AddNet

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 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 rozwiązań bezpieczeństwa i opcja przyłączenia AddNet do systemów SOC (Security Operation Center), dostarczają całkowicie nowych możliwości w zakresie wykrywania incydentów naruszeń bezpieczeństwa sieci.

NOVICOM – NETWORK MANAGEMENT HAS NEVER BEEN EASIER

Kluczowe zalety AddNet

- **Wysoce wydajny monitoring sieci w warstwie L2**, z uwzględnieniem możliwości fizycznej lokalizacji urządzenia dzięki integracji z ewidencją połączeń (okablowania)
- **Pełna widoczność sieci: NVM (Network Visibility Management)** ułatwia zarządzanie zasobami sieci oraz przyspiesza identyfikację i dalszą weryfikację incydentów naruszeń bezpieczeństwa
- **Usprawnia zarządzanie 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
- W pełni zautomatyzowana **administracja BYOD i urządzeń mobilnych** oraz ich jednoznaczna identyfikacja w sieci
- **Standaryzuje sieciowe procedury** operacyjne oraz umożliwia scentralizowanie administracji w dużych i rozproszonych sieciach
- 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 przez podłączone urządzenia sieciowe.
- **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 operacyjnych przechowywanych w odległych lokalizacjach:** 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 **wdrożenia w ramach sieci technologicznych: OT/ SCADA**
- **Integracja z SOCami:** zapewnienie szybkiej reakcji na incydent naruszenia bezpieczeństwa (rejestr zdarzenia/ ocena/ reakcja)
- **Możliwość integracji z innymi narzędziami bezpieczeństwa,** np. MS Active Directory, SIEM, Log management, Network Behavior Analysis (NBA), Data Loss Prevention (DLP), itd.

Zakres funkcjonalności AddNet

Wydajny monitoring sieci L2

Monitoring w czasie rzeczywistym przekazuje kompleksową wiedzę na temat lokalizacji urządzenia (zarówno IP jak i MAC adres) w sieci (z uwzględnieniem portu switch i fizycznej lokalizacji). Dostarcza również pełną historię operacji sieciowych dla celów audytowych (kontrolnych).
Kompletny DDI (DHCP/ DNS/ IPAM)
Zapewnia dystrybucję i niezawodność kluczowych usług sieciowych (DHCP i DNS). Łatwe zarządzanie poprzez zintegrowane narzędzie IPAM. Połączenie tego modułu wespół z monitoringiem sieci L2 umożliwia rozwiązanie w czasie rzeczywistym różnic miedzy 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 proste.

> DHCP

Rozbudowane usługi, które zostały zaprojektowane z myślą o 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 ustanowienia 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

Zdecydowaną zaletą, będącego częścią AddNet modułu kontroli dostępu do sieci 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 w pełni obsługiwane w ramach AddNet lub uzyskane drogą integracji ze środowiskiem Microsoft Active Directory. AddNet wspiera wszystkie standardowe tryby uwierzytelniania: wszelkie możliwe kombinacje certyfikatów klienta/ ID użytkownika/ hasła.

• Bezpieczny dostęp klienta: suplikant 802.1x

Aby sprostać wciąż rosnącym wymaganiom użytkowników w kontekście zachowania bezpieczeństwa sieci, AddNet oferuje możliwość wykorzystania zaawansowanego suplikanta, który umieszczony na urządzeniu w formie oprogramowania będzie stanowił dodatkową formę uwierzytelniania.

• Uwierzytelnianie MAC z dodatkową ochroną

Jako alternatywa w stosunku do urządzeń, których uwierzytelnianie nie dokonuje się z wykorzystaniem suplikantów, pozostaje uwierzytelnienie 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 switch 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.

Planowanie kryzysowe

AddNet umożliwia zdefiniowanie tzw. zestawów kryzysowych oraz elementów infrastruktury krytycznej. Dlatego gdy dojdzie do naruszenia bezpieczeństwa sieci, administrator może przy pomocy jednego kliknięcia natychmiast odłączyć wszystkie urządzenia, które nie zostały ujęte w zestawie kryzysowym lub 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 BOYD 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 (up/ down state of ports) 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, po kliknięciu przycisku kursora.

Kompleksowe raportowanie

AddNet to rozbudowana możliwość obserwacji urządzeń sieciowych podczas ich pracy. Dotyczy to zarówno monitoringu sieci L2 w czasie rzeczywistym, podglądu szczegółowych danych z serwera DHCP czy informacji, pochodzących z jednostkowych switchy. 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 w przypadku 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.
Zaufane

• 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.

• Przypisanie urządzenia do konkretnej sieci VLAN

AddNet wspiera modele sieci o zdefiniowanych politykach bezpieczeństwa, zarządzanych w warstwie L2, wykorzystując w tym celu dostęp do switchy. Pozwala to na bezproblemowe i globalne zarządzanie siecią VLAN we wszystkich jej lokalizacjach. Urządzenia podpięte do konkretnej sieci będą dopuszczone do komunikacji wyłącznie z wybranymi źródłami. Tym samym w przypadku wystąpienia jakiejkolwiek infekcji (np. ransomware) zostanie ona szybko ograniczona i wyeliminowana.

Widoczność sieci – Business visibility suite

Moduł Business visibility suite wchodzący w skład AddNet jest narzędziem umożliwiającym natychmiastową analizę i wizualizację komunikacji sieciowej wybranego adresu IP. Został on zaprojektowany z myślą szybkiej detekcji i weryfikacji incydentów naruszeń bezpieczeństwa w ramach istniejącej infrastruktury. BVS pomaga w zakresie zrozumienia kontekstu zdarzenia, jego wpływu na świadczone przez organizacje usługi oraz obniża ryzyko ponownego wystąpienia incydentu.

• Standardowa widoczność sieci BVS Network

Wizualizacja podłączonych do infrastruktury komunikacyjnej urządzeń i wchodzących w jej skład zasobów jest fundamentem wszelkich działań zespołów It, wchodzących w skład SOCów: przede wszystkim szybkiej i skutecznej reakcji na zaistniałe incydenty. BVS Network modul analizuje sieć pod kątem wydajności i każdej podejrzanej komunikacji, identyfikując odbiorców dostarczanych usług. Ułatwia również pracę z zasobami, kreując zdefiniowane przez użytkowników zestawy metadanych. BVS sprawdza się także w przypadku migracji infrastruktury ICT do chmury.

• Zaawansowana widoczność sieci BVS Business

Ze względu na ustawienia i funkcjonalność, BVS Business modul jest przystosowany do zarządzania priorytetami w kontekście indywidualnych operacji usługowych. Stanowi on też wsparcie dla zespołów SOC, które mogą dzięki niemu monitorować ryzyko związane ze świadczonymi usługami, ich dostępnością i powiązaniem z indywidualnymi narzędziami wsparcia IT. BVS Business modul ułatwia proces identyfikacji połączeń między usługami biznesowymi/ aplikacjami a infrastrukturą. Usługi wystawione na zagrożenia w sieci są w prosty sposób wykrywane.

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 syslogu czy transmisji danych z odległych lokalizacji.
Integracja narzędzi SOC z AddNet zapewnia natychmiastową reakcję na incydent w formie izolacji lub odłączenia wadliwego urządzenia przez operat SOCu, 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, Anty malware czy IDS/IPS mogą dostarczać informacji i wskazówek koniecznych do podjęcia niezbędnych interwencji w zakresie administracji siecią