NACVIEW

Your Network- Your Rules

DATASHEET

NACVIEW jest systemem typu NAC (Network Access Control),

który jest kluczowym narzędziem w zarządzaniu bezpieczeństwem sieciowym, umożliwiającym organizacjom kontrolę nad dostępem do swoich zasobów. Poprzez skuteczną autoryzację i uwierzytelnianie użytkowników oraz urządzeń podłączających się do sieci, NACVIEW pomaga zapobiegać nieautoryzowanemu dostępowi do danych oraz infrastruktury sieciowej. Zapewniając kontrolę nad tym, kto i co ma dostęp do sieci, NACVIEW wzmacnia bezpieczeństwo organizacji i pomaga zminimalizować ryzyko ataków oraz naruszeń zasad bezpieczeństwa. Rozwiązanie jest idealne dla sieci heterogenicznych, gdyż umożliwia obsługę wszystkich dostawców rozwiązań sieciowych.

Kontrola dostępu

NACVIEW zapewnia skuteczną i bezpieczną funkcjonalność kontroli dostępu do sieci, opartą na protokole 802.1x. Wspierane są również inne metody autoryzacji po adresie MAC dla urządzeń typu IoT, czy dostęp przez Captive Portal dla urządzeń gościnnych wraz z możliwością rejestracji urządzeń prywatnych (BYOD). Dzięki zaawansowanym politykom bezpieczeństwa możliwe jest skonfigurowanie precyzyjnych reguł dostępu, zapewniając tym samym bezpieczny i kontrolowany dostęp do firmowej infrastruktury sieciowej.

Reguło Zero Trust – chroń to, co znasz

Reguła zero trust odnosi się do podejścia do bezpieczeństwa sieciowego, w którym domyślnie nie ufamy żadnemu urządzeniu ani użytkownikowi w sieci. Kontrola dostępu do sieci w ramach tego podejścia oznacza, że każde połączenie, próba dostępu lub komunikacja musi być starannie uwierzytelniona, zidentyfikowana i autoryzowana. Dzięki temu każde urządzenie lub użytkownik jest dokładnie sprawdzany i autoryzowany przed uzyskaniem dostępu do zasobów sieciowych, zgodnie ze zdefiniowanymi politykami bezpieczeństwa.

Widoczność sieci

Widoczność wszystkich urządzeń końcowych podłączonych do sieci organizacji ma zasadnicze znaczenie dla każdej strategii bezpieczeństwa. Świadomość tego, kto i co łączy się z siecią, pozwala zastanowić się, jak optymalnie zapewnić bezpieczeństwo wszystkich zasobów sieciowych. NACVIEW gromadzi wszystkie informacje o tożsamościach i urządzeniach końcowych, które łączą się z siecią, a także o tym, która reguła autoryzacji zapewniała dostęp, na jakim przełączniku, do jakiej podsieci VLAN i wiele innych. Wszystkie zebrane informacje są łatwo dostępne i przejrzyście wyświetlane na dwa sposoby. Widok tabelaryczny – umożliwiający łatwe wyszukanie informacji lub widok graficzny – pozwalający na zrozumienie tego co jest w twojej sieci.

Zgodność z politykami bezpieczeństwa

NACVIEW wspiera organizacje w spełnianiu wymagań regulacyjnych oraz zasad bezpieczeństwa poprzez skuteczne monitorowanie i egzekwowanie polityk bezpieczeństwa. Dzięki temu administratorzy mogą śledzić zgodność z politykami bezpieczeństwa oraz reagować na wszelkie niezgodności w czasie rzeczywistym, co pozwala organizacjom utrzymać wysoki poziom zabezpieczeń. Rozwiązanie umożliwia również dostosowywanie zasad dostępu do sieci w zależności od zmieniających się wymagań regulacyjnych, co jest kluczowe dla organizacji działających w środowiskach podlegających różnym przepisom branżowym czy ustawom.

Integracja z systemami zewnętrznymi

System NACVIEW jest integralną częścią całościowego rozwiązania bezpieczeństwa sieci. Dzięki integracji z innymi systemami bezpieczeństwa takimi jak NGFW, UTM, SIEM, Antivirus, MDM itp., kluczowe informacje są wymieniane między platformami, aby zapewnić najwyższy poziom bezpieczeństwa użytkownikom i urządzeniom korzystającym z sieci firmowej.

Widoczność urządzeń sieciowych

Podgląd wszystkich urządzeń sieciowych w organizacji daje możliwość zarządzania nimi w czasie rzeczywistym. NACVIEW umożliwia wyświetlanie kluczowych parametrów urządzenia, takich jak obciążenie, zdarzenia autoryzacji, status przełącznika oraz wiele innych. Wszelkie nieprawidłowości związane z liczbą odrzuconych autoryzacji lub zwiększonym obciążeniem można łatwo wykryć. System umożliwia również centralne zarządzanie wszystkimi urządzeniami sieciowymi, na poziomie konfiguracji portów (możliwość włączenia lub wyłączenia portu).

Centralizacja zarządzania

Centralizacja zarządzania ułatwia administratorom skuteczne zarządzanie dostępem do sieci oraz implementację zasad bezpieczeństwa. Dzięki temu możliwe jest stosowanie spójnych reguł bezpieczeństwa we wszystkich obszarach sieci, niezależnie od ich ilości czy złożoności. Ponadto, centralizacja zarządzania umożliwia szybką reakcję na zmieniające się warunki i potrzeby sieciowe, co przyczynia się do zwiększenia efektywności operacyjnej oraz lepszej ochrony zasobów sieciowych.

Funkcjonalność systemu:

Autoryzacja

- Autoryzacja użytkowników i urządzeń w sieci LAN i WiFi.
- Wbudowany serwer RADIUS do obsługi autoryzacji w oparciu o protokół 802.1x.
- Lokalna, wbudowana baza danych z informacjami o użytkownikach i urządzeniach końcowych.
- Możliwość uwierzytelniania w oparciu o zewnętrzne bazy danych w tym AD, LDAP, SQL, Radius, Eduroam, API, Google Workspace, Facebook, Google, LinkedIn.
- Obsługa różnych metod autoryzacji: 802.1x, na podstawie adresu MAC, za pośrednictwem Captive Portalu.
- Funkcja rozłączania oparta o protokół: RADIUS CoA, SNMP, Telnet /SSH.

Widoczność

- Rozbudowana funkcjonalność monitorowania i raportowania.
- Monitorowanie SNMP urządzeń sieciowych z opcją bieżącego sprawdzania obciążenia, liczby uprawnień lub prawidłowej pracy urządzenia.
- Monitorowanie urządzeń końcowych za pomocą SNMP.
- Graficzne diagramy fizycznej topologii sieci.

Zarządzanie siecią

- Wbudowana funkcjonalność serwera DHCP.
- Możliwość zarządzania i wizualizacji adresacji IP (funkcjonalność IPAM).
- Wykrywanie obcych serwerów DHCP.
- Funkcjonalność zdalnej konfiguracji przełącznika na poziomie portu (możliwość włączenia/wyłączenia portu).
- Wbudowany serwer TFTP.
- Repozytorium konfiguracji urządzeń sieciowych z narzędziem umożliwiającym porównywanie konfiguracji.

Integracja

- Dwukierunkowa integracja z innymi systemami bezpieczeństwa pracującymi w sieci firmowej.
- Możliwość automatycznej reakcji na zagrożenia wykryte przez inne systemy bezpieczeństwa i zablokowania lub przeniesienia do kwarantanny niebezpiecznego urządzenia końcowego.

Administracja i zarządzanie

- System centralnie zarządzany z poziomu interfejsu graficznego.
- Konsola zarządzająca dostępna w języku polskim i angielskim.
- Możliwość tworzeni grup administracyjnych i przydzielania szczegółowych uprawnień do poszczególnych funkcjonalności systemu.
- Praca w sieciach heterogenicznych z urządzeniami sieciowymi, które spełniają standardy.
- Praca w środowisku wielodomenowym (całkowicie niezależne domeny).
- Funkcjonalność autodiscovery, umożliwiająca wyszukanie urządzeń sieciowych w sieci.

Certyfikaty

- Wbudowany serwer CA do obsługi autoryzacji przy użyciu własnych certyfikatów.
- Możliwość wdrożenia w środowiskach obsługiwanych przez wiele urzędów certyfikacji CA.
- Dystrybucja certyfikatów z zewnętrznych CA przez SCEP.

Dostęp gościnny

- Możliwość obsługi dostępu do sieci poprzez zewnętrzny Captive Portal na punkcie dostępowym (AP).
- Możliwość obsługi dostępu do sieci poprzez dedykowany Captive Portal.
- Captive Portal dostępny w różnych wersjach językowych (m.in. polskim, angielskim, niemieckim, ukraińskim, francuskim).
- Możliwość obsłużenia kont pochodzących w mediów społecznościowych (np. Google, LinkedIn, Facebook, miniOrange).
- Możliwość rejestracji nowych kont gościnnych.
- Obsługa kont czasowych.
- Obsługa sponsorów.

Skalowanie i dostępność

- W celu zapewnienia niezawodności działania w ramach podstawowej licencji systemu dostępna jest funkcjonalność HA.
- Wersja rozproszona dostępna w podstawowej wersji oprogramowania.
- Graficzne diagramy fizycznej topologii sieci.

Funkcjonalność dodatkowa

- Profilowanie urządzeń końcowych.
- Dedykowany agent (NACVIEW Scout) dla weryfikacji podatności na zagrożenia urządzeń końcowych.
- Rozłączanie sesji z wykorzystaniem agenta NACVIEW Scout.
- OTP (One Time Password) dla VPN – dodatkowe zabezpieczenie przy logowaniu do sieci VPN (obsługa SMS/ tokenów).
- Możliwość zarządzenia urządzeniami końcowymi przez Captive Portal.
- Aplikacja NACVIEW Assistant dla automatycznej konfiguracji sieci na urządzeniu końcowym.
- Możliwość resetowania haseł użytkowników domenowych przez Captive Portal lub Portal Zarządzający.
- Wbudowany serwer Tacacs+.

Dostępne platformy:

NACVIEW jest dostępny jako platforma wirtualna.

Platformy wirtualne są obsługiwane przez:

- VMware (version 5.5 oraz nowsze),
- Windows Hyper-V (version 2016 oraz nowsze),
- KVM (version 7 oraz nowsze),
- Citrix XenServer (version 4 oraz nowsze),
- Proxmox (version 7 oraz nowsze).

System jest dostępny również na inne platformy wirtualizacyjne. W celu otrzymania dodatkowych informacji skontaktuj się z dostawcą.

Platformy wirtualne dostępne są jako licencje dożywotnie lub subskrypcja. Więcej o wymaganiach technicznych i licencjach w dokumencie Instrukcja wprowadzająca.

Obsługiwane metody autoryzacji

- PAP
- EAP-MD5
- CHAP, MSCHAPv1, MSCHAPv2
- EAP-TLS
- EAP-FAST (EAP-MSCHAPv2, EAP-TLS)
- PEAP (EAP-MSCHAPv2, EAP-TLS, EAP-PEAP)
- TTLS (EAP-MSCHAPv2, EAP-TLS, EAP-MD5)
- TEAP
- MAC
- Captive Portal (wbudowany, zewnętrzny na punkcie dostępowym, integracja z sieciami społecznościowymi, obsługa sponsorów)
- Kerberos
- Tacacs+
- Token

Wspierane bazy przechowujące informację o użytkownikach i urządzeniach

- Lokalna wbudowana
- Microsoft Active Directory
- RADIUS (np. EDUROAM)
- LDAP
- Microsoft SQL, MySQL, PostgreSQL, Oracle, ODBC
- Kerberos
- przez API
- media społecznościowe
- Google Workspace

NACVIEW Scout

Lekki agent zapewniający dodatkową kontrolę podatności urządzeń na zagrożenia. Jego zastosowanie pozwala na wykluczenie z sieci urządzeń, które nie spełniają wymogów bezpieczeństwa.

Opcje sprawdzenia przez agenta:

- Antywirus
- Aktualizacje systemowe
- Szyfrowanie dyskowe
- Firewall
- Procesy
- Pliki
- Klucze rejestru
- Połączenie z domeną
- Aplikacje

Agent dostępny dla:

Mac OS Windows Linux

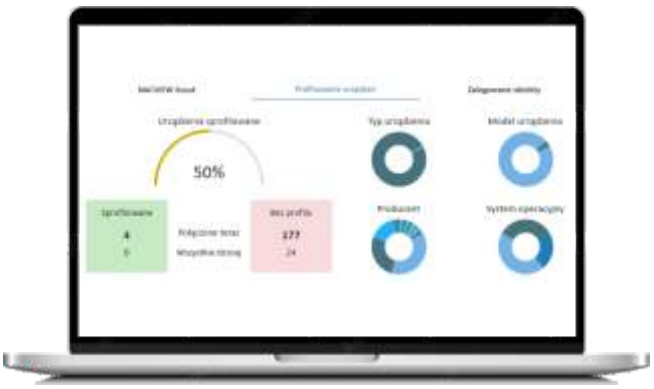
Metody profilowania

Pasywne

- DNS
- RADIUS
- Vendor OUI
- Active Directory
- HTTP/S
- CDP/LLDP

Aktywne

- WMI
- SNMP
- NMAP
- TCP
- DHCP Fingerprinting
- DHCP SPAN
- dedykowany Agent (NACVIEW Scout)
- MDM
- UTM
- NGFW
- API
- ONVIF



Rys. Panel administracyjny - podgląd sprofilowanych urządzeń końcowych.

W każdej licencji systemu dostępne są wszystkie funkcjonalności bez ograniczeń.
Rozwiązanie licencjonuje się na liczbę unikatowych urządzeń końcowych poprawnie zautoryzowanych w sieci.

Licencja dożywotnia

Nazwa licencji	Ilość urządzeń końcowych*
NV-100-VM	100
NV-250-VM	250
NV-500-VM	500
NV-1000-VM	1 000
NV-1500-VM	1 500
NV-2500-VM	2 500
NV-5K-VM	5 000
NV-10K-VM	10 000
NV-15K-VM	15 000
NV-20K-VM	20 000
NV-25K-VM	25 000
NV-50K-VM	50 000
NV-100K-VM	100 000

Wsparcie

Nazwa produktu
Sup-NV-100
Sup-NV-250
Sup-NV-500
Sup-NV-1000
Sup-NV-1500
Sup-NV-2500
Sup-NV-5K
Sup-NV-10K
Sup-NV-15K
Sup-NV-20K
Sup-NV-25K
Sup-NV-50K
Sup-NV-100K

Roczna subskrypcja

Nazwa licencji	Ilość urządzeń końcowych*
NV-100-VM-AS	100
NV-250-VM-AS	250
NV-500-VM-AS	500
NV-1000-VM-AS	1 000
NV-1500-VM-AS	1 500
NV-2500-VM-AS	2 500
NV-5K-VM-AS	5 000
NV-10K-VM-AS	10 000
NV-15K-VM-AS	15 000
NV-20K-VM-AS	20 000
NV-25K-VM-AS	25 000
NV-50K-VM-AS	50 000
NV-100K-VM-AS	100 000

Dla licencji dożywotniej wymagany zakup pierwszego roku wsparcia

Wsparcie wliczone w cenę subskrypcji

* Liczba aktualnie poprawnie zautoryzowanych i zalogowanych urządzeń do sieci.