Informacje techniczne i wdrożeniowe

DOSTĘPNE PLATFORMY

NACVIEW jest dostępny jako platforma wirtualna. Platformy wirtualne są obsługiwane przez:

Vmware	Hyper-V	Citrix XenServer	KVM	Proxmox
5.5 oraz nowsze	2016 i nowsze	4 i nowsze	7 i nowsze	7 i nowsze

System jest dostępny również na inne platformy wirtualizacyjne. Szczegółowe informacje można uzyskać u dostawcy.
Platformy wirtualne dostępne są jako licencje dożywotnie lub subskrypcja.
Więcej o wymaganiach technicznych i licencjach w dokumencie *Instrukcja wprowadzająca.*

WSPIERANE BAZY PRZECHOWUJĄCE INFORMACJE 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

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+

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: • macOS • Windows • Linux.

Metody profilowania

P Pasywne

Protokoły i usługi sieciowe: DNS, HTTP/S
Autoryzacja i zdarzenia dostępowe: RADIUS
Źródła katalogowe i tożsamościowe: Active Directory
Identyfikacja producenta urządzenia: Vendor OUI
Protokoły topologii sieci: CDP/LLDP

A Aktywne

Odpytywanie i skanowanie: WMI, SNMP, NMAP, TCP
Analiza DHCP: DHCP Fingerprinting, DHCP SPAN
Agent NACVIEW: Dedykowany agent NACVIEW Scout
Systemy zarządzania urządzeniami: MDM
Integracje z systemami bezpieczeństwa i urządzeniami: UTM, API, NGFW, ONVIF

Licencjonowanie

System NACVIEW jest dostępny w dwóch modelach licencjonowania: dożywotnim oraz subskrypcyjnym. Licencja dożywotnia wymaga zakupu co najmniej jednego roku wsparcia. W modelu subskrypcyjnym wsparcie jest zawarte w cenie subskrypcji. Każda licencja zapewnia pełną funkcjonalność systemu. Aktualne warianty licencji są dostępne na stronie: https://nacview.com/pl/system/oferta

DATASHEET

NACVIEW

Your Network. Your Rules.

NACVIEW to fundament cyberbezpieczeństwa

NACVIEW to system klasy NAC (Network Access Control), który umożliwia firmom i instytucjom kontrolę dostępu do zasobów – w sieci przewodowej, bezprzewodowej i VPN. Wspiera autoryzację i uwierzytelnianie użytkowników oraz urządzeń końcowych podłączających się do sieci, pomaga ograniczać ryzyko nieautoryzowanego dostępu do danych i infrastruktury, a także umożliwia egzekwowanie zdefiniowanych polityk bezpieczeństwa. Dzięki obsłudze środowisk heterogenicznych, NACVIEW może być wdrażany w realnej, mieszanej infrastrukturze IT, bez uzależnienia od jednego producenta rozwiązań sieciowych.

ZASADA ZERO TRUST

Nie ufaj. Weryfikuj. Autoryzuj.

Reguła zero trust odnosi się do podejścia do bezpieczeństwa sieciowego, w którym domyślnie nie ufa się 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.

Kluczowe możliwości systemu

Cyberbezpieczeństwo zaczyna się od wiedzy, kto i co łączy się z firmową siecią.

NAC + VIEW

Kontrola dostępu 01

NACVIEW zapewnia funkcjonalność kontroli dostępu do sieci opartą na protokole 802.1X oraz innych metodach autoryzacji, w tym na podstawie adresu MAC dla urządzeń typu IoT i dostępu przez Captive Portal dla urządzeń gościnnych, wraz z możliwością rejestracji urządzeń prywatnych (BYOD). Mechanizmy kontroli dostępu pozwalają przypisywać uprawnienia adekwatnie do roli użytkownika, typu urządzenia, sposobu połączenia i przyjętych scenariuszy dostępowych. Dzięki temu dostęp do firmowej infrastruktury może być nadawany, ograniczany lub blokowany, zgodnie z politykami bezpieczeństwa obowiązującymi w danej organizacji.

Widoczność sieci 02

Widoczność wszystkich urządzeń końcowych podłączonych do sieci ma zasadnicze znaczenie dla skutecznej strategii bezpieczeństwa. Wiedza o tym, kto i co łączy się z siecią oraz skąd i kiedy, pozwala precyzyjniej zarządzać ryzykiem i chronić zasoby. NACVIEW gromadzi informacje o użytkownikach i urządzeniach końcowych łączących się z siecią, a także o regułach autoryzacji, przełącznikach, podsieciach VLAN oraz innych parametrach połączenia. Zebrane dane są prezentowane w widoku tabelarycznym, który ułatwia wyszukiwanie informacji oraz w widoku graficznym, który pomaga zrozumieć strukturę i kontekst połączeń w sieci.

Monitoring i zarządzanie infrastrukturą sieciową 03

NACVIEW umożliwia monitorowanie wszystkich urządzeń infrastruktury sieciowej w czasie rzeczywistym oraz analizę kluczowych parametrów ich pracy, takich jak obciążenie, status przełącznika, zdarzenia autoryzacji, stan portów i inne. Dzięki temu administratorzy mogą szybciej wykrywać nieprawidłowości, takie jak np. wzrost liczby odrzuconych autoryzacji czy nietypowe obciążenie urządzenia. System umożliwia również zarządzanie konfiguracją portów, w tym ich włączanie lub wyłączanie w ramach bieżącej obsługi infrastruktury.

Centralizacja i automatyzacja zarządzania 04

Centralizacja zarządzania ułatwia administratorom skuteczne kontrolowanie dostępu do sieci oraz implementację zasad bezpieczeństwa z jednego panelu administracyjnego. Dzięki temu możliwe jest stosowanie spójnych reguł bezpieczeństwa we wszystkich obszarach sieci, niezależnie od ich liczby czy złożoności. Takie podejście umożliwia szybką reakcję na zmieniające się warunki i potrzeby sieciowe, a tym samym podnosi efektywność operacyjną, ogranicza ryzyko niespójnej konfiguracji oraz wzmacnia ochronę zasobów sieciowych.

Zgodność z politykami Bezpieczeństwa 05

NACVIEW wspiera firmy i instytucje w egzekwowaniu zasad bezpieczeństwa oraz dokumentowaniu zgodności z wymogami regulacyjnymi. System umożliwia administratorom śledzenie zgodności z politykami bezpieczeństwa oraz reagowanie na nieprawidłowości w czasie rzeczywistym, pomagając utrzymać wysoki poziom zabezpieczeń. Umożliwia również dostosowywanie zasad dostępu do sieci w zależności od zmieniających się wymagań regulacyjnych, co ma kluczowe znaczenie zwłaszcza dla organizacji działających w sektorach silnie regulowanych.

Integracja z zewnętrznymi systemami 06

NACVIEW działa jako bazowa warstwa kontroli dostępu w szerszej architekturze bezpieczeństwa sieciowego, współpracując z takimi systemami, jak NGFW, UTM, SIEM, antywirus, MDM oraz innymi platformami bezpieczeństwa. Dzięki możliwości integracji z rozwiązaniami wykorzystywanymi już w firmowej infrastrukturze, system zapewnia wymianę kluczowych informacji między platformami, wspierając automatyczną reakcję na zdarzenia, egzekwowanie polityk bezpieczeństwa oraz ograniczanie ryzyka po stronie użytkowników i urządzeń korzystających z sieci.

Szczegółowy zakres funkcjonalny

Autoryzacja

- Autoryzacja użytkowników i urządzeń w sieci LAN i Wi-Fi.
- 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 źródła danych i tożsamości, 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 autoryzacji oraz 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.

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.

Administracja i zarządzanie

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

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 w różnych wersjach językowych, m.in. polskiej, angielskiej, niemieckiej, ukraińskiej, francuskiej.
- Możliwość obsługi kont pochodzących z mediów społecznościowych (np. Google, LinkedIn, Facebook, miniOrange).
- Możliwość rejestracji nowych kont gościnnych.
- Obsługa kont czasowych.
- Obsługa sponsorów.

Skalowanie i dostępność

- System udostępnia funkcjonalność HA, wspierającą niezawodność działania.
- Może działać w rozproszonej architekturze.
- Obsługuje nieograniczoną liczbę węzłów w ramach licencji.

Funkcjonalności dodatkowe

- Profilowanie urządzeń końcowych.
- Dedykowany agent NACVIEW Scout do 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 zarządzania urządzeniami końcowymi przez Captive Portal.
- Aplikacja NACVIEW Assistant do automatycznej konfiguracji sieci na urządzeniu końcowym.
- Możliwość resetowania haseł użytkowników domenowych przez Captive Portal lub Portal Zarządzający.
- Wbudowany serwer TACACS+.