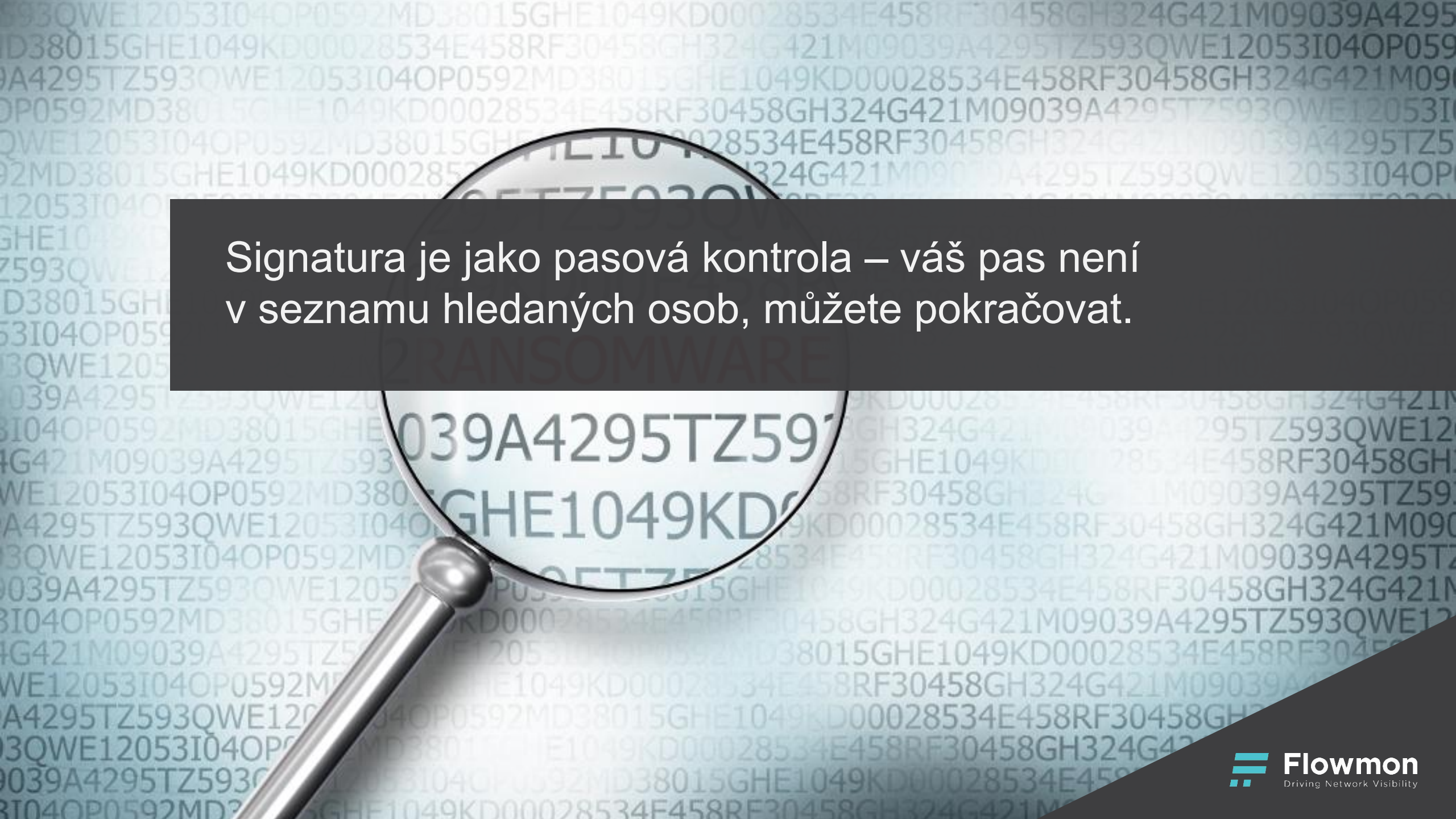


Anylýza chování NBA
Pokročilé algoritmy pro datovou analýzu
Detekce nevolumetrických anomálií

Flowmon
Driving Network Visibility

Behaviorální analýza a detekce anomálií

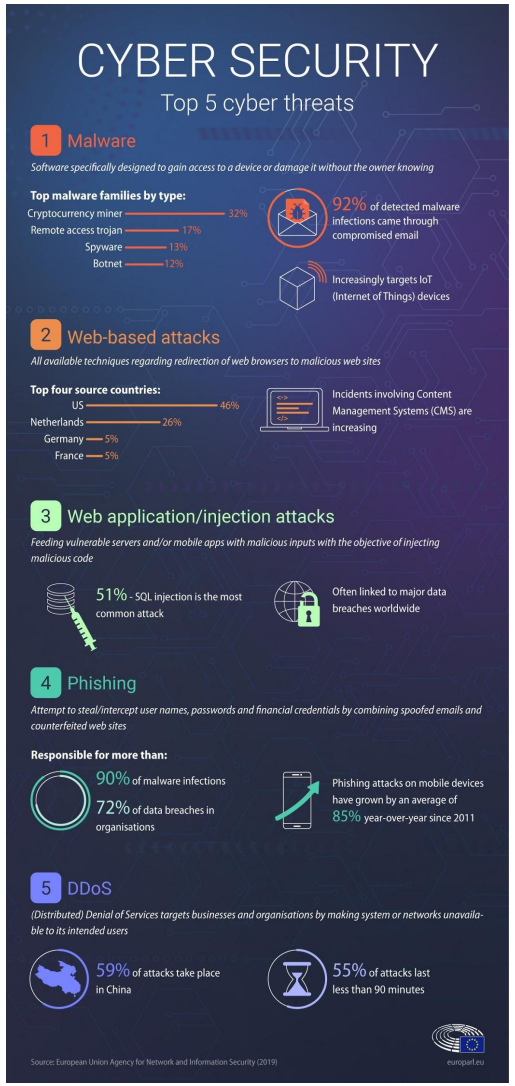
Flowmon
Driving Network Visibility


Signatura je jako pasová kontrola – váš pas není v seznamu hledaných osob, můžete pokračovat.
Flowmon
Driving Network Visibility

Behaviorální analýza je mozek, který sleduje veškerý pohyb na letišti a s vysokou přesností určí podezřelé osoby.

Flowmon
Driving Network Visibility

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

Skenování portů

Flowmon
Driving Network Visibility

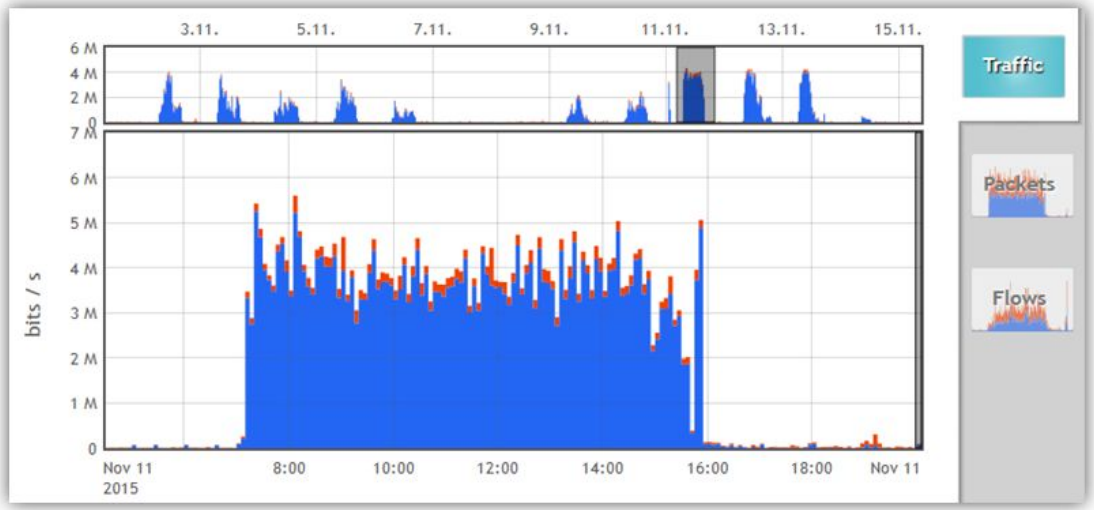
Využití sítě

- Pomalé připojení k internetu

Síť je dnes opravdu pomalá
Načítání webových stránek trvá dlouhé minuty
Vzdálení uživatelé na home office nemohou pracovat v IS

Využití sítě

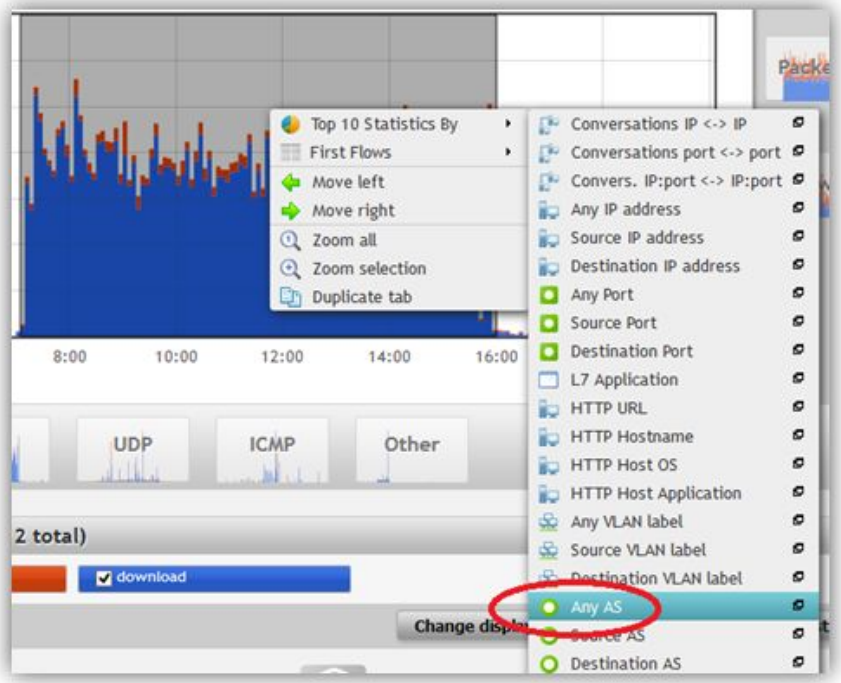
Internetová linka je dnes saturována více než obvykle

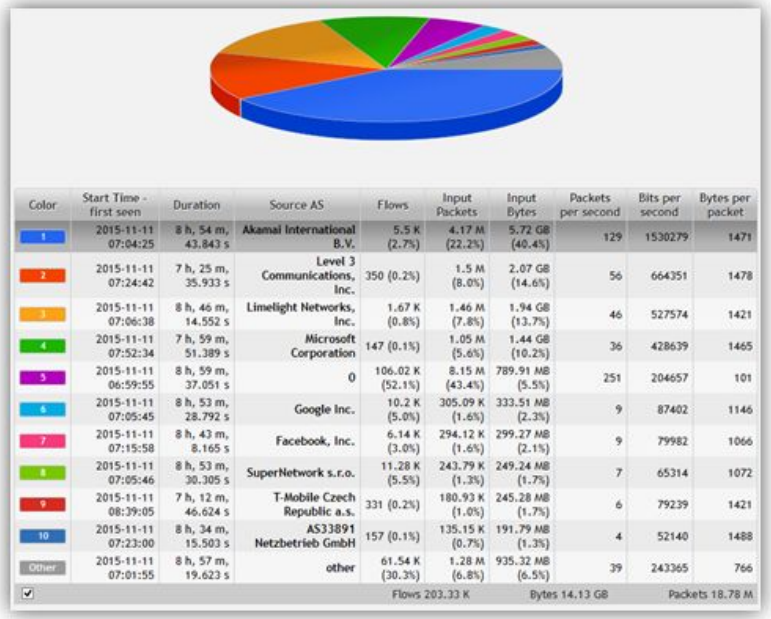


Flowmon
Driving Network Visibility

Využití sítě

Odkud to přichází?



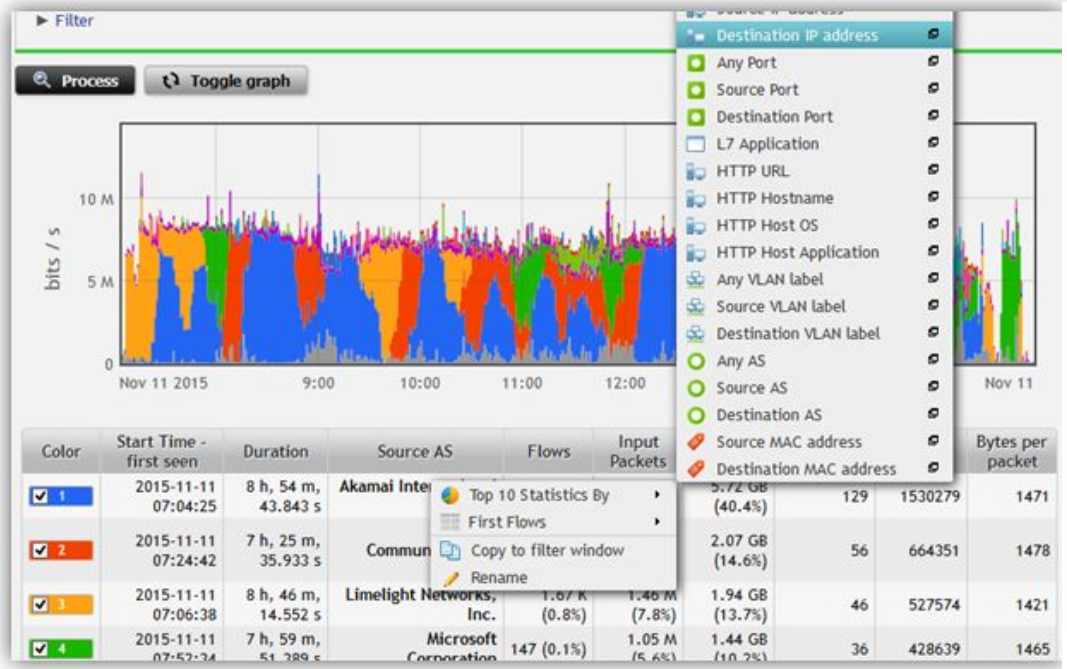


Color	Start Time - first seen	Duration	Source AS	Flows	Input Packets	Input Bytes	Packets per second	Bits per second	Bytes per packet
1	2015-11-11 07:04:25	8 h, 54 m, 43.843 s	Akamai International B.V.	5.5 K (2.7%)	4.17 M (22.2%)	5.72 GB (40.4%)	129	1530279	1471
2	2015-11-11 07:24:42	7 h, 25 m, 35.933 s	Level 3 Communications, Inc.	350 (0.2%)	1.5 M (8.0%)	2.07 GB (14.6%)	56	664351	1478
3	2015-11-11 07:06:38	8 h, 46 m, 14.552 s	Limelight Networks, Inc.	1.67 K (0.8%)	1.46 M (7.8%)	1.94 GB (13.7%)	46	527574	1421
4	2015-11-11 07:52:34	7 h, 59 m, 51.389 s	Microsoft Corporation	147 (0.1%)	1.05 M (5.6%)	1.44 GB (10.2%)	36	428639	1465
5	2015-11-11 06:59:55	8 h, 59 m, 37.051 s	0	106.02 K (52.1%)	8.15 M (43.4%)	789.91 MB (5.5%)	251	204657	101
6	2015-11-11 07:05:45	8 h, 53 m, 28.792 s	Google Inc.	10.2 K (5.0%)	305.09 K (1.6%)	333.51 MB (2.3%)	9	87402	1146
7	2015-11-11 07:15:58	8 h, 43 m, 8.165 s	Facebook, Inc.	6.14 K (3.0%)	294.12 K (1.6%)	299.27 MB (2.1%)	9	79982	1066
8	2015-11-11 07:05:46	8 h, 53 m, 30.305 s	SuperNetwork s.r.o.	11.28 K (5.5%)	243.79 K (1.3%)	249.24 MB (1.7%)	7	65314	1072
9	2015-11-11 08:39:05	7 h, 12 m, 46.624 s	T-Mobile Czech Republic a.s.	331 (0.2%)	180.93 K (1.0%)	245.28 MB (1.7%)	6	79239	1421
10	2015-11-11 07:23:00	8 h, 34 m, 15.503 s	AS33891 Netzbetrieb GmbH	157 (0.1%)	135.15 K (0.7%)	191.79 MB (1.3%)	4	52140	1488
Other	2015-11-11 07:01:55	8 h, 57 m, 19.623 s	other	61.54 K (30.3%)	1.28 M (6.8%)	935.32 MB (6.5%)	39	243365	766
				Flows 203.33 K		Bytes 14.13 GB			Packets 18.78 M

Flowmon
Driving Network Visibility

Využití sítě

Aktualizace Windows?
A ne z našeho serveru WSUS?



Start Time - first seen	Duration	Destination IP address
2015-11-11 07:15:01	8 h, 41 m, 4.621 s	192.168.0.102
2015-11-11 07:06:35	8 h, 40 m, 6.357 s	192.168.0.45
2015-11-11 08:06:41	7 h, 50 m, 33.773 s	192.168.0.52
2015-11-11 07:24:15	7 h, 41 m, 53.019 s	192.168.0.85
2015-11-11 08:16:02	7 h, 43 m, 2.050 s	192.168.0.31
2015-11-11 07:43:07	7 h, 4 m, 31.266 s	192.168.0.211
2015-11-11 07:40:29	8 h, 18 m, 23.623 s	192.168.0.54
2015-11-11 08:00:43	7 h, 38 m, 53.390 s	192.168.0.56
2015-11-11 12:04:27	3 h, 54 m, 42.020 s	192.168.0.40
2015-11-11 08:26:47	6 h, 53 m, 34.327 s	192.168.0.73

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

Flowmon
Networks

Výrobce inovativního řešení pro monitorování provozu, výkonnosti a bezpečnosti sítí

1000+ zákazníků ve více než 30 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

Patricie Baroňová

patricie.baronova@flowmon.com

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

Flowmon
Driving Network Visibility