

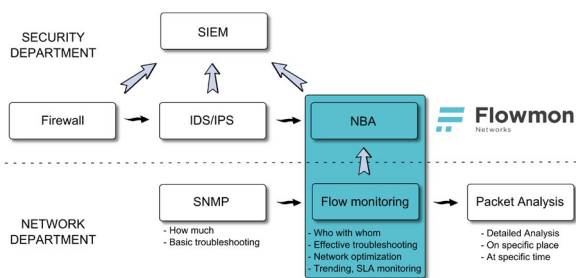
#### ÚVOD

Spolehlivá a dobře zabezpečená počítačová síť je klíčem k úspěšnému fungování každé organizace. Již krátkodobý výpadek sítě nebo úspěšný útok na data či síťovou infrastrukturu může způsobit obrovské finanční škody, poškození dobrého jména společnosti a nespokojenost nebo dokonce ztrátu zákazníků.

Síťoví a bezpečnostní administrátoři tak čelí složitému úkolu, kdy musí zvládnout správu neustále komplexnějšího IT prostředí a současně zajistit jeho ochranu proti stále pokročilejším a četnějším útokům a hrozbám. To vyžaduje využívání moderních přístupů a nástrojů, které umožní efektivně spravovat počítačovou síť a zajistí její bezpečnost. Proto většina organizací již využívá, nebo zvažuje nasazení řešení založeného na technologii monitorování datových toků, nejlépe v kombinaci s analýzou chování sítě (behaviorální analýzou).

#### MONITOROVÁNÍ SÍTÍ

Technologie monitorování datových toků (nejčastěji založená na standardu NetFlow či IPFIX) přináší detailní pohled do síťového provozu s rozlišením na jeho jednotlivé složky. Díky tomu je vhodná pro efektivní správu a řešení problémů počítačové sítě a zároveň umožňuje odhalení vnitřních i vnějších bezpečnostních hrozeb včetně těch, které nejsou schopny odhalit jiné bezpečnostní nástroje.



Monitorování datových toků poskytuje detailní informace o tom, kdo komunikoval s kým, kdy, jak dlouho, jak často, nad kterým protokolem a kolik bylo přeneseno dat. Tyto statistiky umožňují sledování vyžití sítě v reálném čase, monitorování aktivit uživatelů i služeb, optimalizaci síťové infrastruktury, sledování využití internetu a jsou vhodné i pro bezpečnostní účely v podobě detekce útoků a hrozeb či prokazování bezpečnostních incidentů. To však vyžaduje neustálou detailní analýzu dat, kterou nabízí navazující technologie behaviorální analýzy (Network Behavior Analysis – NBA), jež data nepřetržitě analyzuje s cílem detekovat v síti jakékoliv podezřelé aktivity, anomálie, útoky či hrozby.

#### KLÍČOVÉ PŘÍNOSY A VLASTNOSTI

- ▶ **Detailní přehled o dění v počítačové síti**
- ▶ **Rychlé a efektivní řešení problémů v síti**
- ▶ **Zvýšení bezpečnosti počítačové sítě**
- ▶ **Detekce pokročilých hrozeb a cílených útoků**
- ▶ **Odhalování malware a potenciálních úniků dat**
- ▶ **Snadné plánování kapacit a optimalizace sítě**
- ▶ **Zjednodušení správy sítě pro administrátory, zvýšení spokojenosti uživatelů a zákazníků**
- ▶ **Detailní monitorování uživatelů a služeb**
- ▶ **Unikátní přínosy pro všechny části organizace – síťoví a bezpečnostní administrátoři, CIOs**
- ▶ **Snadné neinvazivní nasazení do infrastruktury**
- ▶ **Založené na standardech NetFlow a IPFIX**

#### ŘEŠENÍ FLOWMON

Řešení Flowmon vhodně kombinuje technologie monitorování datových toků a analýzy chování sítě (NBA). Díky tomu velmi efektivně pomáhá síťovým i bezpečnostním administrátorům se správou, řešením problémů, optimalizací i zabezpečením počítačové sítě.

Flowmon je řešení vhodné pro nasazení do jakékoliv počítačové sítě (včetně těch virtuálních), neboť zahrnuje výkonné autonomní **Flowmon sondy** generující statistiky o síťovém provozu, **Flowmon kolektory** pro uložení, zobrazení a analýzu těchto statistik, systém **Flowmon ADS** pro automatickou analýzu provozu a identifikaci bezpečnostních a provozních incidentů, **Flowmon DDoS Defender** pro ochranu proti volumetrickým DDoS útokům, **Flowmon APM** pro monitorování výkonnosti HTTP/HTTPS a databázových aplikací a **Flowmon Traffic Recorder** pro kompletní záznam datového provozu.

Díky využití průmyslových standardů NetFlow a IPFIX je systém jednoduše rozšiřitelný, dobře škálovatelný a kompatibilní s produkty třetích stran.

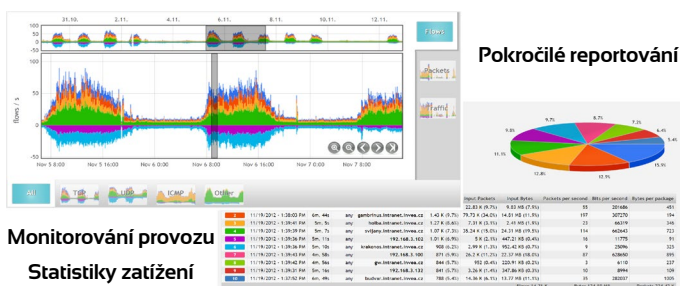


### ŘEŠENÍ FLOWMON

Flowmon je kompletní řešení pro monitorování a bezpečnost počítačových sítí **na základě IP toků** (technologie NetFlow a IPFIX) od 10 Mb/s do 100 Gb/s. Řešení Flowmon poskytuje nástroje pro sledování provozu a zabezpečení sítě, řešení problémů v síti, monitorování aktivit uživatelů a aplikací, správu a optimalizaci síťového provozu, splnění zákonných požadavků, sledování výkonových parametrů sítě (Network Performance Monitoring) a mnohem více. **Technologie analýzy chování sítě** (NBA – Network Behavior Analysis) umožňuje detekovat i hrozby, proti kterým jsou ostatní bezpečnostní nástroje neúčinné.

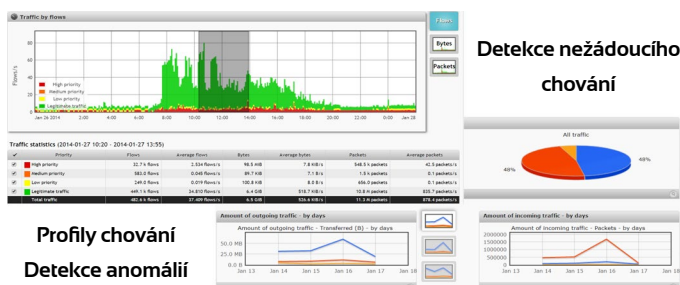
### MONITORING SÍTĚ

Podrobný přehled o provozu v síti (NetFlow, IPFIX, sFlow) pro jakékoli organizace (malé a střední podniky, velké firmy, vládní a akademické instituce, ISP).



### BEZPEČNOSTNÍ MONITORING – NBA

Modul analýzy chování sítě (NBA) používá automatickou analýzu toků k odhalení nežádoucích aktivit a chování v síti, zero-day útoků, polymorfního malware a dalších pokročilých hrozeb.



### GARTNER

**„NBA přináší viditelnost do chování vaší sítě a díky tomu doplňuje nástroje pracující na základě vzorů (signatur).“**

Network Behavior Analysis Update, GARTNER

### PŘÍNOSY ŘEŠENÍ FLOWMON

#### EFEKTIVNÍ SPRÁVA SÍTĚ A PROCESY

- ▶ Provozní a konfigurační problémy jsou detekovány a identifikovány před tím, než mohou způsobit pracovní prostoje nebo nespokojenost uživatelů a zákazníků.
- ▶ Administrátoři nejsou přetíženi provozními problémy a mohou se soustředit na optimalizaci infrastruktury a poskytovaných služeb.
- ▶ Procesy monitorování sítě požadované zákonem nebo vnitřními směrnici jsou plně automatizované.

#### ZABEZPEČENÁ INFRASTRUKTURA

- ▶ Infrastruktura je lépe chráněna proti aktuálním hrozbám (sociální inženýrství, vnitřní útoky, úniky dat, pokročilé hrozby, sofistikované útoky hackerů, atd.).
- ▶ Bezpečnostní incidenty jsou detekovány a analyzovány v reálném čase.
- ▶ Je možné eliminovat problém nelegálního software nebo zneužívání sítě zaměstnanci.

#### SNIŽOVÁNÍ NÁKLADŮ

- ▶ Významné snížení manuálních činností, problémy jsou vyřešeny rychle a efektivně.
- ▶ Snížení nákladů vyplývající z menší škody způsobené bezpečnostními incidenty.
- ▶ Optimalizace licencí síťových aplikací, SLA, optimalizace peeringových dohod, atd.

### REFERENCE



### JAK ZÍSKAT PRODUKTY FLOWMON?



Obratť se na svého systémového integrátora či přímo na nás. Rádi Vám řešení předvedeme, provedeme analýzu či navrhne projekt monitorování Vaší sítě.

[www.flowmon.com](http://www.flowmon.com)