Progress® Flowmon®

Flowmon Packet Investigator

PRODUKTOVÁ BROŽURA

Flowmon Packet Investigator (FPI) se postará o automatický audit síťového provozu, který zachytává a analyzuje kompletní paketová data.

Pomůže vám v případě, kdy flow data nestačí a potřebujete více podrobností. V takové situaci Investigator zachytává veškeré pakety týkající se provozu v okolí události a usnadní vám hloubkový troubleshooting.

Od podobných nástrojů se liší zejména tím, že obsahuje odborné znalosti. Dokáže vám tak poskytnout mnoho podrobností, zautomatizovat analýzu, vyhodnotit zaznamenané události, vyhledat chybové kódy, přinést vysvětlení chyb a navrhnout způsoby, jak je vyřešit. Příklady, kde může FPI, být nápomocné:

Problémy s připojením k síti

Tedy když komunikaci blokuje firewall, adresa je nedostupná, vyskytnou se TCP chyby a další.

Poruchy nebo špatná konfigurace

Týká se to zejména kritických síťových služeb, jako je ARP, DNS či DHCP.

Nekompatibilní šifrování mezi klientem a serverem

Odhalí nekompatibilitu u SSL/TLS verzí, šifrovacích algoritmů, certifikátů a podobně.

Problémy se sadou aplikačních protokolů

Zejména u protokolů HTTP, Samba, FTP, IMAP, POP a dalších.

90 %

času na vyřešení problému se využívá jen k tomu, aby se zjistilo, v čem přesně spočívá problém.

Zdroj: Zeus Kerravala, ZK Research

35 %

času na správu sítě stráví administrátoři reaktivním troubleshootingem.

Zdroj: Network Management Megatrends 2018, EMA

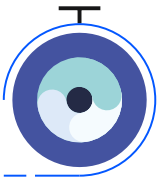
Výhody

Automatizovaná analytika

Autonomní zjišťování hlavních příčin provozních problémů vám ušetří řadu hodin i dnů.

Odborné znalosti

Zabudované odborné znalosti chybových kódů i jejich okolností vám usnadní práci – stejně jako návrhy vhodných řešení.



Zkrácení odstávek

Stačí jen pár vteřin a FPI zaznamená anomálie, vyšetří jejich původ a poradí vám s jejich řešením.

Jasné důkazy kdykoliv potřebujete

Systém nahrává pouze opravdu důležitá data, která uchovává pro pozdější analýzy a audity. Nehrozí vám tak žádný informační šum.

Méně potřebných nástrojů

Dostupnost, kapacita, troubleshooting, dodržování předpisů a forenzní analýza. S tím vším vám pomůže jeden nástroj – v jediném uživatelském rozhraní.

Inteligentní analytický rozhodovací strom

Flowmon Packet Investigator pracuje s PCAP soubory, které do něj importujete či automaticky nahrajete za pomocí Flowmon sondy podle nastavených pravidel nebo poté, co zaznamenáte anomálii či dostanete upozornění. Investigator pak v souborech pomocí analytického enginu vyhledá příčiny provozních problémů a navrhne jejich řešení.

Vyšetřování

FPI automaticky analyzuje PCAP soubory, a odhaluje tak odchylky od specifikací RFC z příslušných protokolů a jejich kombinací. Zároveň zaznamenává všechny chybové kódy a informace o dalších selháních. Mezi podporovanými protokoly najdete všechny běžné služby užívané ve firmách, jako je TCP, IP, HTTP, HTTPS, IMAP, SMTP, DNS, DHCP, SMB a řada dalších.

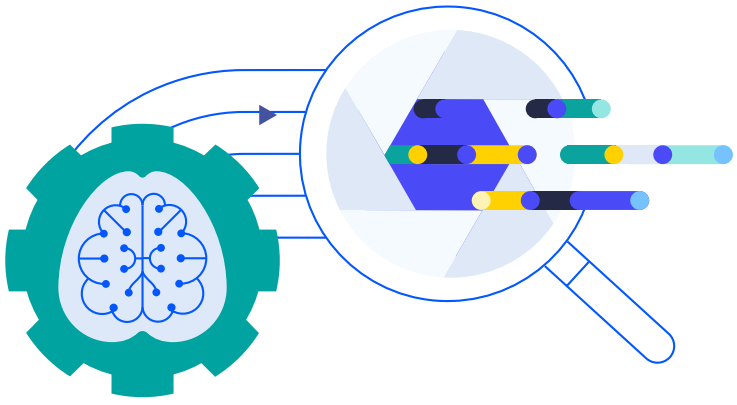
Zabudované odborné znalosti

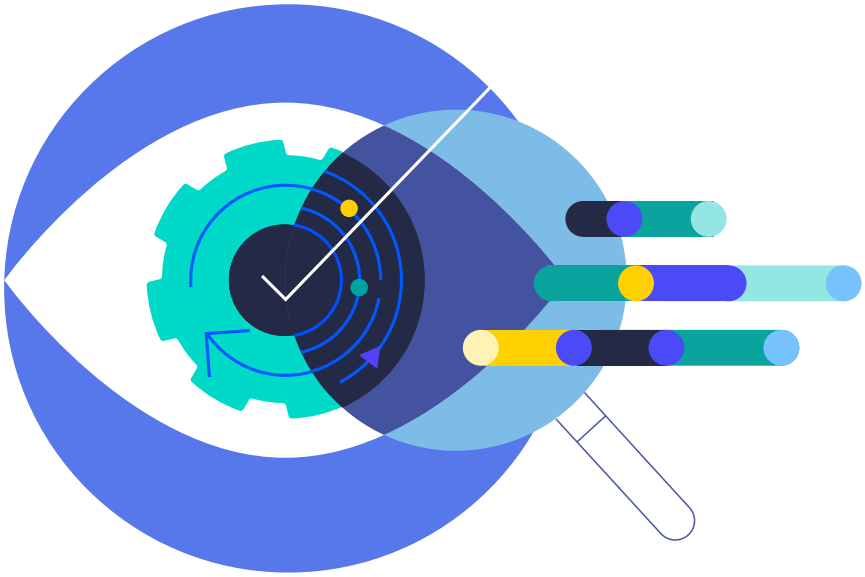
Flowmon Packet Investigator využívá zabudovanou databázi chybových kódů, které převádí do jasných sdělení. Jako například v případě, kdy se klient snaží se serverem sjednat šifrovací kanál, ale tento pokus selže kvůli odlišným certifikátům.

```
✓ SMTP: Zjištěno spojení (TCP@81.95.97.100:25-192.168.0.253:1357)
    ✓ SMTP: Server přijal klienta
        ✓ SMTP: Server je připravený
            ! SMTP: Nebylo nalezeno žádné ověření
                ✓ SMTP: Šifrování úspěšné
                    ✓ SSL: Spojení zahájeno
                        ⚠ SSL: Zjištěna závažná chyba
```

Okamžité výsledky

Výsledky vidíte na dashboardu, který zobrazuje počet událostí i jejich závažnost. Díky tomu se můžete v první řadě zaměřit na důležité chyby a ihned jednat. Zabudovanou databázi chybových kódů a vhodných řešení navíc stále rozšiřují naši experti, kteří tak do systému vkládají desítky let svých zkušeností.



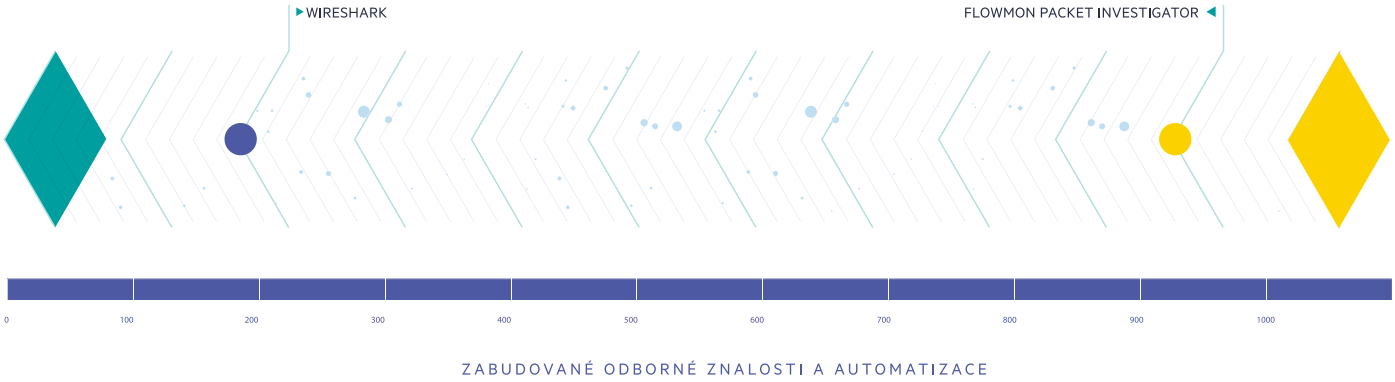


FPI vs. Wireshark

Wireshark je v současnosti nejpopulárnější analyzátor paketů. Funguje totiž jako open-source nástroj a má miliony uživatelů.

Na rozdíl od Wiresharku však FPI využívá sondy rozmístěné napříč celou sítí. Díky tomu můžete spustit zachytávání paketů i vzdáleně. Specializované síťové sondy přitom nabízejí rychlost až 100G. Ke zpracování paketů pak Investigator využívá analytický engine, který automaticky zobrazí veškeré nalezené problémy.

FPI je navíc uživatelsky přívětivější. Zejména pro méně zkušené síťové administrátory totiž může být práce s Wiresharkem složitá a časově náročná. Naopak FPI ji uživatelům usnadní tím, že jim sám poskytne odborné znalosti. A také zautomatizuje jejich práci.



Nahrávání

On-demand zachytávání paketů je účinný nástroj, který ukládá jen relevantní pakety – a to rychlostí až 100G. Nemusíte se tak bát, že bude zaznamenávat nepotřebné informace a zbytečně plýtvat zdroji.

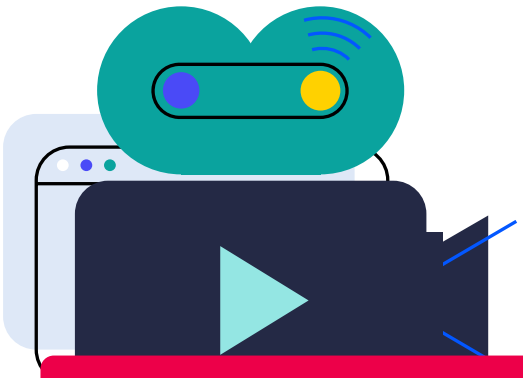
Navíc můžete využít řadu triggerů, které umožňují plánovat záchyty například podle MAC adresy, IP adresy, podsítě (CIDR), protokolu, portu, VLAN tagu nebo MPLS štítku. Samozřejmostí je i manuální a zcela automatické zachytávání paketů.

Automatické spouštění

Příklad: Flowmon ADS detekuje anomálii, která svědčí o narušení sítě, při němž se určité zařízení snaží získat přístup k doméně známé šířením malwaru. Automaticky proto pakety zachytí, a zajistí tak kompletní paketová data pro zevrubnou analýzu.

Cyklický buffer

Díky cyklickému bufferu zůstane sada paketů pro každý datový tok uložená na předem stanovenou dobu ve vyrovnávací paměti. Na vyžádání ji pak zaevidujete. Získáte tak méně náročnou alternativu k průběžnému zachytávání paketů a zároveň o žádné pakety nepřijdete.



Více informací najdete na www.flowmon.com

Worldwide Headquarters

Progress Software Corporation
15 Wayside Rd, Suite 400, Burlington, MA01803, USA
Tel: +1-800-477-6473

facebook.com/progresssw
twitter.com/progresssw
youtube.com/progresssw
linkedin.com/company/progress-software
progress_sw_

Progress