NETSCOUT™

Widoczność bez barier

Potęga ciągłej widoczności wydajności sieci, dostępności aplikacji oraz usług i zagrożeń bezpieczeństwa w każdej sieci, w każdym data center, chmurze, 5G i innych

NETSCOUT

Spis treści

bako tech®

nGeniusONE

Platforma nGeniusONE zapewnia niezrównaną widoczność usług biznesowych opartych na IP wraz z kontekstowymi przepływami pracy w celu przyspieszenia rozwiązywania problemów w sposób, który jest zarówno łatwy w użyciu dla specjalisty poziomu 1, jak i wydajny dla eksperta. Zamiast patrzeć na poszczególne elementy w sposób wyizolowany, nGeniusONE zapewnia ogólny wgląd w wydajność komponentów związanych z dostarczaniem usług.

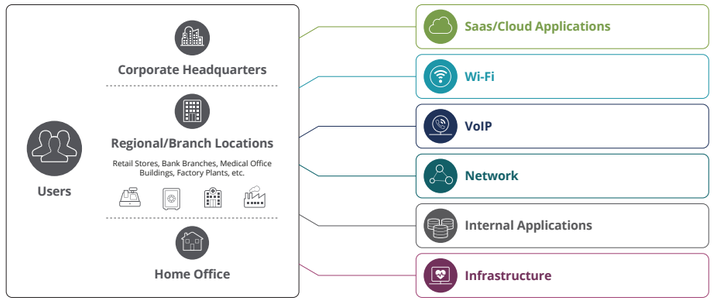
Takie podejście odsłania podstawowe zależności między usługami, które pomagają działom operacyjnym IT efektywnie zarządzać problemami związanymi ze stabilnością, dostępnością i doświadczeniem użytkowników końcowych, jednocześnie poprawiając zdolność do proaktywnego identyfikowania i usuwania pierwotnych przyczyn problemów z wydajnością.

Możliwości te pozwalają działom operacyjnym IT zapewnić ciągłość biznesową wspieranym przez nie organizacjom, w tym:

• Monitorowanie technologii UC&C niezbędne do zapewnienia wydajności platform konferencyjnych wielu dostawców (np. (np. Cisco Webex, Microsoft Teams, Zoom, Google), a także rozwiązań obejmujących centra obsługi klienta, opcje UCaaS (Unified Communications-as-a-Service), lokalne usługi głosowe i wideo oraz wdrożenia trunkingowe z wykorzystaniem protokołu Session Initiation Protocol.

• Zarządzanie wydajnością aplikacji w ramach operacji hybrydowych centrów danych i usług w wielu chmurach, w tym widoki przed, w trakcie i po, które zapewniają, że migracje aplikacji nie pogorszyły dostępu lub wydajności.

• Zarządzanie wydajnością sieci, w tym sprawdzanie wydajności pasma internetowego, przepustowości sieci VPN oraz poziomów wydajności chmury hybrydowej/SaaS.



Rysunek 1.
Analityka nGeniusONE i inteligentna widoczność NETSCOUT umożliwiają NetOps, SecOps, i działom IT wgląd we wszystkie operacje niezależnie od miejsca pracy pracowników.

Kluczowe cechy

1. Analiza wydajności

Rzut oka na ogólną wydajność usług wymaganą do utrzymania działalności firmy we wszystkich sieciach i na wszystkich platformach.

2. Mapowanie zależności usług

Zmniejszenie ryzyka migracji poprzez wizualizację "ukrytych" zależności klient/serwer oraz wydajności przesyłania komunikatów.

3. Analiza aplikacji

Monitory specyficzne dla firm i protokołów, z metrykami umożliwiającymi rozwiązywanie problemów i poprawę komfortu pracy użytkowników końcowych.

4. Analiza sesji

Analiza sesji i pakietów w celu uzyskania szczegółowych informacji - wszystko bez użycia narzędzi innych firm.

5. Analiza wydajności

Działający w czasie rzeczywistym, konfigurowalny Service Dashboard zapewnia pojedynczy widok środowisk usług biznesowych typu end-to-end.

Korzyści

1. Zapewnienie jakości doświadczeń użytkownika

Wgląd w dowolną usługę, w dowolnie złożone środowisko chmury hybrydowej, w dowolnym czasie.

2. Sukces cyfrowej transformacji

Monitorowanie usług "przed, w trakcie i po" wdrożeniu w celu zapewnienia wysokiej jakości obsługi użytkowników.

3. Lepsze rozwiązywanie problemów IT

Dzięki kompleksowemu wglądowi w krawędzie usług i monitorowaniu doświadczeń użytkowników końcowych można poprawić MTTK i zmniejszyć MTTR.

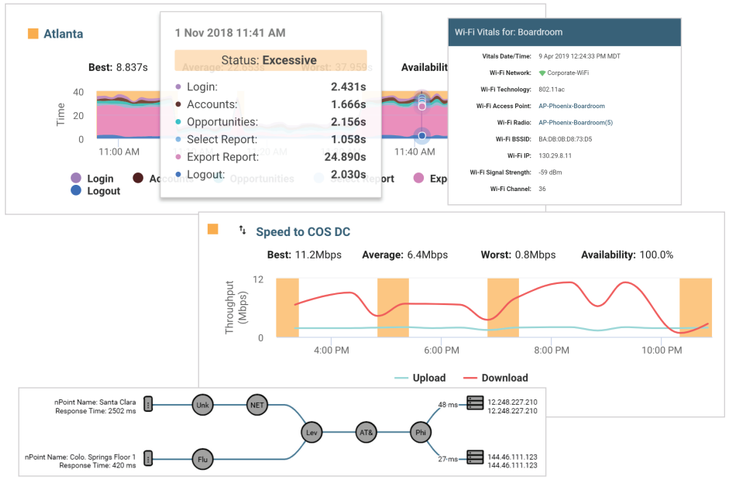
4. Wsparcie dla światowych wymagań biznesowych

Skalowalna, gotowa do globalnego wdrożenia architektura dla mieszanych centrów danych, która rozwija się wraz z Twoimi potrzebami.

nGeniusPULSE

Jako część portfolio nGenius Service Assurance zapewniającego widoczność sieci end-to-end, nGenius®PULSE jest zawsze dostępnym i zautomatyzowanym rozwiązaniem dla środowisk chmurowych, hybrydowych i wirtualnych, które pomaga klientom zarządzać doświadczeniem użytkownika i izolować problemy pomiędzy posiadanymi przez nich aktywami i wieloma dostawcami usług, z których korzystają. nGeniusPULSE koreluje również dostarczanie usług ze stanem infrastruktury wspierającej, zapewniając, że najbardziej krytyczne elementy ekosystemu biznesowego są połączone i działają.

Dzięki automatycznemu i ciągłemu aktywnemu (syntetycznemu) testowaniu dostępności i wydajności usług biznesowych, nGeniusPULSE zapewnia całodobowe monitorowanie krytycznych aplikacji i usług z dowolnego miejsca w przedsiębiorstwie; w centrum danych, w odległych oddziałach, wśród pracowników zdalnych, dla urządzeń IoT i nie tylko.



Rysunek 2.
nGeniusPULSE dostarcza użytecznych informacji do zarządzania aplikacjami SaaS

Kluczowe cechy

1. Status działania w mgnieniu oka

Pulpity nawigacyjne z możliwością wgłębiania się w szczegóły wyświetlają wyniki ciągłych, zautomatyzowanych testów, aby pokazać ich zakres i wpływ.

2. Kontekstowe przepływy pracy pozwalające zrozumieć sytuację wyjściową i wyodrębnienie przyczyn problemów

Zmniejszanie średniego czasu do uzyskania wiedzy o usterce (MTTK) dzięki alertom o odchyleniach od normalnej wydajności w nGeniusPULSE i wskazywanie przyczyny w nGeniusONE w celu zmniejszenia średniego czasu do rozwiązania problemu (MTTR).

3. Monitorowanie za pomocą połączeń przewodowych i Wi-Fi

Porównywanie wydajności połączeń przewodowych i Wi-Fi w celu wyodrębnienia czy problem dotyczy Wi-Fi.

4. Monitorowanie wydajności infrastruktury

Monitoruj stan serwerów, routerów, przełączników, interfejsów, VMware i infrastruktury Wi-Fi. Przeglądaj metryki stanu, takie jak wykorzystanie CPU, pamięci, wykorzystanie dysków, wykorzystanie kanałów, błędy, itp.

Korzyści

1. Lepsze doświadczenia użytkowników końcowych

Możliwość sprawdzenia dostępności i wydajności aplikacji oraz sieci w dowolnym miejscu i czasie z perspektywy użytkownika.

2. Przechwytywanie inteligentnych danych z miejsc pracy w domu/zdalnie

Używaj testów syntetycznych, aby uzyskać inteligentne dane do dogłębnej analizy z nGeniusePULSE do nGeniusONE.

3. Szybko monitoruj stan aplikacji i sieci

Przeglądaj status Re-Yellow-Green na tablicy rozdzielczej, zagłębiaj się w wyniki testów i wydajność w czasie oraz przeglądaj wykresy i analizę trendów.

4. Skoreluj dostarczanie usług z kondycją infrastruktury

Weryfikacja kondycji infrastruktury wspierającej sieć i krytyczne dla biznesu aplikacje.

InfiniStreamNG i vSTREAM

Inteligentne przechwytywanie pakietów, analiza w czasie rzeczywistym, analizy historyczne sieci oraz zarządzanie wydajnością aplikacji. **nGenius InfiniStream** jest dedykowanym urządzeniem o dużej wydajności głębokiej inspekcji pakietów, które umożliwia tworzenie analiz ruchu sieciowego w czasie rzeczywistym oraz przechowuje natywne pakiety sieciowe po to, by wspierać szerokie możliwości śledzenia i analizowania informacji kryminalistycznych z perspektywy historycznej.

nGenius InfiniStream zapewnia spójność funkcjonalną całej rodziny urządzeń, dzięki odpowiedniemu doborowi interfejsów do pokrycia całego środowiska dostarczania usług - od data center, przez rdzeń do krawędzi sieci i jej wydzielonych elementów.

InfiniStreamNG® (ISNG) wykorzystuje opatentowaną technologię **Adaptive Service Intelligence® (ASI)** do generowania NETSCOUT "Smart Data" wymaganych do ciągłej i jednolitej widoczności w dzisiejszych środowiskach sieciowych na dużą skalę. Inteligentna analityka platformy NETSCOUT nGeniusONE® Service Assurance wykorzystuje te inteligentne dane, aby dostarczyć widoki, alerty i raporty na temat kluczowych wskaźników wydajności, sieci i szczegółów błędów aplikacji, specjalistycznych monitorów usług, zapisów sesji i dekodowania pakietów.

Dzięki rozwiązaniu NETSCOUT, zespoły informatyczne (IT) oraz dostawcy usług posiadają technologię niezbędną do zapewnienia użytkownikom najwyższej jakości usług, jednocześnie zapewniając pomyślną realizację celów biznesowych związanych z transformacją cyfrową, w tym między innymi migracji centrów danych i chmur obliczeniowych, wdrażania zunifikowanej komunikacji (UC) oraz inicjatyw związanych z analizą bezpieczeństwa.

Dzięki inteligentnym danym generowanym przez ASI, które służą również jako wspólne źródło danych dla wirtualnych urządzeń vSTREAM firmy NETSCOUT dla środowisk multi-cloud (np. Amazon Web Services, Google Cloud, Microsoft Azure, Oracle Cloud Infrastructure) i wirtualnych (np. VMware NSX-V i NSX-T), oprogramowanie ISNG i urządzenia sprzętowe mogą być wdrażane w tandemie z vSTREAM.

Wirtualne urządzenie NETSCOUT® vSTREAM uzupełnia istniejące oprzyrządowanie Adaptive Service Intelligence® (ASI) w celu zapewnienia tej samej inteligentnej widoczności danych w chmurze i zwirtualizowanych infrastrukturach, która jest już możliwa w środowiskach fizycznych. Zapewnia to doskonałą analizę typu end-to-end, dodając monitorowanie ruchu w kierunku wschód-zachód, aby pomóc w identyfikacji problemów z wydajnością i bezpieczeństwem w każdym miejscu, w którym one występują.

Zalety ISNG

1. Potęga inteligentnych danych

Pochodzące z ISNG "inteligentne dane" są wykorzystywane w widokach, alarmach i raportach nGeniusONE, w tym w kluczowych wskaźnikach wydajności, szczegółach błędów sieci i aplikacji, monitorach usług specjalistycznych, zapisach sesji i dekodowaniu pakietów.

2. Zoptymalizowane dla ISNG

Sprzęt jest zoptymalizowany pod kątem wydajności i funkcjonalności oprogramowania ISNG. Urządzenia sprzętowe i certyfikowane urządzenia programowe wykorzystują specjalnie skonstruowany sprzęt, który jest zaprojektowany w celu zapewnienia najlepszej wydajności, najwyższej niezawodności i najbardziej kompletnej funkcjonalności z oprogramowaniem ISNG firmy NETSCOUT.

3. Zwiększone bezpieczeństwo i niezawodność

Oprogramowanie i sprzęt ISNG są zaprojektowane dla maksymalnej dostępności i niezawodności.

4. Doskonała cena/wydajność z elastycznością

Trzy modele wdrożeń zapewniają niezrównaną elastyczność w celu osiągnięcia optymalnej wydajności i całkowitego kosztu posiadania (TCO).

Korzyści

1. Swoboda wyboru

Interfejsy i rozszerzone opcje pamięci masowej skutecznie spełniają wymagania dotyczące wyjątkowej szybkości sieci, pożądanej wydajności przetwarzania i pojemności.

2. Doskonałe dopasowanie

Modele ISNG sprawdzają się w każdym środowisku, począwszy od brzegu sieci, małych zdalnych obiektów, biur satelitarnych i miejsc odzyskiwania danych po awarii, aż po rdzeń centrum danych.

3. Rozszerzona wartość

Funkcja Omnis Smart Edge Monitoring obsługuje inteligentne dane pochodzące zarówno z pasywnego monitorowania pakietów, jak i testów syntetycznych z nPoints przy użyciu Omnis Cloud Adaptor.

PFS Packet Broker

Strategiczna widoczność pakietów w połączonym świecie

Potrzebujesz ujednoliconego widoku, który pozwala wielu grupom IT na dostęp do przepływów pakietów bez powodowania zakłóceń. Z produktami NETSCOUT, nie ma żadnych zakłóceń. Dlatego potrzebujesz możliwości tworzenia dynamicznych połączeń z dowolnego punktu TAP w sieci do dowolnego narzędzia.

Systemy zabezpieczeń online i wykrywania zagrożeń

Wraz ze wzrostem natężenia ruchu w sieci, rośnie również gotowość do reagowania na pojawiające się problemy. Przełącznik przepływu pakietów NETSCOUT nGenius (PFS) i rodzina TAPs umożliwia wielu grupom IT agregację, replikację i zarządzanie przepływem ruchu w sieci, czy to w celu monitorowania wydajności aplikacji, ujednoliconej komunikacji (UC), czy bezpieczeństwa. Zarządzanie ruchem i funkcje bezpieczeństwa zapewniają wolne od ryzyka wdrożenie systemów bezpieczeństwa i wykrywania zagrożeń.

Eliminacja zakłóceń w ruchu lub transakcjach protokołów

Łącząc wiodący w branży przełącznik przepływu pakietów NETSCOUT nGenius, pasywny TAP i naszą wysoce elastyczną platformę zarządzania nGenius PFS, upraszczamy pozyskiwanie i dystrybucję ruchu dla różnych operacji ruchu sieciowego, w tym zarządzania wydajnością, zarządzania dostarczaniem usług i monitorowania bezpieczeństwa. Nasza solidna rodzina TAP zapewnia urządzeniom InfiniStream zasilanym przez technologię Adaptive Service Intelligence (ASI) i przełącznikom przepływu pakietów nGenius pełny dostęp do ruchu sieciowego, pozostając jednocześnie przezroczystą dla infrastruktury sieciowej i eliminując zakłócenia ruchu lub transakcji protokołów.

Strategiczna widoczność pakietów

Architektura przełącznika przepływu pakietów umożliwia strategiczną widoczność pakietów, która skaluje się i działa dynamicznie, umożliwiając wszechobecną widoczność poprzez wykorzystanie urządzeń InfiniStream firmy NETSCOUT, części platformy nGeniusONE Service Assurance, lub systemów bezpieczeństwa, niezależnie od modyfikacji infrastruktury lub zmian w źródle ruchu sieciowego. Dzięki przełącznikom przepływu pakietów NETSCOUT, narzędzia do zapewnienia i monitorowania usług w przedsiębiorstwie mogą być fizycznie wszędzie i logicznie wszędzie.

Kluczowe cechy

- Urządzenia o stałej konfiguracji, zajmujące 1, 2 lub 4RU (Rackmount Unit), zajmujące mało miejsca
- Przepustowość od 720 Gb/s do 12800 Gb/s dzięki nieblokujące się przełączanie łączy
- Porty 1GbE, 10GbE, 25GbE, 40GbE i opcje portów 100GbE
- Funkcje brokera pakietów sieciowych w tym konwersja szybkości, agregacja, replikację, filtrowanie, równoważenie obciążenia i oznaczanie portów źródłowych
- Usuwanie i de-enkapsulacja protokołów (np. VLAN, VN-tag, VXLAN)
- IP tunelling (np. ERSPAN)
- Inteligentne meshed stacking / interconnect (pfsMesh)
- Elastyczne, definiowane politykami wyzwalacze do obsługi zdarzeń, definiowane politykami wyzwalacze dla obsługi zdarzeń i scenariuszy wysokiej dostępności
- Zarządzanie poprzez wiersz poleceń, NETCONF, i graficzne interfejsy użytkownika dla lokalnego i zdalnego zdalnego dostępu
- Zero Touch Provisioning (ZTP) dla łatwego uruchomienie systemu
- Oparte na oprogramowaniu i zasilane przez NETSCOUT® Packet Flow Operating System (PFOS) Packet Flow Operating System (PFOS)

Arbor Edge Defense

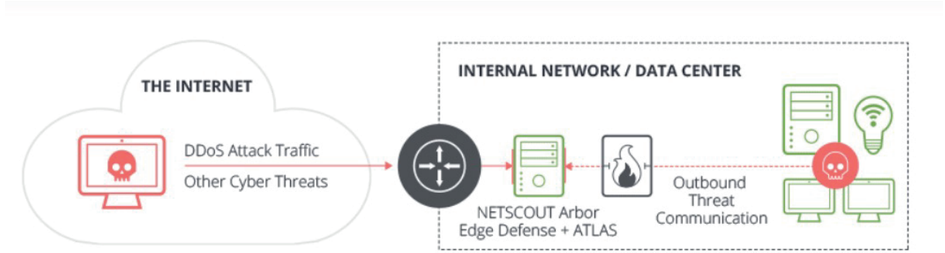
Pierwsza i ostatnia linia inteligentnej, zautomatyzowanej obrony obwodowej

Arbor Edge Defense (AED) jest urządzeniem zabezpieczającym inline, które jest instalowane na granicy sieci (tj. pomiędzy routerem internetowym a firewallem).

Unikalna pozycja AED na brzegu sieci, jego bezstanowy silnik przetwarzania pakietów oraz ciągłe, oparte na reputacji informacje o zagrożeniach otrzymywane z NETSCOUT's ATLAS Threat Intelligence feed pozwalają mu automatycznie wykrywać i zatrzymywać zarówno przychodzące zagrożenia jak i komunikację wychodzącą z wewnętrznych, skompromitowanych hostów - zasadniczo działając jako pierwsza i ostatnia linia obrony dla organizacji.

Obrona na styku sieci

Wdrażana pomiędzy brzegowym firewall a routerem i wykorzystująca wysoce skalowalną technologię bezstanowego przetwarzania pakietów, Arbor Edge Defense działa jako punkt egzekwowania danych wywiadowczych o zagrożeniach sieciowych, gdzie blokuje masowo przychodzące zagrożenia cybernetyczne (np. ataki DDoS, IOC) oraz wychodzącą złośliwą komunikację - zasadniczo działając jako pierwsza i ostatnia linia obrony obwodowej dla organizacji.



Rysunek 3.

Korzyści wynikające z Arbor Edge Defense

1. Pierwsza linia obrony

AED zatrzymuje wszystkie rodzaje przychodzących ataków DDoS (np. wolumetryczne, wyczerpanie stanu TCP, warstwa aplikacji), aby chronić dostępność sieci, usług i urządzeń brzegowych organizacji (np. NGFW). W pełni zintegrowany z Arbor Cloud (globalną, opartą na chmurze usługą ochrony przed DDoS o przepustowości ponad 11 Tbps), AED jest samodzielnym komponentem wiodącego w branży, hybrydowego rozwiązania NETSCOUT do ochrony przed DDoS.

2. Ostatnia linia obrony

Uzbrojony w potencjalnie miliony IOC opartych na reputacji i innych informacji o zagrożeniach z NETSCOUT ATLAS lub innych firm (poprzez STIX/TAXII), AED może zatrzymać komunikację wychodzącą z zagrożonych urządzeń wewnętrznych Command & Control; aby pomóc zatrzymać rozprzestrzenianie się złośliwego oprogramowania lub napastników w organizacji i uniknąć naruszenia danych.

3. Integracja

Zdolność AED do działania jako pierwsza i ostatnia linia obrony, wykorzystanie REST API, wsparcie dla standardów takich jak STIX/TAXII, SYSLOG (CEF, LEEF) oraz dodatkowy kontekst zapewniany przez ATLAS pozwalają na integrację AED z istniejącym w organizacji systemem zabezpieczeń i procesami.

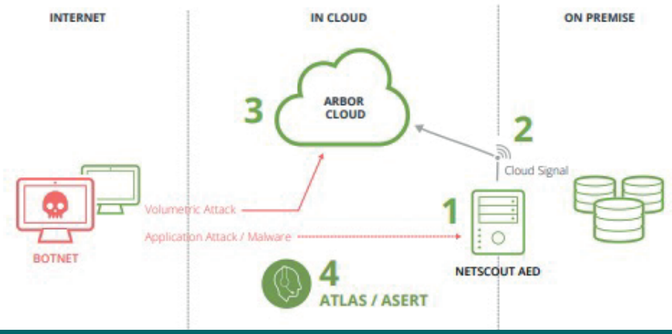
AED zapewnia najlepszą w swojej klasie i kompleksową ochronę przed atakami DDoS.

1. AED może automatycznie wykrywać i zatrzymywać przychodzące ataki w warstwie aplikacji, wyczerpanie stanu TCP (które mogą spowodować awarię firewalli) oraz ataki DDoS o wielkości nawet 40 Gb/s.

2. W przypadku większego ataku DDoS, AED Cloud Signaling automatycznie przekierowuje ruch do Arbor Cloud lub MSSP. Arbor Cloud lub opartego na chmurze centrum łagodzenia ataków DDoS firmy MSSP.

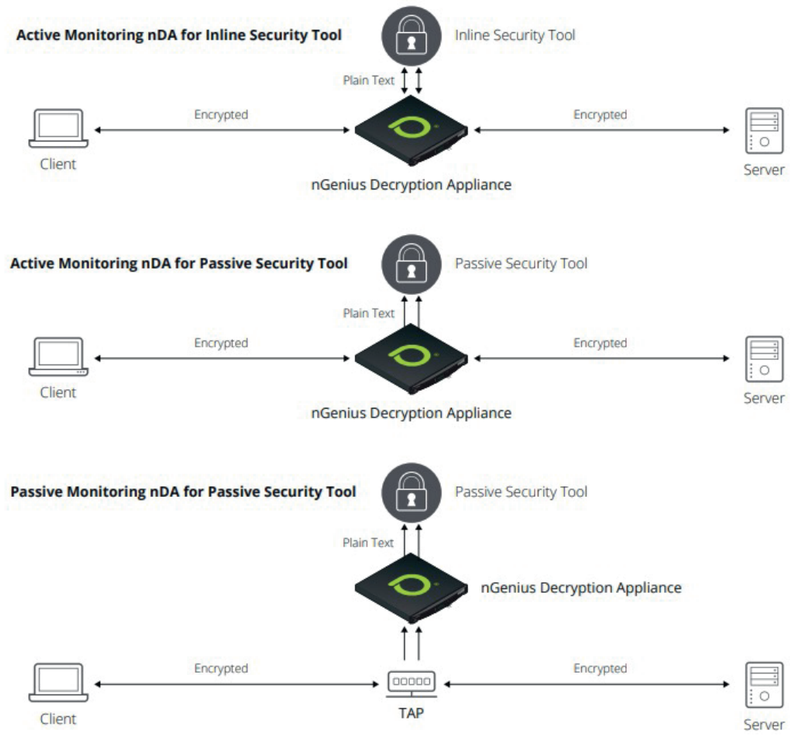
3. Arbor Cloud zapewnia ochronę przed największymi atakami DDoS poprzez 14 światowych centrów zapewniających ponad 11 Tbps zdolności łagodzenia ataków.

4. AED jest na bieżąco z najnowszymi zagrożeniami DDoS dzięki usłudze ATLAS Threat Intelligence Feed.



nGenius Decryption Appliance

Urządzenie nGenius Decryption Appliance (nDA) umożliwia inspekcję ruchu szyfrowanego SSL/TLS, nie naruszając przy tym wykorzystania SSL/TLS ani nie zmniejszając wydajności. Jest ono wdrażane jako przezroczyste urządzenie inline bump-in-the-wire (BITW), co umożliwia jego stosowanie w środowiskach L2 lub L3 bez konieczności rearchitektury sieci lub konfigurowania urządzeń klienckich do jawnego wysyłania ruchu do serwerów proxy. W tym trybie, nDA przekazuje zdeszyfrowany ruch do pasywnych narzędzi bezpieczeństwa i zapewnienia usług. Alternatywnie, nDA może być wdrożone jako pasywne urządzenie out of band do deszyfrowania i przekazywania ruchu do pasywnie podłączonych narzędzi zapewniających i zabezpieczających usługi.



Rysunek 5.
nGenius Decryption Appliance wdrożony z pasywnymi i aktywnymi narzędziami bezpieczeństwa

Omnis IDS

Ulepszona użyteczność, widoczność i analiza IDS

NETSCOUT zaprojektował Omnis™ IDS z bogatym zestawem funkcji, które radykalnie poprawiają użyteczność IDS, w tym intuicyjny interfejs użytkownika, analizę kontekstową, metryki stanu czujników oraz zautomatyzowany eksport danych do innych platform bezpieczeństwa. System Omnis IDS skaluje się od niewielkich instalacji do największych i najbardziej złożonych środowisk obliczeniowych. Oferuje szeroki i spójny zakres dzięki wykorzystaniu danych o pakietach sieciowych w celu zapewnienia rzeczywistego, kontekstowego wglądu na poziomie aplikacji we wszystkich infrastrukturach.

Rozwiązanie Omnis IDS zapewnia monitorowanie i wykrywanie zagrożeń dla znanych zagrożeń i ataków cyberbezpieczeństwa, w tym:

- złośliwe oprogramowanie
- oprogramowanie ransomware
- trojany sieciowe
- ataki typu „Brute-force”
- ruchy boczne
- eskalacja przywilejów
- ataki typu „command & control”
- naruszenia prywatności w firmach

Kluczowe cechy

1. Oprzyrządowanie sieciowe

Omnis™ IDS Sensor zapewnia wszechstronny, skalowalny wgląd w pakiety sieciowe w całym środowisku. Omnis™ IDS Sensor wykorzystuje technologię Suricata i obsługuje zestawy reguł open-source, komercyjne, prywatne i niestandardowe, zapewniając wysoką wydajność wykrywania zagrożeń.

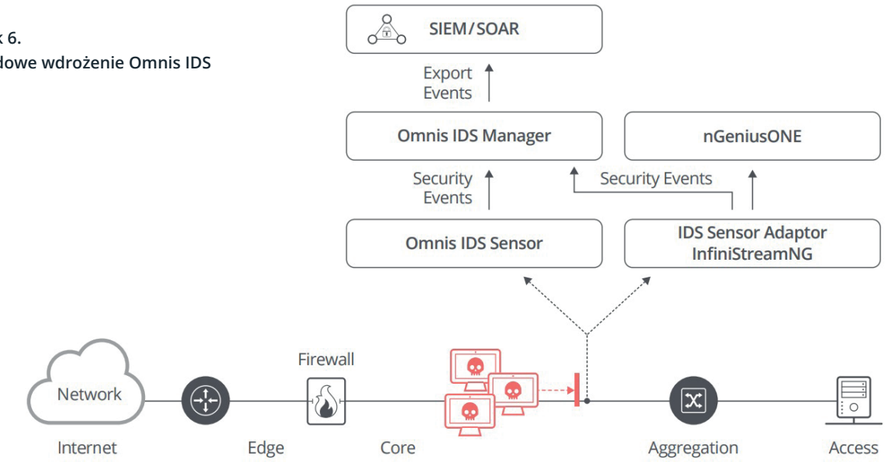
2. Scentralizowana analiza i wizualizacja

Omnis™ IDS Manager zapewnia potężną analitykę i scentralizowane zarządzanie w celu dalszej analizy i wyzwalania alarmów poprzez wykorzystanie zdarzeń i alarmów związanych z zagrożeniami bezpieczeństwa z czujników Omnis™ IDS.

3. Płynna integracja

System Omnis™ IDS wykorzystuje otwarte standardy, interfejsy API oraz intuicyjne przepływy pracy w celu łatwej integracji z istniejącymi systemami i procesami zabezpieczeń. System można skonfigurować tak, aby przekazywał zdarzenia i alarmy związane z zagrożeniami bezpieczeństwa do systemów SIEM innych firm, w tym Splunk, w celu skonsolidowanego zarządzania zdarzeniami bezpieczeństwa.

Rysunek 6.
Przykładowe wdrożenie Omnis IDS

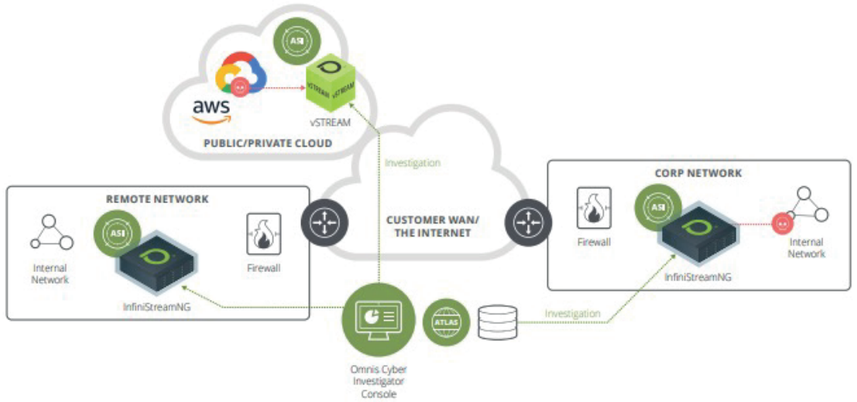


Omnis Cyber Investigator

Wykrywanie zagrożeń sieciowych, wykrywanie ryzyka i prowadzenie dochodzeń.

Omnis™ Cyber Investigator (OCI) to rozwiązanie do badania zagrożeń sieciowych i ryzyka, które pomaga zmniejszyć wpływ cyberzagrożeń na działalność firmy. Dzięki kompleksowej widoczności zabezpieczeń oraz globalnej informacji o zagrożeniach dostarczanej przez NETSCOUT, Omnis™ Cyber Investigator umożliwia szybkie i efektywne wykrywanie, weryfikację, badanie i reagowanie na zagrożenia cybernetyczne, zarówno w sieci jak i w chmurze. Organizacje odniosą korzyści z posiadania tego efektywnego kosztowo i wysoce skalowalnego systemu analizy zagrożeń cybernetycznych, który może również łatwo zintegrować się z popularnymi platformami SIEM używanymi przez wiele korporacji.

Podejście Omnis Cyber Investigator oparte na chmurze pomaga firmom w zarządzaniu zagrożeniami w coraz bardziej złożonych infrastrukturach cyfrowych, które charakteryzują się migracją aplikacji do chmur obliczeniowych, takich jak Amazon AWS. Dzięki połączeniu bezagentowego dostępu do pakietów Omnis Cyber Investigator z wirtualnym oprzyrządowaniem AWS, użytkownicy korporacyjni mogą bezproblemowo rozszerzyć swoją widoczność cybernetyczną na AWS. Platforma integruje się z AWS Security Hub i obsługuje Amazon Virtual Private Cloud (VPC), mirroring ruchu, VPC ingress routing oraz Gateway Load Balancer (GWLB).



Rysunek 7.
Poglądowe wdrożenie systemu Omnis Cyber Investigator

NETSCOUT™

Skontaktuj się z nami:

www.bakotech.pl
netscout@bakotech.pl
+48 12 340 90 30

bako tech®

@bakotechpl
@bakotechpl
Bakotech Poland&CEE