ADDNET

novicom

Integracja DDI/NAC klasyfikuje ADDNET jako narzędzie administracji i ochrony bezpieczeństwa sieci, zapewniając organizacjom pełną jej widoczność oraz oferując wysoką wydajność w procesie zarządzania adresacją IP i zaawansowaną kontrolę dostępu do sieci.

ADDNET jest wyjątkowym instrumentem, który w znaczącym stopniu poprawia efektywność zarządzania przestrzenią adresacji IP, a także zwiększa poziom bezpieczeństwa dostępu do sieci, zwłaszcza w przypadku sieci dużych i rozproszonych. Osiągnięto to dzięki połączeniu ze sobą szeregu funkcjonalności: skutecznego monitoringu sieci, zarządzania przestrzenią adresacji IP (IPAM), kluczowych usług sieciowych (DHCP, DNS), kontroli dostępu do sieci (NAC – Network Access Control) oraz narzędziami do wymiany informacji z infrastrukturą sieciową. Integracja tych, standardowo niezależnych względem siebie, elementów pozwoliła w znaczący sposób usprawnić proces administracji siecią i jej bezpieczeństwem.

Wykorzystując autorskie i innowacyjne technologie oraz rozwiązania Novicom: platformę zarządzania siecią (SGP – Secure Grid Platform), protokół komunikacji (SDP – Secure Delivery Protocol) czy dostępne opcje systemów appliance, ADDNET zapewnia integralność, niezawodność i bezpieczeństwo sieci, z zachowaniem elastycznych metod wdrożenia.

Kompletna widoczność sieci, prosta integracja z innymi rozwiązaniami bezpieczeństwa i opcja wykorzystywania ADDNET jako systemu SOC (Security Operation Center), dostarczają całkowicie nowych możliwości w zakresie wykrywania i reagowania na incydenty naruszeń bezpieczeństwa sieci.

KLUCZOWE ZALETY ADDNET:

- **Wysoce wydajny monitoring sieci w warstwie L2,** z uwzględnieniem możliwości lokalizacji urządzenia dzięki integracji z ewidencją połączeń (okablowania).
- **Usprawnienie zarządzania przestrzenią adresacji IP: wykorzystanie DDI (DHCP/DNS/IPAM)** pozwala znacząco zredukować czas pracy administratorów sieci.
- **Wdrożony NAC (Network Access Control)** zapewnia bezpieczny dostęp do sieci za pomocą protokołu 802.1x/ MAC uwierzytelniania i autoryzacji (przypisanie do sieci VLAN).
- **W pełni zautomatyzowana administracja BYOD i urządzeń mobilnych** oraz ich jednoznaczna identyfikacja w sieci.
- Standaryzacja sieciowych procedur operacyjnych oraz centralizacja administracji i zarządzania dużymi i rozproszonymi sieciami.
- Wyraźnie **podwyższona wydajność i niezawodność działania DNS, DHCP i NAC** za sprawą wielokrotnej redundancji i wysokiej skalowalności.
- **Zmniejszenie kosztów administracji siecią** jako rezultat mniejszych nakładów pracy adminów oraz długookresowego monitoringu wykorzystania portów urządzeń sieciowych.
- **Heterogeniczność i pełna kompatybilność** z wiodącymi producentami sprzętu sieciowego.
- **Unikalne wsparcie dla modelu rozproszonej sieci** – gwarancja zachowania ciągłości monitoringu sieci L2, funkcjonalności DDI i NAC nawet w przypadku utraty łączności z serwerami ADDNET w centralnej lokalizacji.
- **Tworzenie kopii zapasowych danych zebranych z odległych lokalizacji:** w oparciu o syslogi, dataflow.
- **Uniwersalne zastosowanie:** ADDNET spełnia swoją rolę zarówno w organizacjach o scentralizowanej jak i rozproszonej strukturze.
- **Prosta implementacja:** opiera się na połączeniu wstępnej analizy adresacji sieciowej (IP sniffing) z precyzyjną metodologią wdrożeniową Novicom.
- Gotowość do **wdrożenia w ramach sieci technologicznych: OT/ SCADA.**
- **Integracja z SOCami: z**apewnienie szybkiej reakcji na incydent naruszenia bezpieczeństwa.
- **Możliwość integracji z innymi narzędziami IT i bezpieczeństwa,** np. MS Active Directory, SIEM, Log management, Network Behavior Analysis (NBA), Data Loss Prevention (DLP), itd.
- **Alertowanie** – wbudowany system szybkiego powiadamiania w przypadku potencjalnych problemów w sieci.

FUNKCJONALNOŚĆ ADDNET

Wydajny monitoring sieci L2

Monitoring w czasie rzeczywistym daje kompleksową wiedzę na temat lokalizacji urządzenia (zarówno IP jak i MAC adres) w sieci, z uwzględnieniem portu przełącznika i fizycznej lokalizacji, aż do wizualizacji fizycznej lokalizacji urządzenia na planie kondygnacji. Dostarcza również pełną historię operacji sieciowych dla celów kontrolnych i audytowych.

Kompletny DDI (DHCP/DNS/IPAM)

Zapewnia dystrybucję i niezawodność kluczowych usług sieciowych (DHCP i DNS) oraz łatwe zarządzanie poprzez zintegrowane narzędzie IPAM. Połączenie tego modułu z monitoringiem sieci L2 umożliwia określenie w czasie rzeczywistym różnic między istniejącym stanem adresacji IP a jego planem, pomagając tym samym utrzymać projektowaną adresację IP w zgodności z sytuacją rzeczywistą przez cały czas.

- **IPAM**

System zarządzania adresacjami IP stanowi kompleksowe i przyjazne użytkownikowi narzędzie, uwzględniające możliwość administracji jego wszystkimi niezbędnymi elementami (DHCP/DNS/NAC). Dzięki temu dodanie nowego urządzenia lub wprowadzenie zmian parametrów sieciowych do funkcjonujących urządzeń w ramach planu adresacji jest wyjątkowo proste.

- **DHCP**

Rozbudowane usługi, które zostały zaprojektowane z myślą o dużych, rozproszonych sieciach, gdzie wymagana jest całkowita niezawodność i wysoka wydajność działania. Integracja DHCP z monitoringiem L2 dostarczyła wielu możliwości operacyjnych, w tym opcję przydzielania adresów IP przez DHCP wg znanych adresów MAC.

- **DNS**

Usługi DNS, jako część modułu DDI, zapewniają niezawodność dokonywanych operacji w sieciach rozproszonych. W wyniku elastyczności ADDNET możliwe jest również sprawowanie kontroli nad istniejącą infrastrukturą DNS z wykorzystaniem dynamicznych aktualizacji DNS. Takie działanie zapewnia pełną spójność środowiska IPAM, DHCP i DNS.

Zintegrowany NAC (Network Access Control)

Zdecydowaną zaletą będącego częścią ADDNET modułu kontroli dostępu do sieci (NAC) pozostaje proste wdrożenie w ramach dużych, rozproszonych sieci. Tym samym pełna funkcjonalność NAC dla odległych, zdalnych lokalizacji, nawet w przypadku tymczasowego odłączenia od ośrodka centralnego, pozostaje zachowana.

- **Pełne uwierzytelnianie 802.1x**

ADDNET zapewnia bezpieczne uwierzytelnianie urządzenia w jakimkolwiek punkcie sieci organizacji. Dane uwierzytelniania mogą być lokalne w ramach ADDNET lub uzyskane drogą integracji ze środowiskiem Microsoft Active Directory czy z innych źródeł (m.in. OpenLDAP, Novell). ADDNET wspiera wszystkie standardowe tryby uwierzytelniania: wszelkie możliwe kombinacje certyfikatów klienta/ID użytkownika/hasła.

- **Uwierzytelnianie MAC z dodatkową ochroną**

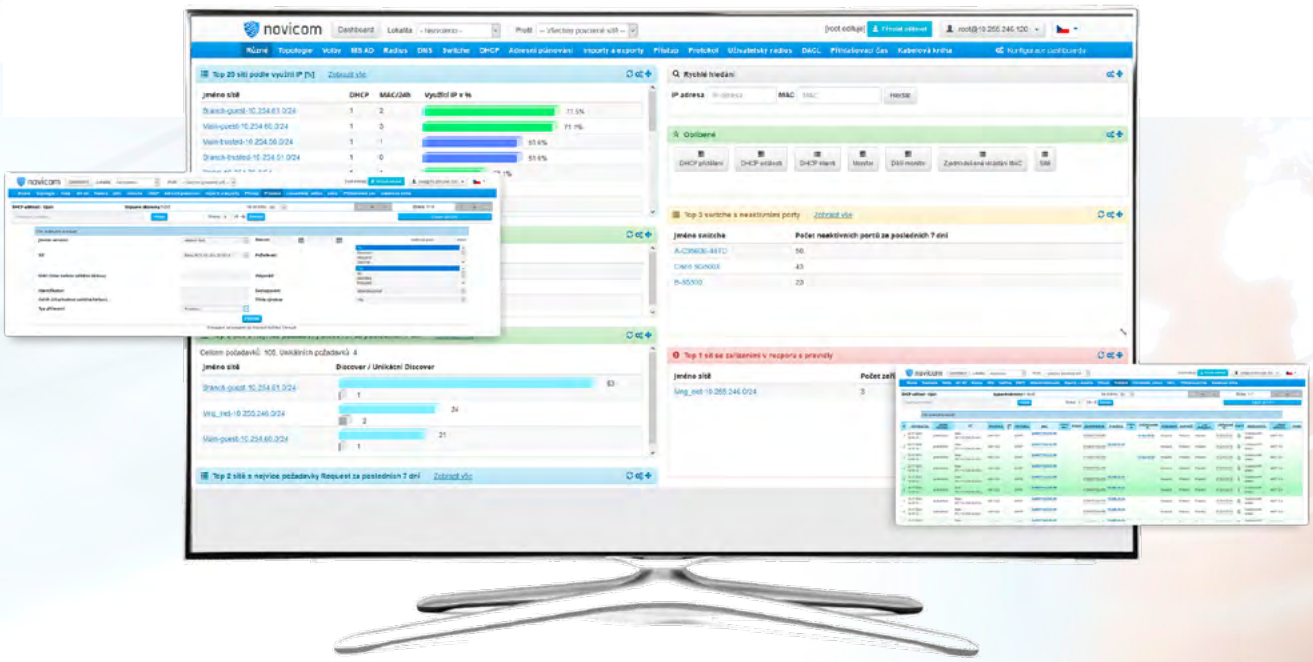
Jako alternatywa w stosunku do urządzeń, których uwierzytelnianie nie jest możliwe z wykorzystaniem suplikantów 802.1x, pozostaje uwierzytelnianie poprzez ich MAC adresy. Zintegrowany monitoring L2 jest w stanie ocenić szereg parametrów i powiadomić admina o zmianie MAC adresu na urządzeniu. Korzyściami jakie wiążą się z tym podejściem, są oszczędność czasu a także wyeliminowanie złożonego procesu implementacji czy obsługi sytuacji wyjątkowych. Tym samym, oferowana jest możliwość praktycznie pełnej funkcjonalności 802.1x, gdzie wszystkie porty przełączników pozostają pod stałą kontrolą.

- **Autoryzacja**

Gdy uwierzytelnianie zostało już dokonane, rozpoczyna się proces autoryzacji, determinującej sieć (VLAN), do której urządzenie zostanie przypisane. W oparciu o korelację z monitoringiem sieci L2, ADDNET pozwala na dynamiczną autoryzację urządzenia w jakiejkolwiek lokalizacji w ramach rozległej sieci.

- **Informacje z operacji NAC w czasie rzeczywistym**

ADDNET oferuje wizualizację informacji o urządzeniach, które logują się do sieci w ramach NAC - kiedy, jaki identyfikator (dla użytkownika zewnętrznego), na którym przełączniku/porcie i do której sieci zostało przydzielone urządzenie.



Planowanie kryzysowe

ADDNET umożliwia zdefiniowanie elementów infrastruktury IT, które traktować należy jako krytyczne. W chwili naruszenia bezpieczeństwa lub stabilności sieci, administrator może przy pomocy jednego kliknięcia, natychmiast odłączyć wszystkie urządzenia, które nie wchodzą w skład infrastruktury krytycznej.

Administracja sieci i kontrola dostępu z perspektywy BYOD i urządzeń mobilnych

ADDNET oferuje możliwość pełnego zarządzania adresacją IP w kontekście sieci wi-fi i działających w jej ramach modelu BYOD (Bring Your Own Device) i urządzeń mobilnych. Stanowi to naturalne uzupełnienie (rozwinięcie) standardowych funkcjonalności administrowania w ramach modelu DDI/NAC. ADDNET posiada samoobsługową strefę jednorazowego uwierzytelniania i autoryzacji BYOD oraz specjalne obszary (jednorazowy dostęp i ograniczona ważność) przyjmowania gości (reception zones). Moduł BYOD ADDNET udziela wsparcia dla wszystkich urządzeń użytkownika, niezależnie od jego systemu operacyjnego czy środowiska.

Zaawansowana komunikacja ze sprzętem sieciowym

ADDNET zapewnia szczegółowe dane dotyczące sprzętu sieciowego, zdefiniowanego w repozytorium. Nieprzerwany monitoring portów pozwala stale weryfikować ich wykorzystanie oraz określać liczbę urządzeń nieaktywnych w sieci. ADDNET posiada także funkcję automatycznego backupu konfiguracji sprzętu sieciowego.

Dashboard: panel administratora

Kluczowe informacje i parametry sieciowe prezentowane na jednym ekranie. Pojedyncze kliknięcie przenosi błyskawicznie administratora z ogólnego widoku danych (dashboard) do szczegółowych informacji dostępnych w ramach wszystkich modułów ADDNET. Istnieje możliwość uzyskania dodatkowych informacji odnośnie każdego adresu IP/MAC w dowolnym momencie. Dashboard można w pełni dostosować do potrzeb administratora/operatora.

Kompleksowe raportowanie

ADDNET to rozbudowana możliwość monitoringu urządzeń sieciowych w trakcie ich pracy. Dotyczy to zarówno monitoringu sieci L2 w czasie rzeczywistym, podglądu szczegółowych danych z serwera DHCP czy informacji, pochodzących z przełączników. Połączenie wielu różnych źródeł informacji w jednym, ujednoliconym interfejsie, otwiera przed administratorem ogromne pole możliwości wnikliwych i kompleksowych obserwacji zachowań wszystkich urządzeń przyłączonych do sieci. Nie pozostaje to bez znaczenia w przypadku efektywnych i szybkich reakcji na wystąpienia naruszeń bezpieczeństwa sieci.

Zaawansowane polityki sieciowe

Powiązane wzajemnie funkcjonalności ADDNET umożliwiają łatwą implementację zaawansowanych polityk sieciowych przy jednoczesnym ograniczeniu bardziej złożonej eksploatacji każdego narzędzia sieciowego z osobna. Niektóre z tych polityk obejmują:

- **Mikrosegmentację**

ADDNET efektywnie definiuje i zarządza politykami DACL na większości przełączników dostępu. Dlatego w praktyce łatwo jest dostosować globalne polityki dla urządzenia tak, aby komunikowało się w sieci dokładnie według jego właściwej funkcjonalności. Wskazując, że można komunikować się tylko w określonych obszarach sieci, inne rodzaje komunikacji są niedozwolone, co znacznie zwiększa ochronę przed potencjalnym rozprzestrzenianiem się infekcji ransomware bez konieczności instalowania agenta na stacjach.

- **Zaufane urządzenia**

ADDNET wspiera zaufane urządzenia i obszary, umożliwiając automatyzację konfiguracji sieciowych i polityk dostępu w zdalnych oddziałach dużych organizacji. Zaufane urządzenia mogą zatem korzystać z różnych sposobów uwierzytelniania, autoryzacji i przypisywania adresów IP bez każdorazowej konieczności interwencji ze strony administratora.

- **Czas logowania**

Organizacje o stałych godzinach pracy mogą dostosować ADDNET do działania tylko w określonych godzinach (np. 7:00–19:00). To dostosowanie może również dotyczyć określonych urządzeń lub przyznać wybranym urządzeniom wyjątek.

Aktywny SOC

Za sprawą swojej funkcjonalnej elastyczności i dostępności w modelu rozproszonym, ADDNET stanowi wysoce poszukiwane dopełnienie każdego SOCu. Razem z informacjami uzyskanymi w wyniku monitoringu i wglądu w sieć, dostarcza operatorom centr operacyjnych danych na temat kluczowych usług sieciowych (DHCP/DNS, NAC). Mogą one zostać później dopełnione informacjami z logów czy transmisji danych z odległych lokalizacji. Integracja narzędzi SOC z ADDNET zapewnia natychmiastową reakcję na incydent w formie izolacji lub odłączenia wadliwego urządzenia przez operatora SOC, bez konieczności ingerencji administratora sieci lokalnej.

Integracja

ADDNET wykazuje gotowość pod względem licznych integracji, których celem jest usprawnienie procesu administrowania siecią i szybka reakcja na zaistniałe zagrożenia.

- **Dostarczanie danych operacyjnych i ich przechowywanie**

ADDNET to cenne źródło informacji służących ocenie ryzyka, które wykorzystuje przy tym wyspecjalizowane narzędzia typu Log management i SIEM. Dane operacyjne i informacje o niestandardowych sytuacjach zostają dostarczane przy pomocy interfejsu sysloga. ADDNET umożliwia ciągłe i nieprzerwane gromadzenie danych związanych z operacjami sieciowymi (flow) i stanem infrastruktury (syslog). Informacje te są bezpiecznie przekazywane celem oceny ryzyka do wyspecjalizowanych aplikacji (SIEM, NBA) w centralnej lokalizacji.

- **Integracja aplikacji**

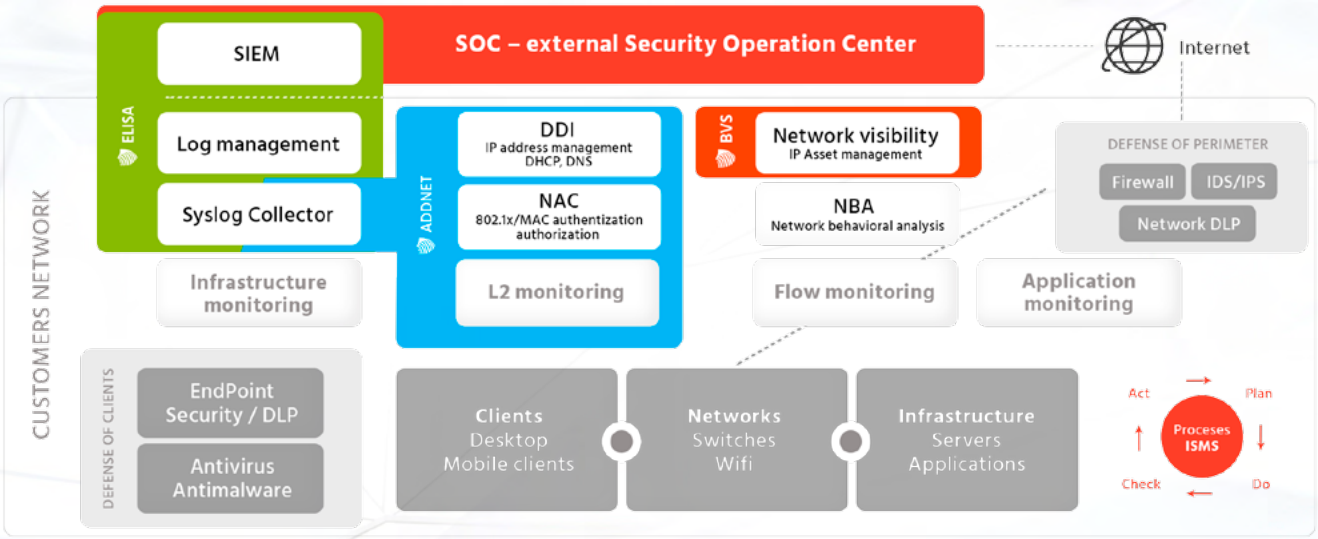
ADDNET udostępnia interfejs celem integracji aplikacji z innymi narzędziami, jak NBA, Log management czy SIEM. ADDNET jest też gotowy względem implementacji interfejsu służącego automatyzacji interwencji. Miarodajne systemy detekcji jak DLP, NBA, Antymalware czy IDS/IPS mogą dostarczać informacji i wskazówek koniecznych do podjęcia niezbędnych interwencji w zakresie administracji siecią.

Centrum Alarmowania

ADDNET składa się z interfejsu, w którym administrator/operator może zarządzać alarmami dotyczącymi potencjalnych problemów. Celem Centrum Alarmowania jest uproszczenie i zautomatyzowanie całego procesu administracyjnego związanego z badaniem zdarzeń. System integruje alarmy z monitoringu L2 (np. zduplikowany MAC), operacji NAC (np. nieudane uwierzytelnienie 802.1x) i więcej.

ADDNET i AKTYWNY SOC

ADDNET jest ważną częścią rozwiązania Active SOC (Security Operation Center), którą Novicom wraz ze swoimi partnerami SOC stara się promować na rynku. **Novicom ADDNET, wraz z rozwiązaniem Novicom BVS** (do wizualizacji zasobów sieciowych, w tym ich wpływu na usługi biznesowe) oraz **Novicom ELISA** (do przechwytywania i ewaluacji zdarzeń cyberbezpieczeństwa) **tworzą unikalne portfolio, które przygotowuje klientów do szybkiego i bezproblemowego połączenia z usługą SOC lub budową własnej tego typu usługi.**



Klienci korzystający z tych produktów, mogą w pełni korzystać z usług premium Active SOC. Dzięki temu wybrani operatorzy SOC są w stanie zagwarantować w pełni kwalifikowaną, aktywną reakcję na cyberataki w trybie 365x24x7 bez konieczności ścisłej współpracy z administratorami systemu u klienta.

Jest to całkowicie zgodne z obecnym trendem polegającym na zastosowaniu najwyższego poziomu nadzoru bezpieczeństwa (SOC) jako usługi. Klient nie musi już ponosić wysokich kosztów związanych z budową wysoce wyspecjalizowanego zespołu do walki z cyberzagrożeniami oraz zakupu drogiej technologii.

NOVICOM – NETWORK MANAGEMENT HAS NEVER BEEN EASIER

novicom

Novicom, s.r.o.
Praga, Republika Czeska

www.novicom.eu
sales@novicom.eu

ADDNET

NVC PL 2020-11