LIVEACTION – WIELE TWARZY WSPÓŁCZESNEGO MONITORINGU SIECI

Linus Brand

LiveAction

Sławomir Białas

NetFormers

Po co to wszystko ?

Pasywnie czy aktywnie?

Ruch syntetyczny

Kopia ruchu

W którym kierunku to idzie?

LiveAction

Wiele twarzy współczesnego monitoringu sieciowego

NETFORMERS

Po co to wszystko

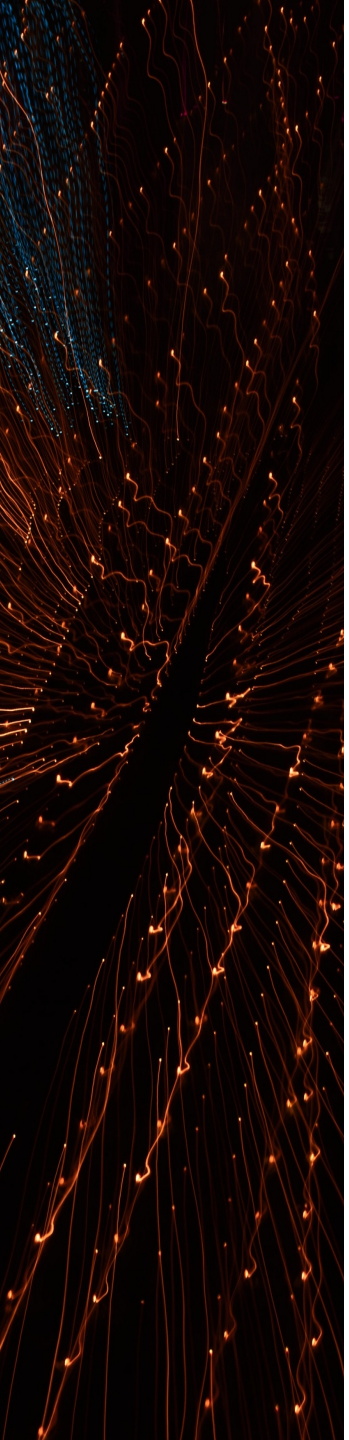
90 lat temu dwóch genialnych matematyków rozmawiało sobie o kompetencjach

***Matematykiem** jest, kto umie znajdować analogie między twierdzeniami, lepszym – kto widzi analogie między dowodami, jeszcze lepszym – kto dostrzega analogie między teoriami, a można wyobrazić sobie i takiego, co widzi analogie między analogiami.*

90 lat później skromny magister inżynier …
…sparafrazował powyższą myśl

Dobry inżynier potrafi dostrzegać fakty, inżynier wybitny – analogie między faktami, zaś inżynier genialny – analogie między analogiami.

NETFORMERS



Baza, narzędzia, intuicja

Oto kilka cech, które często definiują dobrego inżyniera:

- **Fachowa wiedza (baza):** Posiada solidną wiedzę techniczną związana z daną dziedziną inżynierii, jak również umiejętność jej praktycznego zastosowania;
- **Umiejętność analitycznego myślenia:** Potrafi dokładnie analizować problemy, rozkładać je na części składowe i identyfikować kluczowe kwestie;
- **Dokładność i precyzja:** Wykazuje się starannością w pracy oraz dbałością o szczegóły, co jest kluczowe dla zapewnienia bezpieczeństwa i skuteczności projektów inżynieryjnych;
- **Komunikatywność:** Potrafi klarownie komunikować się zarówno z członkami zespołu, jak i z klientami, aby zrozumieć ich potrzeby i przekazać swoje pomysły i rozwiązania;
- **Dążenie do ciągłego rozwoju (potrzeba narzędzi):** Jest otwarty na naukę i chętnie rozwija swoje umiejętności oraz wiedzę w zakresie inżynierii.

Dobry inżynier to osoba posiadająca solidną ***bazę wiedzy technicznej***, którą wykorzystuje do rozwiązywania problemów z wykorzystaniem ***dostępnych narzędzi analitycznych***.

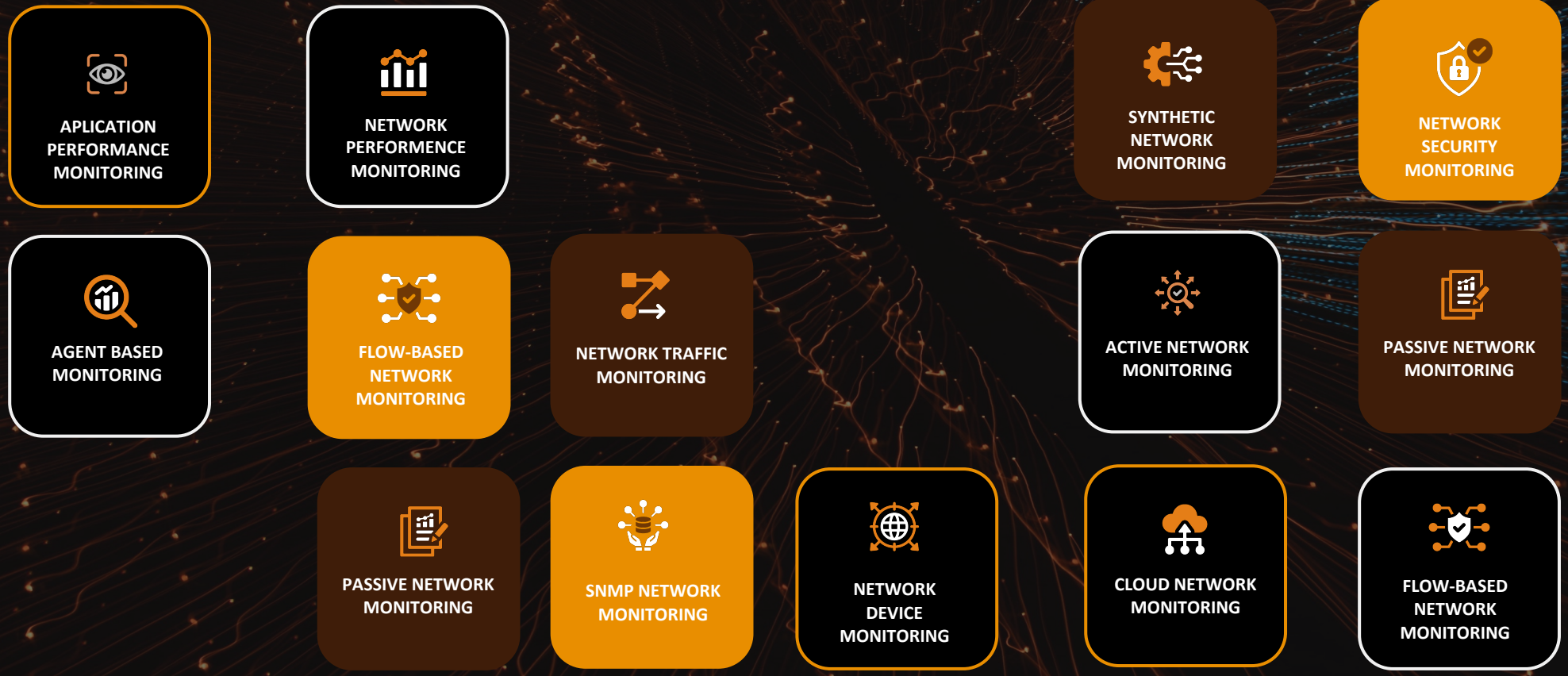
Oto kilka cech, które mogą definiować inżyniera wybitnego:

- **Innowacyjność (intuicja):** Tworzy lub współtworzy nowatorskie rozwiązania technologiczne lub procesy, które mają znaczący wpływ na daną dziedzinę inżynierii;
- **Wiedza i doświadczenie:** Posiada głęboką wiedzę teoretyczną oraz praktyczne doświadczenie w swojej dziedzinie inżynierii, co pozwala mu podejmować skomplikowane wyzwania z powodzeniem;
- **Osiągnięcia zawodowe:** Posiada bogatą historię osiągnięć zawodowych, bierze udział w nowych projektach, które prowadzą do wdrożeń nowoczesnych rozwiązań i są doceniane przez środowisko i szerzej społeczność inżynierską;
- **Współpraca i mentorowanie:** Aktywnie wspiera rozwój innych inżynierów poprzez mentorowanie, udział w szkoleniach lub dzielenie się wiedzą i doświadczeniem;

Inżynier wybitny jest doskonałym specjalistą w swojej dziedzinie, którego działania ***cechuje intuicja*** pozwalająca mu wyszukiwać rozwiązania, które inni oceniają jako innowacyjne.

NETFORMERS

Monitoring – różne twarze



NETFORMERS

Systemy monitorujące

Analiza ruchu	Rzeczywisty	Syntetyczny
System agentowy	APM (AppDynamics)	System aktywny (ThousendEyes)
System pasywny	NPM (LiveAction)	Jeszcze nie wymyślono

Rodzaj analizowanego ruchu

NETFORMERS

Systemy Aktywne

Aktywne monitorowanie sieci odnosi się do praktyki generowania i wysyłania określonych pakietów testowych w celu oceny i pomiaru wybranych parametrów sieciowych. Aktywne monitorowanie obejmuje proaktywne działania i celowe testowanie sieci.

Jako źródło danych wykorzystuje

- Sondy HW instalowanie w wybranych miejscach w sieci;
- Agentów SW instalowanych na zasobach HW/VM/Cloud;

Kluczowe cechy

- Proaktywne testowanie sieci – tetsy HTTP/HTTPs/DNS/VoIP, Traceroute/dostępność, działanie mechanizmów redundancji;
- Egzekwowanie polityk SLA;
- Ocena skalowalności, np. migracja do nowych usług czy aplikacji;

System APM

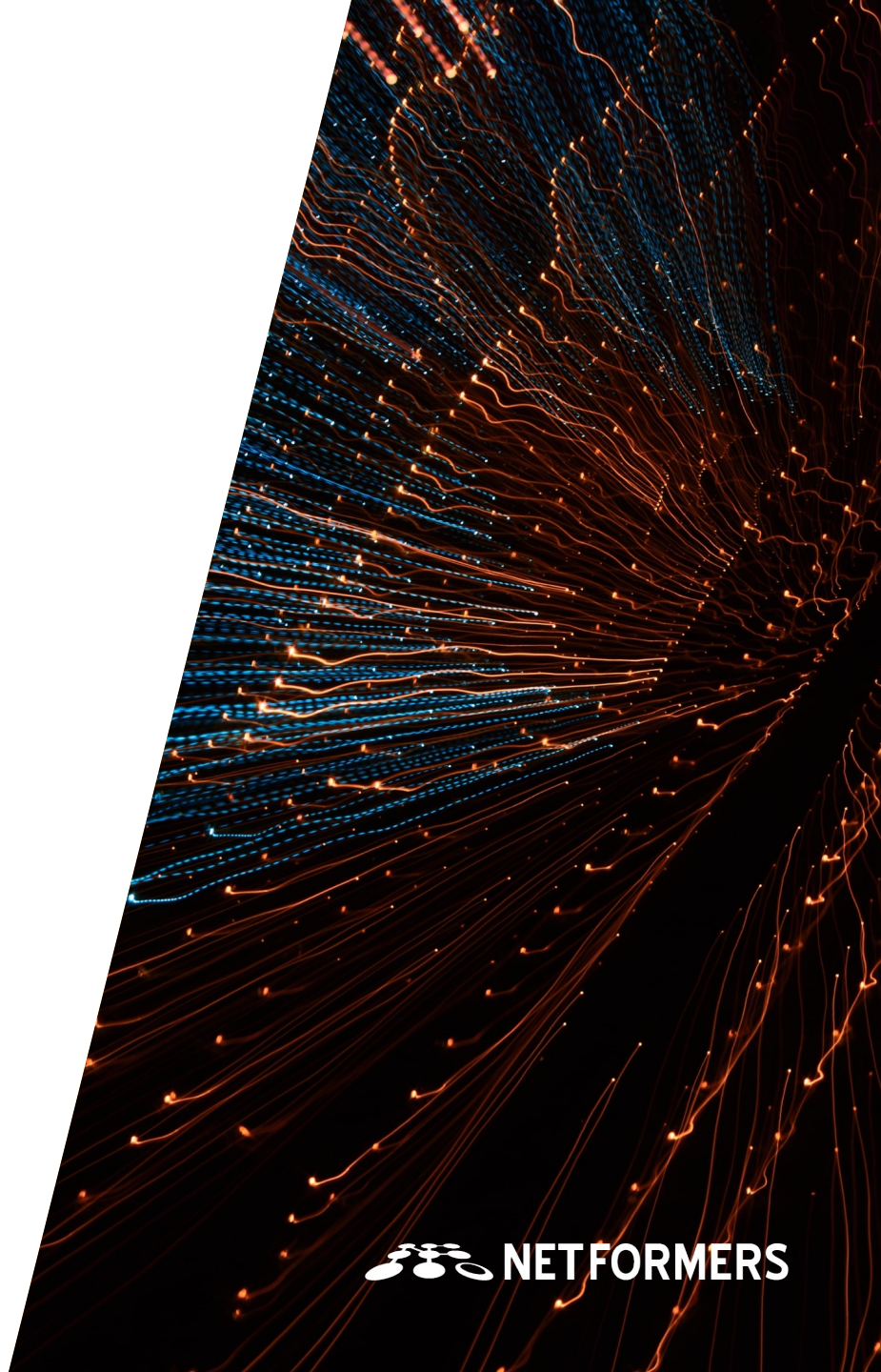
***Monitorowanie APM* to praktyka polegająca na zarządzaniu wydajnością i dostępnością aplikacji. Domeną systemu APM jest optymalizacja wydajności kodu, poszczególnych transakcji i zapytań np. HTTP/WEB.**

Jako źródło danych wykorzystuje

- Systemy agentowe instalowane na zasobach sieciowych, które zapewniają „obserwowalność” pełnego stosu – metryk, dzienników, transakcji;

Kluczowe cechy

- Monitorowanie doświadczeń cyfrowych, tzw. DEM – śledzenie interakcji użytkownika z aplikacją (czas ładowania strony, ścieżki kliknięć, wskaźniki zakończenia transakcji);
- Obserwowalność End-to-End (rozumienie zachowania transakcyjnego aplikacji i jego wpływu na wyniki biznesowe);
- Monitorowanie architektury aplikacji (mikroserwisy, kontenery, API) aby zrozumieć ich wpływ na działanie aplikacji;
- Śledzenie transakcji, dzienników, błędów jako element integrujący zadania pomiędzy DevOps



System NPM

***NPM* (Network Performance Monitoring) polega na analizowaniu pakietów sieciowych podczas ich przechodzenia przez sieć bez zakłócania czy modyfikowania ruchu. Dostarcza informacji na temat tego czy usługi sieciowe i aplikacje są dostarczane efektywnie do użytkowników za pomocą dostępnej infrastruktury sieciowej.**

Jako źródło danych wykorzystuje

- Protokół SNMP (1988r.) - zbieranie informacji o stanie „zdrowia” urządzeń sieciowych;
- Telemetrię, czyli protokoły przepływowe Netflow (1996r.), IPFIX, sflow, j-flow, cflow (wzorzec komunikacji sieciowej oparty o profil ruchu – sposób utylizacji łączy);
- Podsłuchiwanie pakietów (Sniffer 1986r.) wraz z analizą DPI – Deep Packet Inspection (dostarcza informacji o tym jak szybko pakiety są transferowane przez wybrane segmenty sieciowe);

Kluczowe cechy

- Monitorowanie i optymalizacja wydajności działania sieci IP (opóźnienia, utrata pakietów, jitter, retransmisje);
- Zarządzanie przepustowością (jak są wykorzystywane zasoby, kto i czym utylizuje łącza);
- Egzekwowanie polityk, zarządzanie jakością usług (QoS, SD-WAN);
- Analiza kryminalistyczna i rozwiązywanie problemów sieciowych (pełna kopia ruchu sieciowego);

NDR (transformacja NPM)

***NDR (Network Detection & Response)* monitoring, który używa innych mechanizmów niż wyłącznie sygnatury do wykrywania podejrzanego ruchu w sieciach korporacyjnych, a właściwie wyposażony jest zdolny do podjęcia działań zapobiegawczych.**

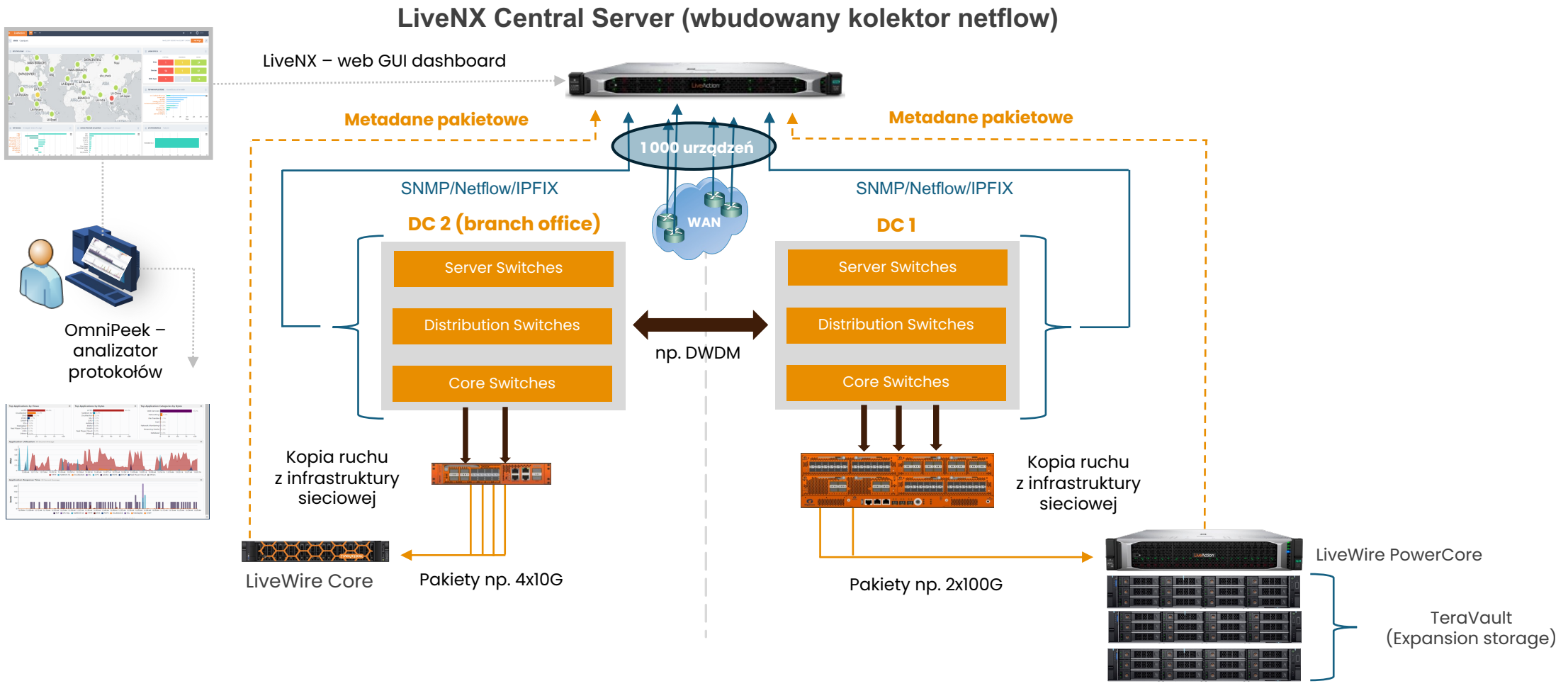
Jako źródło danych wykorzystuje

- Netflow/IPFIX (wzbogacony o parametry wydajnościowe przesyłanych pakietów);
- Podsłuchiwanie pakietów tzw. DPD – Deep Packet Dynamics (analiza dynamiki przesyłanych pakietów w zaszyfrowanej treści, tzw. analiza ETA);

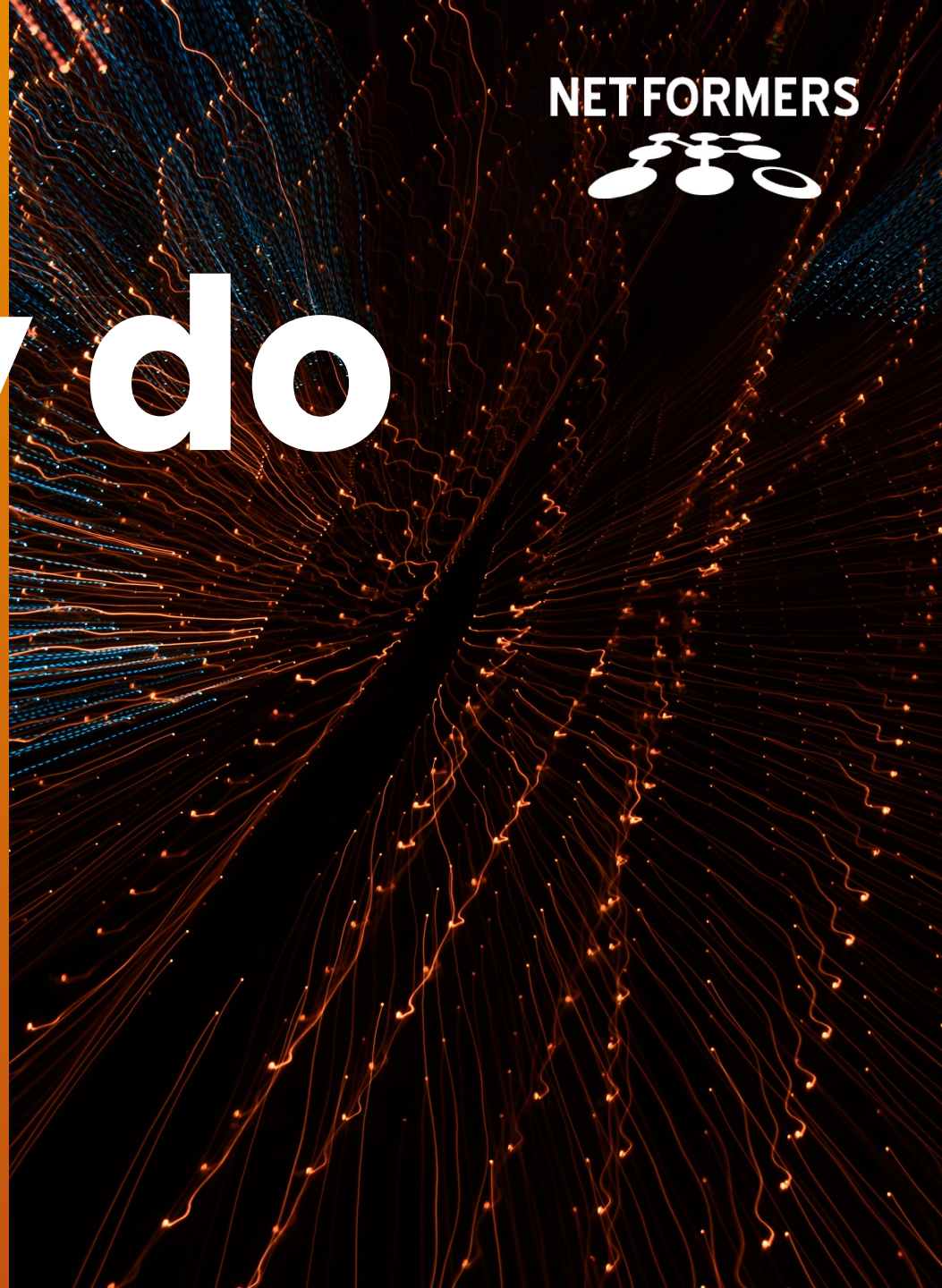
Kluczowe cechy

- Używa tych samych źródeł danych co monitoring NPM, przez co stanowi naturalne rozwinięcie systemów NPM i łatwo integruje działy SecOps;
- Jest niezauważalny dla atakującego, przez to trudno go wyłączyć/oszukać;
- Nie wymaga dekrypcji SSL/TLS;

Architektura LiveAction



Przejdźmy do praktyki



Zaproszenie

Dedykowane warsztaty z technologii

LiveAction

w siedzibie NetFormers
Mińska 75, Warszawa

w dniu 23.05.2024 r.