NACVIEW

Your Network- Your Rules

NIEZBĘDNIK NOWOCZESNEGO MANAGERA

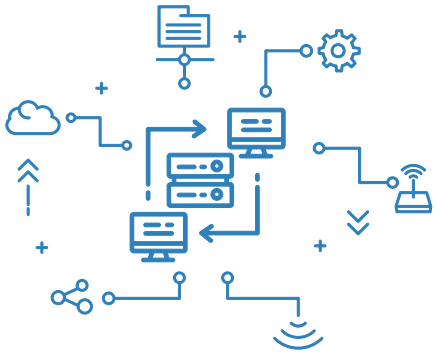
CZY WIESZ JAKIE I ILE URZĄDZEŃ ZNAJDUJE SIĘ W TWOJEJ SIECI?

Prywatne telefony pracowników, urządzenia należące do gości odwiedzających firmę, urządzenia osób pracujących zdalnie, urządzenia IoT, komputery niespełniające wymogów zgodności, które mają niezaktualizowany system operacyjny albo wyłączony system antywirusowy. Każde takie urządzenie połączone z siecią firmową może stanowić zagrożenie.

Wystarczy jedno zainfekowane złośliwym oprogramowaniem, aby problem rozprzestrzenił się na całą sieć komputerową.

W konsekwencji może to doprowadzić do wycieku danych, kradzieży poufnych informacji lub zaszyfrowania danych firmowych, w rezultacie strat finansowych i utraty reputacji.

System kontroli dostępu do sieci NACVIEW chroni przed nieautoryzowanym dostępem do infrastruktury nieznanych lub potencjalnie niebezpiecznych urządzeń. Umożliwia pełną widoczność wszystkich podłączanych do sieci obiektów oraz zarządza przyznawaniem im dostępu do wskazanych zasobów. Dzięki temu cała sieć firmowa jest bezpieczniejsza, lepiej skoordynowana i bardziej wydajna.



W czasach wszechobecnego dostępu do Internetu, dla różnego rodzaju urządzeń, organizacje nie mogą pozwolić sobie na brak kontroli nad tym co i kiedy łączy się z ich siecią firmową. Podczas najbardziej znanych złośliwych ataków - takich jak WannaCry lub NotPeyta organizacje z centralnie zarządzanym dostępem do sieci mogłyby znacząco zmniejszyć ryzyko, izolując niezaktualizowane urządzenia od reszty sieci.

NACVIEW sprawi, że Twoja sieć firmowa będzie lepiej chroniona i wolna od niezidentyfikowanych urządzeń.

DLACZEGO WARTO:

POPRAWA CYBERBEZPIECZEŃSTWA.

Zasoby korporacyjne są narażone na różnego typu zagrożenia jak złośliwe oprogramowanie, ransomware, czy ataki DDoS. Hakerzy nieustannie szukają dostępu do poufnych danych, które mogą sprzedać w Dark Web. Rozwiązanie NACVIEW pomaga minimalizować te zagrożenia, wykluczając niezaktualizowane lub podejrzane urządzenia i ograniczyć to, co użytkownicy mogą zrobić w sieci.

BEZPIECZNY DOSTĘP VPN.

Praca zdalna stała się powszechnym trendem. Sprawia to, że działy IT muszą umożliwić pracownikom dostęp do zasobów sieciowych przedsiębiorstwa z zewnątrz poprzez VPN. Problemem przy takim rozwiązaniu jest brak możliwości ich 100% weryfikacji. Czy na pewno z siecią łączy się nasz pracownik, czy to może osoba, która przejęła urządzenie lub wykradła hasło do VPN. Dlatego tak istotne jest zabezpieczenie dostępu zdalnego drugim czynnikiem uwierzytelniającym. NACVIEW można zintegrować z praktycznie dowolnym systemem VPN i uruchomić dwuskładnikowe uwierzytelnianie z wykorzystaniem dedykowanej aplikacji na telefony lub jednorazowych haseł SMS.

LEPSZE WYKORZYSTANIE INNYCH POSIADANYCH SYSTEMÓW BEZPIECZEŃSTWA.

System NAC jest centralnym bezpiecznikiem, a więc można do niego przekierować logi z innych systemów takich jak Antywirus, Firewall, itp. Dzięki temu możliwa jest automatyczna reakcja na zagrożenia wykryte przez systemy trzecie oraz odłączanie od sieci wewnętrznej potencjalnie niebezpiecznych lub zainfekowanych urządzeń.

CO JESZCZE ZYSKUJESZ:

KONTROLA NAD PRYWATNYMI URZĄDZENIAMI PRACOWNIKÓW BYOD.

W obecnych czasach coraz bardziej zacierają się różnice pomiędzy urządzeniami prywatnymi i służbowymi. Co więcej niektóre firmy wręcz pozwalają pracownikom na korzystanie, z prywatnych urządzeń do celów firmowych, aby zwiększyć efektowność ich pracy oraz zmniejszyć koszty własne. BYOD nie musi oznaczać rezygnacji z bezpieczeństwa. Wdrożona kontrola dostępu do sieci może zezwolić na dostęp tylko zaktualizowanym i zabezpieczonym urządzeniom, lub przekierowywać urządzenia do oddzielnej sieci VLAN albo sieci dla gości.

REDUKCJA KOSZTÓW

System pozwala na szybkie i sprawne przeglądanie danych oraz wyszukiwanie problemów w sieci. Dzięki temu administratorzy mogą sprawnie zdiagnozować problemy i natychmiast wdrażać środki zaradcze poprawiające jej działanie. Ponadto mechanizmy automatyzacji pozwalają zaplanować wiele aspektów z wyprzedzeniem, aby system wykonał je samodzielnie za administratorów. Będą to między innymi zaplanowane wcześniej polecenia systemowe, automatyczne wyłączenia i włączenia sieci Wi-Fi w dniach wolnych od pracy, aby nie pobierały energii, lub przekazywanie informacji o niewykorzystywanych od dłuższego czasu portach, pozwalając na maksymalne wykorzystanie aktualnie posiadanego sprzętu.

KONTROLOWANY DOSTĘP GOŚCINNY.

Bezpieczny i zautomatyzowany dostęp do sieci dla gości to znak nowoczesnej i solidnej firmy. Z wykorzystaniem zautomatyzowanego Captive Portalu goście mogą samodzielnie zarejestrować swoje konto, aby uzyskać dostęp do sieci. Można nadać mu indywidualny wygląd poprzez wstawienie logo i tła graficznego oraz publikować na nim treści marketingowe i informacyjne. Zaprezentujesz swoją markę, możesz informować o aktualnych ofertach lub promować wybrane usługi i produkty. Wszystko to sprawi, że goście będą czuć się mile widziani, a firma będzie posiadać wiedzę kto korzysta z jej sieci.

ZWIĘKSZENIE WYDAJNOŚCI I ERGONOMII PRACY.

Dzięki precyzyjnej polityce NACVIEW pracownicy, niezależnie z jakiego miejsca i w jaki sposób będą podłączać się do sieci, zawsze dostaną się do dedykowanych dla nich podsieci, z dostępem do potrzebnych zasobów i usług sieciowych. Co ważne, wdrożenie systemu NAC wiąże się z segmentacją sieci i uregulowaniem ruchu sieciowego. Dzięki temu zwiększymy przepustowość łącza dla każdego użytkownika.

NIŻSZE KOSZTY EKSPLOATACJI

NACVIEW jest systemem niezależnym od producentów sprzętu sieciowego. Dlatego przy zakupie nowych przełączników lub wymianie starych firma nie będzie zależna cenowo od jednego producenta. Możliwe jest sprawdzenie wielu producentów sprzętu sieciowego, tak aby każdorazowo móc wybrać wariant najkorzystniejszy ze względów bezpieczeństwa, funkcjonalności i wydajności.

ZGODNOŚĆ Z ZASADAMI BEZPIECZEŃSTWA

NAC jest również cennym narzędziem zapewniającym zgodność z odpowiednimi przepisami dotyczącymi cyberbezpieczeństwa. Zasady bezpieczeństwa sieci można zintegrować z planami zgodności RODO lub HIPAA, dostarczając dowodów na to, że sieci spełniają wymagane zewnętrzne standardy.