

Załącznik nr 9 Opis Przedmiotu Zamówienia

1. Firewall UTM - nadmiarowe urządzenia do pracy w klastrze (1 szuka)

Wymagania Ogólne

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji.

Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klastery Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łącz sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
 - 10 portami Gigabit Ethernet RJ-45.
2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB.
3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 1.4 mln jednoczesnych połączeń oraz 100 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 3.5 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 7 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 2.4 Gbps.
6. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1.3 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1.4 Gbps.

Funkcje Systemu Bezpieczeństwa:

W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zaporę ogniową klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN .
4. Ochrona przed malware.

5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
10. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
11. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system.
12. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
 - Translację jeden do jeden oraz jeden do wielu.
 - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP.
5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
 - Amazon Web Services (AWS).
 - Microsoft Azure.
 - Cisco ACI.
 - Google Cloud Platform (GCP).
 - OpenStack.
 - VMware NSX.
 - Kubernetes.

Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
 - Wsparcie dla IKE v1 oraz v2.
 - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
 - Obsługa protokołu Diffie-Hellman grup 19, 20.
 - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
 - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
 - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
 - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
 - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
 - Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
 - Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
 - Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
 - Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łącz W

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPv2), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

Zarządzanie pasmem

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej.
8. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
9. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
8. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.

2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
 - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
 - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
 - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego.
3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Testy wydajnościowe oraz funkcjonalne

1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni).

Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.

Opisy do wymagań ogólnych

1. Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Zaleca się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.

Opis czynności do wykonania podczas wdrożenia urządzenia UTM:

1. Analiza dotychczasowego środowiska sieciowego bezpośrednio związana z posiadanym przez Urząd urządzeniem UTM obejmująca sprawdzenie i usunięcie ewentualnych nieprawidłowości
2. Przeprowadzenie pomiaru przepustowości węzłów sieci doprowadzonych bezpośrednio do urządzenia Fortigate i ewentualne usunięcie nie w pełni sprawnych połączeń
3. Aktualizacja oprogramowania urządzenia do najnowszej wersji dostępnej w dniu przeprowadzania usługi
4. Omówienie dotychczas stosowanych polityk bezpieczeństwa i skonfrontowanie ich z nowymi potrzebami
5. Przygotowanie nowych lub aktualizacja dotychczas stosowanych polityk bezpieczeństwa
6. Konfiguracja i zastosowanie modułów UTM i wykonanie kopii zapasowej ustawień urządzenia
7. Testy przeciążeniowe urządzenia zarówno na samym firewall'u jak i na poszczególnych modułach UTM
8. Inżynier posiadający certyfikat NFS 4 będzie dostępny do pomocy i konsultacji przez cały okres trwania umowy. Zaleca się, aby Wykonawca posiadał co najmniej 2 certyfikowanych inżynierów z zakresu oferowanych rozwiązań.
9. Dla zapewnienia wysokiego poziomu usług zamówienie musi być realizowane przez wykonawcę na poziomie min. zaawansowanym, posiadającego aktywne specjalizacje:
10. a) w zakresie Zdefiniowanej Programowo Sieci Rozległej (SD-WAN),
11. b) w zakresie Krawędzi Usługi Bezpiecznego Dostępu (SASE),
12. Zamawiający planuje wdrożyć wyżej wymienione rozwiązania zgodnie z zaleceniami DYREKTYWY PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (NIS2). Do tego niezbędne mogą być konsultacje dotyczące zgodności z wyżej wymienioną dyrektywą lub Systemem Zarządzania Bezpieczeństwem Informacji Zamawiającego, wobec czego zaleca się, by wykonawca posiadał również co

najmniej jeden certyfikat Audytora Wiodącego Systemu Bezpieczeństwa Informacji zgodnie z normą PN-EN ISO/IEC 27001:2023-08.

13. Zakres wdrożenia

Wdrożenie UTM zaawansowane / pełne

- 14. - Rejestracja urządzenia / serwisów
- Konfiguracja portu WAN / SD-WAN / Failover
- Konfiguracja portów LAN
- Konfiguracja VLAN
- Konfiguracja Profili Bezpieczeństwa
- Konfiguracja Polityk Firewall
- Konfiguracja przekierowań portów
- Konfiguracja VPN
- Dodanie użytkowników
- Dodanie Administratorów
- Integracja z LDAP

15. Dokumenty potwierdzające spełnienie wymagań należy dołączyć do oferty.

2. Switch zarządzalny (2 sztuki)

PARAMETR TECHNICZNY	MINIMALNE WYMAGANIA / OPIS SZCZEGÓŁOWY
Typ urządzenia	Zarządzalny przełącznik sieciowy (Managed Switch) warstwy 2/3 z możliwością montażu w szafie rack 19"
Obudowa	Rack 1U z metalowej konstrukcji przeznaczonej do montażu w szafie rack
Procesor	Qualcomm Atheros QCA9531 o architekturze MIPSBE, taktowanie min. 650 MHz
Pamięć RAM	Min. 64 MB DDR
Pamięć Flash	Min. 16 MB pamięci nieulotnej
Chip przełączający	Marvell 98DX3257 lub równoważny zapewniający pełną wydajność przełączania
Porty Ethernet 10/100/1000 Mbps	48 portów RJ45 Gigabit Ethernet z obsługą auto-negocjacji (10/100/1000 Mbps)
Porty SFP+ 10Gb/s	Min. 4 porty SFP+ obsługujące moduły światłowodowe i miedziany 10 Gigabit Ethernet
Porty QSFP+ 40Gb/s	Min. 2 porty QSFP+ obsługujące moduły światłowodowe 40 Gigabit Ethernet
Port zarządzający	1 port Ethernet 10/100 Mbps RJ45 do zarządzania out-of-band
Port konsoli szeregowej	1 port szeregowy RJ45 do bezpośredniego zarządzania urządzeniem
Całkowita przepustowość non-blocking	Min. 168 Gbps (Layer 2)
Pojemność przełączania (Switching Capacity)	Min. 336 Gbps full-duplex
Forwarding Rate	Min. 235 Mpps (milion pakietów na sekundę) przy pakietach 64-bajtowych
Wydajność Layer 2 (64-bajtowe pakiety)	Min. 235 000 kpps (kilo pakietów na sekundę) przepustowość, min. 120 Gbps throughput
Wydajność Layer 3 (routing sprzętowy)	Min. 160 000 kpps przy pakietach 64-bajtowych w trybie L3HW
Tabela adresów MAC	Min. 16 000 wpisów

Obsługa VLAN	IEEE 802.1Q z obsługą min. 4094 VLAN ID, obsługa QinQ (VLAN stacking)
Spanning Tree Protocol	Sprzętowa obsługa STP, RSTP (IEEE 802.1w), MSTP (IEEE 802.1s)
Link Aggregation	Obsługa agregacji portów LACP (IEEE 802.3ad) realizowana sprzętowo
IGMP Snooping	Tak - sprzętowa obsługa IGMP v1/v2/v3 Snooping
DHCP Snooping	Tak - zabezpieczenie przed nieautoryzowanymi serwerami DHCP
Quality of Service (QoS)	Obsługa priorytetyzacji ruchu IEEE 802.1p, klasyfikacja ruchu, kolejkowanie pakietów
Access Control List (ACL)	Obsługa list kontroli dostępu dla filtrowania ruchu na poziomie Layer 2 i Layer 3
Routing IPv4	Routing statyczny, RIP, OSPF, BGP
Routing IPv6	Obsługa routingu IPv6
Jumbo Frame	Obsługa ramek Jumbo do min. 10 218 bajtów
Flow Control	IEEE 802.3x Flow Control (pause frames)
Storm Control	Ochrona przed broadcast, multicast i unicast storm
Port Mirroring	Możliwość monitorowania ruchu poprzez mirror/span portów
System operacyjny	RouterOS z licencją Level 5 lub równoważny pełnofunkcyjny system operacyjny z możliwością przełączenia w tryb SwitchOS
Interfejs zarządzania	Web GUI (HTTPS), SSH, Telnet, Serial Console, Winbox, API
Protokoły zarządzania	SNMP v1/v2c/v3, LLDP, CDP
Monitoring i diagnostyka	RMON, syslog, NetFlow, RADIUS, TACACS+
Konfiguracja backupu	Możliwość tworzenia kopii zapasowych konfiguracji i ich przywracania
Aktualizacje oprogramowania	Możliwość aktualizacji systemu operacyjnego przez sieć lub lokalne pliki
Zasilanie	Dual redundantne zasilacze wbudowane 100-240V AC, 50/60 Hz z automatycznym przełączaniem
Maksymalny pobór mocy	Nie więcej niż 60W przy pełnym obciążeniu
Typowy pobór mocy	Około 50W bez obciążenia portów SFP+/QSFP+
Chłodzenie	Aktywne chłodzenie wentylatorowe z automatyczną regulacją obrotów zależną od temperatury
Temperatura pracy	Zakres od -20°C do +60°C
Wilgotność względna	10-90% bez kondensacji
Wysokość pracy	Do 3000 m n.p.m.
MTBF	Min. 100 000 godzin
Wskaźniki LED	Wskaźniki LED dla każdego portu (Link/Activity), wskaźniki statusu zasilania, wskaźniki aktywności systemu
Funkcje bezpieczeństwa	Firewall, kontrola dostępu MAC/IP, Port Security, IEEE 802.1X (RADIUS authentication), SSH v2, zabezpieczenia DoS
Zarządzanie przepustowością	Traffic shaping, bandwidth limitation per port, Simple Queues, Queue Trees
Hot Swap	Redundantne zasilacze z możliwością wymiany na gorąco
Normy i certyfikaty	CE/RED, EAC, RoHS oraz inne wymagane certyfikaty bezpieczeństwa i kompatybilności elektromagnetycznej

Akcesoria w zestawie	2 kable zasilające IEC, zestaw śrub montażowych (K-48), uszy montażowe do rack 19", wsporniki do zarządzania kablami (cable management brackets), instrukcja obsługi
Gwarancja	Min. 12 miesięcy gwarancji producenta

1. Oferent może zaoferować urządzenie równoważne o parametrach nie gorszych niż opisane w powyższej specyfikacji.
2. W przypadku oferowania urządzenia równoważnego, Oferent zobowiązany jest wykazać spełnienie wszystkich wymaganych parametrów technicznych poprzez załączenie stosownej dokumentacji technicznej producenta.
3. Urządzenie musi posiadać system operacyjny umożliwiający pełne zarządzanie funkcjami warstwy 2 i 3, w tym routing, VLAN, QoS i mechanizmy bezpieczeństwa.
4. Przełącznik musi obsługiwać redundantne zasilanie z możliwością pracy ciągłej przy awarii jednego z zasilaczy.
5. Urządzenie musi być dostarczone w oryginalnym, nienaruszonym opakowaniu producenta wraz z wszystkimi akcesoriami standardowo dostarczonymi przez producenta.
6. Zamawiający wymaga, aby oferowane rozwiązanie umożliwiało rozbudowę o moduły SFP+ i QSFP+ zgodnie ze standardami branżowymi.
7. System operacyjny musi umożliwiać zarządzanie urządzeniem przez interfejs webowy, CLI oraz dedykowane oprogramowanie producenta.

3. Licencja na oprogramowanie Network Access Control (NAC)

Podstawowa funkcjonalność systemu NAC:

1. System musi posiadać funkcjonalność aktywnego zapobiegania dostępu do sieci nieautoryzowanych użytkowników i urządzeń końcowych.
2. System musi współpracować z urządzeniami wielu producentów (tzw. multi vendor)
3. System musi być w pełni zarządzany z poziomu interfejsu graficznego dostępnego przez przeglądarkę internetową z jednej konsoli, interfejs WEB w wersji HTML5 niewymagających obsługi dodatkowych wtyczek.
4. System musi wspierać funkcjonalność instalacji rozproszonej na wielu maszynach (serwerach) fizycznych lub wirtualnych w ramach jednej licencji.
5. System musi wspierać mechanizm DISASTER RECOVERY – tworzenia kopii lustrzanej całego systemu w celu zachowania ciągłości działania w ramach jednej licencji.
6. System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych stacji końcowych.
7. System musi umożliwiać obsługę co najmniej 250 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do przynajmniej 1 000 jednoczesnych unikatowych autoryzacji do sieci poprzez rozbudowę oferowanego rozwiązania.
8. Licencja ma być zwalniana po rozłączeniu urządzenia końcowego.
9. System musi umożliwiać obsługę jednocześnie podłączonych agentów oraz BYOD (Bring Your Own Device) co najmniej tyle samo co licencja na jednoczesne unikatowe autoryzacje do sieci w ciągu dnia.
10. System musi umożliwiać instalację na maszynie wirtualnej (VM), PaaS lub maszynie fizycznej, w tym:
 - VM – min. VMWare ESXi co najmniej w wersji 5.x, Hyper-V w wersji min 2012, Proxmox w wersji min 5.x, KVM w wersji min 7.x, Citrix XenServer w wersji min 4.x
 - Maszyny fizyczne - serwery wspierane przez producenta.
11. System musi posiadać funkcjonalność serwerów:
 - serwera RADIUS dla infrastruktury sieciowej,
 - serwera OTP dla infrastruktury VPN, Captive Portal, Tacacs+,
 - serwera SYSLOG,
 - serwera TACACS+,
 - serwera Monitoringu,

- serwera DHCP,
 - serwera polityk uwierzytelniania i kontroli dostępu 802.1X,
 - serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego.
12. System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, poprzez zapewnienie redundancji dla modułów realizujących dostęp do sieci i DHCP.
 13. System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC.
 14. System musi umożliwiać uwierzytelnianie tożsamości i urządzeń końcowych za pomocą wewnętrznej bazy i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, Google G Suite, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC.
 15. System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z zewnętrznymi systemami (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc, Microsoft Active Directory, Radius, OpenLDAP, relacyjnych baz danych (jak MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC), CheckPoint, Service Now).
 16. Podczas synchronizacji musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenia lokalnych haseł, certyfikatów, wysłania konfiguracji dostępowych poprzez email.
 17. System musi wspierać funkcjonalność API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci.
 18. System musi mieć możliwość autoryzacji protokołem NTLM z wieloma serwerami Microsoft Active Directory, także nie połączonych relacjami zaufania.
 19. System musi mieć możliwość obsługi wielu PKI dla różnych grup użytkowników.
 20. System musi posiadać funkcjonalność tworzenia kont administracyjnych z konfigurowalnym dostępem do dowolnych spośród wszystkich funkcjonalności systemu oraz do dowolnych obiektów utworzonych i/lub zarządzanych w systemie.
 21. System musi mieć możliwość zmiany parametrów kont Microsoft Active Directory (min. Login, Hasło, Imię, Nazwisko, Email, Status).
 22. System musi posiadać funkcjonalność konfiguracji praw kontroli dostępu do poszczególnych elementów menu interfejsu oraz obiektów na poziomie ich dodawania, edycji, kasowania.
 23. Interfejs graficzny systemu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim i polskim).
 24. System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP lub podsieci.
 25. System musi posiadać możliwość raportowania podłączonych tożsamości, urządzeń końcowych podłączonych do sieci, min. Tożsamość, mac adres, urządzenie końcowe, port, SSID, urządzenie sieciowe, informacja o autoryzacji oraz przydzielony Vlan z przydzielonym adresem IP.
 26. System musi zapewniać scentralizowane monitorowanie urządzeń sieciowych. W systemie musi być dostępny dedykowany interfejs graficzny, na którym dostępny jest podgląd wszystkich portów i modułów zarządzanego urządzenia.
 27. System musi umożliwiać monitoring urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP.
 28. System musi umożliwiać zbieranie danych inwentaryzacyjnych, ich zmian oraz sprawdzanie kondycji urządzeń sieciowych oraz końcowych za pomocą min. protokołu SNMP.
 29. Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu konfiguracji zmian, konfiguracji ustawień portu z zakresu min. VLANów, Autoryzacji, Statusu, Opisu.
 30. System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej.
 31. System musi posiadać możliwość konfiguracji serwera DHCP dla stworzonych podsieci IP.
 32. System musi umożliwiać konfigurację własnych szablonów przesyłanych wiadomości e-mail oraz wydruku poświadczeń dostępu do sieci.

33. System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsieciach minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3.
34. System musi posiadać funkcjonalność wysyłania zdarzeń np. do systemów SIEM minimum protokołem Syslog informacji z serwerów autoryzacji, DHCP, VPN, OTP, Tacacs+.
35. System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa lokalnie lub na udziałach zewnętrznych.
36. System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD).
37. System musi posiadać możliwość logowania w oparciu o portale społecznościowe, minimum: Facebook i Google, LinkedIn.
38. System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez email, bramkę SMS oraz zapasową bramkę SMS.
39. System musi posiadać funkcję personalizacji strony gościnnej.
40. Captive Portal musi się automatycznie dostosować formatem do podłączonego urządzenia końcowego min: komputer, tablet, telefon.
41. Captive Portal musi umożliwiać rejestracje gości potwierdzanych przez konta typu sponsor.
42. Captive Portal musi mieć możliwość włączenia dwuskładnikowego uwierzytelniania konta (OTP) minimum za pomocą tokenu wygenerowanego na Google Authenticatorze lub wysłanego przez bramkę SMS oraz zapasową bramkę SMS.
43. Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory.
44. Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory.
45. Captive Portal musi umożliwiać logowanie typu HotSpot za pomocą kodu dostępu.
46. Captive Portal musi umożliwiać tworzenie dynamicznych pól formularza rejestracyjnego, np.: pole tekstowe, lista wyboru.
47. Interfejs graficzny Captive Portalu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim, polskim, niemieckim, hiszpańskim, francuskim i ukraińskim).
48. Captive Portal musi posiadać możliwość pobrania konfiguracji dla OTP.
49. Captive Portal powinien wspierać automatyczne kasowanie wygasłych kont gościnnych: na żądanie, okresowo wg zadanej liczby dni.
50. Captive Portal powinien umożliwiać konfigurację maksymalnej ilości nieudanych logowań.
51. System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP.
52. System powinien posiadać mechanizm integracji z systemami zewnętrznymi za pomocą protokołu, min. Syslog, SNMP Trap, Rest API, w celu wykrywania anomalii, blokowania dostępu do sieci, rozłączania tożsamości/urządzenia końcowego.
53. System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny.
54. System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z RFC 5176.
55. System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych.
56. System musi obsługiwać różne metody profilowania do wykrywania typu urządzenia, systemu operacyjnego, przez co najmniej DHCP Fingerprinting, DHCP SPAN, SNMP, Vendor OUI, TCP, Active Directory, CDP/LLDP, HTTP/S, DNS, Radius, WMI, MDM, WinRM, ONVIF.
57. System musi umożliwiać integracje z zewnętrznymi rozwiązaniami typu MDM (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc).
58. System musi posiadać funkcjonalność dwuskładnikowego uwierzytelniania konta (OTP) realizowaną poprzez tworzenie tokenu w Google Authenticator i SMS, minimum na systemach: FortiGate, Pulse Secure, OpenVPN, Palo Alto, Cisco ASA.

59. System musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa co najmniej:
- Czy system jest aktualny z możliwością automatycznego naprawienia niezgodności
 - Czy włączony jest firewall
 - Czy jest uruchomiony system antywirusowy i aktualna baza sygnatur
 - Czy jest włączone szyfrowanie dysku systemowego
 - Czy urządzenie końcowe jest podłączone do domeny Microsoft Active Directory
 - Czy na dysku znajdują się pliki lub katalogi wskazane przez administratora
 - Czy w systemie są uruchomione procesy wskazane przez administratora
 - Czy w systemie są uruchomione usługi wskazane przez administratora z możliwością automatycznego naprawienia niezgodności
 - Czy w systemie są wpisy w rejestrze wskazane przez administratora wg klucza, a także pod kątem:
 - Wartości klucza rejestru
 - Typu wartości: Number, String, Version
60. System musi posiadać możliwość wysyłania komunikatów do użytkowników min za pomocą agenta i Captive Portal.
61. System musi współpracować z serwerem tokenów.
62. System musi posiadać mechanizm autokonfiguracji sieci (autokonfigurator sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania pracowników działu IT dla systemów co najmniej:
- Microsoft Windows
 - Mac OS
 - iOS
 - Android
63. System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfigurator sieci).
64. System musi wspierać protokół IPv6 min dla konsoli SSH, komunikacji RADIUS, NTP, SNMP, komunikację z Microsoft Active Directory.

Mechanizmy uwierzytelniania

1. System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS.
2. System musi obsługiwać uwierzytelnianie w oparciu o następujące protokoły:
 - MAC,
 - PAP/ASCII,
 - CHAP,
 - SNMP,
 - 802.1X.
3. wraz z możliwością wyboru szczegółowego sposobu uwierzytelniania np. IEEE 802.1x (PEAP), IEEE 802.1x (EAP-TLS), IEEE 802.1x (EAP-TTLS), MAC (PAP), MAC (CHAP), MAC (MD5), TEAP, itp.
4. System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości.
5. System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych.
6. System musi wspierać implementację protokołu 802.1X z różnymi suplikantami (min. Windows XP, Windows Vista, Windows 7, Windows 8 i 8.1, Windows 10, Windows 11, Apple Mac OS X Supplicant, Apple iOS Supplicant, Google Android Supplicant, Ubuntu Supplicant).
7. System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły:
 - Tożsamość/Urządzenie końcowe,
 - Grupa tożsamości/urządzeń końcowych,
 - Parametry urządzeń końcowych, min: system operacyjny, wersja,
 - Atrybuty Active Directory,
 - Jednostka organizacyjna tożsamości/urządzeń końcowych,

- Urządzenia sieciowe sieci przewodowej, bezprzewodowej,
 - Grupy urządzeń sieciowych,
 - Porty urządzeń sieciowych,
 - Grupy portów urządzeń sieciowych,
 - Jednostka organizacyjna portów,
 - Punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID),
 - Data, czas ważności polityki,
 - Wewnętrzny Captive Portal,
 - Metoda autoryzacji.
8. System musi umożliwiać przypisywanie sieci VLAN i/lub atrybutów RADIUS zwrotnych VSA podczas etapu autoryzacji, np.: ACL, Quality of Service, co najmniej następujących producentów: Cisco Networks, Aruba Networks, Extreme Networks, Hewlett Packard Enterprise, Juniper Networks, Ruckus Networks, MicroTik, Ubiquiti Networks.
 9. System musi wspierać funkcjonalność *IP-to-ID Mapping*, polegającą na łączeniu tożsamości, adresu IP, adresu MAC.
 10. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu tożsamości, urządzenia końcowego, adresu MAC podczas etapu autoryzacji, minimum za pomocą mechanizmów SNMP, DHCP, NMAP, WMI.
 11. System musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej konsoli.
 12. System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV.
 13. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o pojedynczy obiekt i/lub w postaci zbiorczego pliku w formacie CSV.
 14. System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach.
 15. System musi umożliwiać tworzenie hasła dnia, dla tożsamości zarejestrowanych przez wewnętrzny Captive portal.
 16. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o urządzenie końcowe i/lub w postaci zbiorczego pliku w formacie CSV. Lokalna baza urządzeń końcowych musi być tworzona per urządzenie końcowe na podstawie unikalnego adresu MAC.
 17. System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów MAC.
 18. System musi wspierać funkcjonalność różnych typów autoryzacji na pojedynczym porcie urządzenia sieciowego: min. autoryzację pojedynczą, autoryzację wielokrotną, uwierzytelnianie urządzeń typu Voice VLAN, równoczesną obsługę różnych typów autoryzacji skonfigurowanych na porcie i/lub autoryzację poprzez portal www.
 19. System musi umożliwiać integrację z EDUROAM w zakresie autoryzacji użytkowników.
 20. System musi umożliwiać przesyłanie zwrotnych parametrów do systemów zewnętrznych i/lub urządzeń sieciowych za pomocą protokołu min. HTTP zawierających min. informacje o identyfikatorze tożsamości, adresie MAC oraz IP.

Obsługa serwerów certyfikatów CA

1. System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA (Certificate Authority) oraz zapewniać współpracę z zewnętrznymi serwerami CA.
2. Funkcja CA zintegrowana oraz zewnętrzna musi zapewniać przynajmniej następujące funkcjonalności:
 - możliwość generowania i podpisywania certyfikatów dla tożsamości i urządzeń końcowych.
 - możliwość bezpiecznego przechowywania certyfikatów tożsamości i urządzeń końcowych.
 - Możliwość generowanie certyfikatów za pomocą protokołu SCEP (Simple Certificate Enrollment Protocol).
 - usługę OCSP (Online Certificate Status Protocol).

Obsługa serwerów DHCP

1. System musi posiadać funkcję zintegrowanego serwera DHCP.
2. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu urządzenia końcowego, adresu MAC podczas pracy serwera DHCP.
3. System musi zapewniać przynajmniej następujące funkcjonalności serwera DHCP:
 - Uruchamianie usługi dla wybranych podsieci,
 - Przypisanie ustalonego adresu IP dla adresu MAC.
 - Przypisanie różnych adresów IP dla konkretnego adresu MAC z różnych podsieci,
 - Możliwość zwracania adresów IP wyłącznie dla wybranej i wcześniej zdefiniowanej grupy adresów MAC,
 - Możliwość określania braku dostępu dla wybranych adresów MAC,
 - Monitoring obciążenia puli dynamicznych, poziomu decline, braku konfiguracji, ograniczenia dla zdefiniowanej grupy adresów MAC,
 - Możliwość ustawienia dodatkowych parametrów zwrotnych przesyłanych przez serwer DHCP,
 - Możliwość podglądu aktualnego obciążenia podsieci w widoku graficznym adresacji IP dla przydziału statycznego i dynamicznego,
 - Możliwość zmiany przydziału dynamicznego na statyczny bez restartu usługi,
 - Dokonywanie zmian bez konieczności wyłączania usług.

Obsługa serwerów TACACS+

System musi umożliwiać tworzenie grup uprawnień do kontroli dostępu urządzeń sieciowych:

1. System musi umożliwiać grupowanie urządzeń końcowych oraz administratorów.
2. System musi umożliwiać tworzenia haseł administratorom.
3. System musi umożliwiać tworzenie listy komend uprawnień dla administratorów
4. System musi raportować o wszystkich wydanych komendach na kontrolowanych urządzeniach sieciowych.
5. System musi umożliwiać zmianę hasła administratora z poziomu urządzenia sieciowego wg ustalonego czasu.
6. System musi umożliwiać logowanie za pomocą poświadczeń Microsoft Active Directory.
7. System musi wspierać logowanie administratorów za pomocą tokenów OTP.
8. System musi umożliwiać przypisywanie atrybutów zwrotnych VSA podczas etapu autoryzacji.

Raportowanie i monitoring

System musi umożliwiać generowanie raportów oraz monitoring przynajmniej następujących parametrów:

1. Monitoring autoryzacji.
2. Monitoring dla zdarzeń systemowych.
3. Monitoring dla zdarzeń DHCP.
4. Monitoring dla tożsamości.
5. Monitoring dla urządzeń końcowych.
6. Monitoring dla urządzeń sieciowych.
7. Raport stanu systemu (min. szczegółowy dane z nodów systemu, wykorzystanie polityk dostępu, ostatnie krytyczne błędy, niski status komponentów drukarek, ostanie aktywności serwerów autoryzacji, DHCP, urządzeń sieciowych uwzględniający ostatnią aktywność autoryzacji, obciążenie procesora, pamięci, zmiany konfiguracji, obciążenie serwera DHCP, autoryzacji, obciążenia portów – przepustowość, liczby autoryzacji) dostępny min. z poziomu konsoli CLI, interfejsu WWW oraz raportu email.
8. Raport ze zdarzeń logowania z informacją o nadanym adresie IP.
9. Raport stanu systemu z poziomu konsoli CLI min. obciążenie procesora, pamięci, przestrzeni dyskowej, działania usług.
10. Raport z logów DHCP z informacją o polityce dostępu logowania do sieci.
11. System musi posiadać mechanizm graficznego podglądu stanu przełącznika i portów w czasie rzeczywistym.
12. System musi wspierać mechanizm graficznego podglądu urządzeń sieciowych działających w stosie.
13. System musi wspierać mechanizm graficznego podglądu wykrytych niezgodności vlanów w urządzeniach sieciowych działających w środowisku.
14. System musi wspierać funkcjonalność graficznego monitoringu zasobów zarządzanych drukarek sieciowych.

15. System musi posiadać mechanizm graficznego podglądu stanu tożsamości oraz urządzeń końcowych w tym podstawowe dane, ostatnia autoryzacja do sieci, wykorzystanie urządzeń końcowych wg tożsamości na dzień, parametry urządzeń końcowych, min: system operacyjny, wersja.
16. System musi umożliwiać podgląd tożsamości, urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych, kontrolerów wifi.
17. Raport z logów OTP z informacją o poprawnej i błędnej autoryzacji, wysłanego tokenu przez bramkę SMS.
18. Raport zdarzeń Microsoft Active Directory, minimum:
 - Logowania, wylogowania z system w tym błędne logowania
 - Logowania do sieci 802.1X

Alarmy

1. System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą:
 - wiadomości e-mail,
 - Syslog,
 - notyfikacji systemowych.
2. Alarmy mogą być generowane w sytuacjach, min:
 - Ilości obsługiwanych transakcji RADIUS,
 - Opóźnienie obsługi transakcji RADIUS,
 - Statusu krytycznego modułów.
3. System musi posiadać zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:
 - badanie łączności IP za pomocą ping, traceroute,
 - tcpdump protokołów RADIUS, TACACS+,
 - wyszukiwanie zdarzeń RADIUS z uwzględnieniem:
 - nazwy użytkownika,
 - adresu MAC,
 - statusu uwierzytelnienia (udana lub nieudana),
 - powodu, jeżeli uwierzytelnienie nieudane,
 - zakresu czasowego, co do dnia, godziny i minuty,
 - wykonanie zdalnego polecenia na urządzeniu sieciowym.

Wymagania dotyczące wdrożenia i harmonogram ramowy:

- Dostawa, instalacja, konfiguracja wstępna i zalicencjonowanie produktu w środowisku klienta.
- Podstawowa konfiguracja Systemu NAC (integracja z domeną, konfiguracja urzędu certyfikacji, uruchomienie HA).
- Konfiguracja urządzenia firewall (dodatkowo VLAN-u gościnnego, ustawienie polityk, etc.).
- Import urządzeń końcowych i tożsamości (z AD oraz dostarczonych przez Zamawiającego list).
- Integracja dostarczanych urządzeń sieciowych (switche, AP) z NACVIEW, w ramach funkcjonalności dostępnych na urządzeniach.
- Uruchomienie uwierzytelniania w oparciu o 802.1X (EAP-TLS) na urządzeniach końcowych wzorcowych po jednym z każdej serii, testy.
- Uruchomienie uwierzytelniania w oparciu o adres MAC w korelacji z innymi możliwościami np. DHCP, SNMP, skan portów, testy.
- Przeprowadzenie szkolenia dla administratorów z konfiguracji i administrowania Systemem NAC. Dwudniowe szkolenie online zdalne dla do 4 osób po 6h dziennie.
- Przygotowanie dokumentacji powykonawczej opisującej wykonane prace oraz sposób konfiguracji poszczególnych urządzeń do 14 dni po zakończeniu wdrożenia.

Szkolenia/warsztaty:

- Wykonawca zapewni 2-dniowe warsztaty (2 dni x 6h) w zakresie użytkowania i administrowania wdrożonym systemem NAC

- Warsztaty zostaną przeprowadzone dla maksymalnie 4 osób i będą uwzględniać informacje z zakresu wdrożonego systemu NAC
- Po zakończeniu warsztatów, uczestnicy otrzymają zaświadczenia potwierdzające uczestnictwo w szkoleniach/warsztatach oraz nabycie umiejętności obsługi systemu NAC
- Warsztaty odbędą się w formie zdalnej.
- Wykonawca dla każdego uczestnika dostarczy materiały szkoleniowe w języku polskim w postaci elektronicznej.
- Szczegółowy plan, zakres i terminy szkoleń/warsztatów zostaną uzgodnione przez Wykonawcę z Zamawiającym

Licencja wsparcia technicznego producenta oprogramowania:

Wykonawca dostarczy wraz dożywotną licencją systemu NAC – 36 miesięczną licencję na wsparcie producenta oprogramowania. Licencja ta powinna obejmować minimum:

- Kontakt mailowy z działem wsparcia technicznego w celu rozwiązania problemów związanych z wdrożeniem lub obsługą systemu NAC
- Rozwiązywanie powtarzalnych i rozwiązywalnych problemów związanych z oprogramowaniem a także wsparcie przy identyfikacji problemów trudnych do powtórzenia.
- Wsparcie przy rozwiązywaniu problemów oraz pomoc w określaniu parametrów dla konfiguracji oprogramowania oraz wstępne obejścia dla wykrytych problemów.
- Dostęp do dokumentacji i instrukcji na stronie internetowej.
- Dostęp do aktualizacji i poprawek, które powinny być dostępne z poziomu interfejsu oprogramowania.

4. Serwer RACK + Win Serv 2022 MS Win Serv 2022 CAL User

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	• Obudowa serwerowa do montażu w szafie RACK 19" o wysokości max 1U • Obudowa powinna posiadać panel LCD umieszczony na froncie obudowy i pozwalający jednoznacznie stwierdzić czy system działa poprawnie i pokazujący podstawowe stany działania serwera (umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze). • Obudowa z możliwością wyposażenia w kartę do bezpośredniej komunikacji z urządzeniem mobilnym. • serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI. • W obudowie powinien być zainstalowany zestaw redundantnych wentylatorów.
Zasilanie	• W obudowie powinien być zainstalowany zestaw redundantnych zasilaczy o mocy co najmniej 700W w standardzie Titanium każdy wymiennych podczas pracy
Płyta główna	• Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • musi być wyposażona w zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust), • Musi umożliwiać utworzenie bezpiecznego profilu w oparciu o konfigurację sprzętową oraz o konfigurację wewnętrznego oprogramowania komponentów serwera. • Zintegrowany z płytą główną moduł TPM w wersji co najmniej 2.0
Chipset	• Dedykowany przez producenta procesora do pracy w serwerach dwuprocessorowych.

Procesor	Dwa procesory typu skalowalnego z uwagi na licencjonowanie posiadające dokładnie po 8 rdzeni działające co najmniej z częstotliwością 2.6GHz i dające w teście Passmark dostępnym na stronie https://www.cpubenchmark.net/ wynik nie mniejszy niż 40 800 dla wersji Dual CPU na dzień 28.10.2025 r.
RAM	- Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci taktowaną przynajmniej z częstotliwością 5200MT/s przy użyciu odpowiednich procesorów. 128GB pamięci RAM w modułach 32GB RDIMM przygotowanych na działanie z częstotliwością co najmniej 5600MT/s
Dyski twarde	- Serwer ma mieć przewidzianą przez producenta możliwość dodania modułu pozwalającego na startowanie systemu z kart SD lub dysków M.2 skonfigurowanych w RAID1 nie zajmujących slotów na dyski. - Miejsce na co najmniej 8 dysków w rozmiarze 2.5" wymienne bez wyłączenia systemu. - Zainstalowane co najmniej 2 dyski minimum 960GB SSD SATA Read Intensive 6Gbps Hot-plug
Kontroler RAID	Serwer powinien posiadać kontroler RAID umożliwiający konfigurację RAID 0,1,5,10,50,6 posiadający co najmniej 8GB pamięci cache zabezpieczonej przed awarią prądu.
Interfejsy sieciowe/FC/SAS	- Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT, 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Elementy montażowe	- Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych - Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych
Bezpieczeństwo	- Zatrask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. - Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. - Możliwość wyłączenia w BIOS funkcji przycisku zasilania. - BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła - Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. - Moduł TPM 2.0 - Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera - Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem - Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
Kontroler eksploatacji serwera	- Serwer powinien być standardowo wyposażony w kontroler eksploatacji - Konfigurowanie ustawień BIOS i sprzętu. - Uproszczoną instalację systemów operacyjnych z wbudowanymi sterownikami, z opcją instalacji bezobsługowej dla systemów Microsoft Windows i Red Hat Enterprise Linux 7.

	• Aktualizację oprogramowania niezależnie od systemu operacyjnego, z możliwością przywrócenia poprzedniej wersji. • Ciągłą dostępność diagnostyki bez zależności od dysku twardego, z automatyczną aktualizacją oprogramowania podczas wymiany komponentów. • Usunięcie danych związanych z serwerem i pamięcią masową na wybranych komponentach. Możliwe jest usunięcie informacji z BIOS. • Dostarczenie informacji o bieżącej i fabrycznej konfiguracji systemu. • Udostępnianie logów sprzętowych w celu rozwiązywania problemów. • Zdalne zarządzanie cyklem życia serwera co najmniej za pomocą interfejsu WS-Man • Konfigurację ustawień sieci dla wbudowanej karty NIC, w tym ustawienia VLAN. • Wykonywanie diagnostyki pamięci, urządzeń we/wy, procesora i dysków fizycznych. • Aktualizację komponentów systemu za pomocą repozytoriów lub pojedynczych pakietów DUP. • Powrót do poprzedniej wersji oprogramowania układowego. • Umożliwia zabezpieczenie konfiguracji systemu - "System Configuration Lockdown mode" • Automatyczną aktualizację oprogramowania i konfiguracji wymienionych części. • Trwałe usunięcie danych przed ponownym wykorzystaniem lub wycofaniem systemu. • Obsługę różnych metod aktualizacji, za pomocą różnych źródeł, takich jak FTP, udziały sieciowe (CIFS, NFS, HTTP, HTTPS) lub lokalne napędy USB/DVD
Karta Zarządzania	• Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: ○ - zdalny dostęp do graficznego interfejsu Web karty zarządzającej ○ - szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika ○ - możliwość podmontowania zdalnych wirtualnych napędów ○ - wirtualną konsolę z dostępem do myszy, klawiatury ○ - wsparcie dla IPv6 - wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH ○ - możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz. ○ - możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer ○ - integracja z Active Directory ○ - możliwość obsługi przez ośmiu administratorów jednocześnie ○ - Wsparcie dla automatycznej rejestracji DNS - wsparcie dla LLDP ○ - wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej ○ - możliwość podłączenia lokalnego poprzez złącze RS-232. ○ - możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy. ○ - Monitorowanie zużycia dysków SSD ○ - możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi, ○ - Automatyczne zgłaszanie alertów do centrum serwisowego producenta ○ - Automatyczne update firmware dla wszystkich komponentów serwera ○ - Możliwość przywrócenia poprzednich wersji firmware ○ - Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych • - Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram.
Oprogramowanie do zarządzania	Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania: - wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych; - możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta;

	- wsparcie dla protokołów – WMI, SNMP, IPMI, WSMAN, Linux SSH; - możliwość oskryptowywania procesu wykrywania urządzeń; - możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram; - szczegółowy opis wykrytych systemów oraz ich komponentów; - możliwość eksportu raportu do CSV, HTML, XLS; - grupowanie urządzeń w oparciu o kryteria użytkownika; - automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń; - szybki podgląd stanu środowiska; - podsumowanie stanu dla każdego urządzenia; - szczegółowy status urządzenia/elementu/komponentu; - generowanie alertów przy zmianie stanu urządzenia; - filtry raportów umożliwiające podgląd najważniejszych zdarzeń; - integracja z service desk producenta dostarczonej platformy sprzętowej; - możliwość przejścia zdalnego pulpitu; - możliwość podmontowania wirtualnego napędu; - kreator umożliwiający dostosowanie akcji dla wybranych alertów; - możliwość importu plików MIB; - przesyłanie alertów „as-is” do innych konsol firm trzecich; - aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania); - możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta; - możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów; - moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjny sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCIe i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie gwarancji, adresy IP kart sieciowych.
Aplikacja do zarządzania	Aplikacja mobilna do zarządzania serwerami powinna umożliwiać: • Monitorowanie stanu serwerów, w tym odczyt parametrów zdrowia, inwentarza i konfiguracji. • Konfigurowanie ustawień serwera, takich jak parametry sieci, hasła administratora i kolejność urządzeń rozruchowych. • Bezpośrednią komunikację z kontrolerem serwera za pomocą technologii bezprzewodowej. • Zdalne zarządzanie serwerami poprzez połączenie z konsolą zarządzania. • Pobieranie informacji o serwerach takich jak inwentarz, status, alerty oraz logi. • Konfigurowanie serwerów zdalnie. • Wysyłanie poleceń sterowania zasilaniem i innych poleceń. • Otrzymywanie powiadomień o alertach z systemów zarządzania. • Pobieranie informacji o gwarancji. • Uruchamianie zewnętrznych aplikacji, takich jak klienty zdalnego pulpitu. • Zabezpieczenie danych w aplikacji poprzez szyfrowanie z użyciem klucza specyficznego dla urządzenia. • Opcjonalne zabezpieczenie dostępu do aplikacji za pomocą hasła i biometrii. • Automatyczne wylogowanie w przypadku braku aktywności. • Połączenie z serwerami za pomocą technologii Bluetooth Low Energy (BLE) lub Wi-Fi. • Wyświetlanie szczegółowych informacji o serwerze oraz dzienników. • Otrzymywanie automatycznych powiadomień z konsoli zarządzania. • Przypisywanie adresów IP i modyfikowanie haseł. • Konfigurowanie atrybutów BIOS. • Wyłączanie i włączanie serwera oraz dostęp do konsoli systemowej. • Pobieranie danych z systemów zarządzania typu "jeden do wielu". • Wyświetlanie certyfikatu systemu w celu weryfikacji tożsamości przy pierwszym połączeniu. Aplikacja powinna być dostępna do pobrania w popularnych sklepach z aplikacjami • Kryterium stanowi dodatkową punktację.

Opcjonalny moduł do podłączenia aplikacji mobilnej	Moduł powinien umożliwiać następujące funkcjonalności: • Bezprzewodową komunikację z urządzeniami mobilnymi wykorzystując technologie Bluetooth Low Energy (BLE) lub Wi-Fi. • Zapewnienie fizycznego bezpieczeństwa poprzez wymóg fizycznej obecności administratora przy serwerze i naciśnięcia przycisku aktywacyjnego na serwerze lub wirtualnego przycisku na wyświetlaczu LCD w przypadku obudów. Bez aktywacji nie jest możliwa wymiana danych. • Ograniczenie zasięgu komunikacji BLE przed uwierzytelnieniem do około 1 metra, a po uwierzytelnieniu do około 5 metrów. Zasięg Wi-Fi wynosi około 5 metrów. • Ograniczenie liczby jednoczesnych połączeń BLE do jednego urządzenia mobilnego na serwer. • Blokowanie dostępu po wielokrotnych próbach połączenia z użyciem nieprawidłowych danych uwierzytelniających, co skutkuje koniecznością ręcznej reaktywacji modułu. • Zabezpieczenie komunikacji BLE z wykorzystaniem protokołu TLS 1.2, wymiany kluczy Diffie-Hellmana (2048-bitowe lub większe liczby pierwsze) oraz szyfrowania AES (128-bitowe klucze symetryczne). • Wykorzystanie trybu szyfrowania GCM z unikalnymi numerami sekwencyjnymi w celu ochrony przed nieautoryzowaną ingerencją, ujawnieniem informacji oraz atakami typu replay. • Aktywację Wi-Fi tylko w przypadku komunikacji wymagającej większej przepustowości lub komunikacji opartej na IP. • Generowanie nowego, losowego klucza WPA2PSK za każdym razem, gdy aktywowane jest Wi-Fi, który jest przesyłany do aplikacji mobilnej za pośrednictwem połączenia BLE. • Uwierzytelnianie użytkowników za pomocą tych samych danych uwierzytelniających co do kontrolera zdalnego dostępu. • Identyfikację serwera za pomocą certyfikatu PKI w formacie x509 oraz wyświetlanie znacznika serwisowego podczas łączenia. • Możliwość aktywacji diody ID LED w celu potwierdzenia połączenia z właściwym systemem. ○ Umożliwienie administratorom zdalnego wyłączenia i włączania serwerów za pomocą poleceń.
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver na terenie Polski według normy wprowadzonej w 2019 roku - Wykonawca złoży dokument potwierdzający spełnianie wymogu. ○ Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.
Dokumentacja użytkownika	• Zamawiający wymaga dokumentacji w języku polskim lub angielskim. ○ Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

Warunki gwarancji	• Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 36 miesięcy. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. • Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. • Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. • Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. • Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. • Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. • Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: ○ Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. ○ Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. ○ Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. ○ Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. ○ Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. • Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.
--------------------------	--

Portal wsparcia produktu	W ramach wsparcia technicznego wymagana jest usługa polegająca na przygotowaniu i dostarczeniu spersonalizowanego panelu w chmurze Usługa powinna pozwalać na identyfikowanie priorytetów i potencjalnych zagrożeń technicznych sprzętu co pomoże w podejmowanie właściwych działań. Usługa powinna spełniać następujące założenia/funkcje: - Proaktywne zarządzanie priorytetami usług serwisowych w tym graficzną reprezentację poziomu zagrożeń. - Możliwość personalizacji widoku przez członków zespołu do zarządzanych przez nich lokalizacji i zasobów. - Dostęp do szczegółów dotyczących sprzętu i oprogramowania, w tym incydentów krytycznych, wsparcia technicznego, eskalacji, konserwacji na miejscu, poziomów kodu, poradników bezpieczeństwa i technicznych, zakresu wsparcia, wymiany części, łączności urządzeń i bram. - Dostęp do danych historycznych i analiz na potrzeby planowania IT
Aplikacja do zarządzania wsparciem	• Oprogramowanie producenta połączone z oficjalnym działem wsparcia technicznego, automatycznie tworzące zgłoszenia serwisowe w przypadku awarii. • Zgłoszenia serwisowe zgłaszane przez aplikację muszą być traktowane na równi z tradycyjnym zgłoszeniem serwisowym przez dział techniczny producenta serwera. • Oprogramowanie powinno być dostępne w postaci aplikacji na systemy Windows lub linux lub w postaci maszyny wirtualnej potrafiącej obsłużyć jednocześnie wiele serwerów. • Konfiguracja i zaoferowany poziom wsparcia powinien po wystąpieniu awarii urządzenia automatycznie zakładać zlecenie serwisowe w dziale wsparcia producenta, poinformować o tym za pomocą wiadomości e-mail, a następnie dział wsparcia powinien się kontaktować z klientem w celu rozwiązania problemu. • Oprogramowanie musi współpracować z kartą do zarządzania w urządzeniu, która będzie działać niezależnie od zainstalowanego systemu operacyjnego, posiadająca dedykowane port RJ-45 Gigabit. Karta musi umożliwiać podmontowanie zdalnych wirtualnych napędów oraz wirtualną konsolę z dostępem do myszy, klawiatury. • Oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające: • - Proaktywne, zautomatyzowane wykrywanie problemów, tworzenie zgłoszeń i wysyłanie powiadomień. • - Predykcyjna analiza i wykrywanie awarii dysków twardych i płyt głównych serwerów. • - Szybsze rozwiązywanie problemów dzięki zdalnemu dostępowi i bezpiecznej dwukierunkowej komunikacji między serwisem producenta serwera, a środowiskiem klienta. • upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, • - możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS'u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji: • poprawkach i usprawnieniach dotyczących aktualizacji • dacie wydania ostatniej aktualizacji • prioritycie aktualizacji • zgodność z systemami operacyjnymi • jakiego komponentu sprzętu dotyczy aktualizacja • wszystkie poprzednie aktualizacje z informacjami jak powyżej • wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne • - możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga.

	- rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr) - sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania) - dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml - raport uwzględniający informacje o: sprawdzaniu aktualizacji, znalezionych aktualizacjach, zainstalowanych aktualizacjach z dokładnym rozbiorem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku *.xml od razu spakowany z rozszerzeniem *.zip. Raport musi zawierać z dokładną datą (dd-mm-rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku.
System operacyjny i licencje dostępu	- Zainstalowany system operacyjny Windows Server Standard 2025 lub równoważny pokrywający zgodnie z warunkami licencji wszystkie rdzenie zainstalowanych procesorów. 40 sztuk licencji dostępowych na użytkownika dedykowane do ww. wersji systemu operacyjnego

5. Macierz do systemów wdrażanych w ramach projektu

Obudowa	Obudowa RACK 2U powinna pozwalać na zamontowanie 24 dysków 2.5" Macierz i serwer (pkt.4) muszą pochodzić od tego samego producenta)
Kontrolery	Macierz powinna posiadać dwa redundantne kontrolery. W każdym z kontrolerów powinno być dostępne po 16GB pamięć cache zapisu mirrorowanej między kontrolerami, zabezpieczonej na wypadek awarii prądu przez min. 72h. W każdym z kontrolerów powinno być dostępne dwa porty iSCSI w standardzie SFP28 pracujące z prędkością do 25GB do macierzy należy dołączyć 2 kable SFP28 to SFP28 przeznaczone do pracy z urządzeniem przez producenta o długości minimum 2 metry.
Dyski	W macierzy powinny być zainstalowane co najmniej trzy dyski o pojemności co najmniej 1.92TB SSD SAS 24Gbps.
Funkcjonalności	Macierz musi posiadać możliwość obsługi standardowych poziomów RAID - 0, 1, 5, 10 lub parzystości opartej na przestrzeniach dyskowych w ramach tego samego rozwiązania - wybór podczas konfiguracji Wsparcie dla autotieringu do trzech tierów oraz musi wspierać thin provisioning i snapshoty w standardzie redirect on write i szyfrowanie dysków.
Zarządzanie	Macierz musi dawać możliwość zarządzania zarówno z interfejsu graficznego obsługującego HTML5 jak i CLI. Obsługa z aplikacji opartej na technologii JAVA jest wykluczona Powiadamianie mailem o awarii, umożliwiające maskowanie mapowanie dysków. Macierz powinna zostać dostarczona z licencją umożliwiającą utworzenie minimum 512 LUN"ów oraz 1024 kopii migawkowych na całą macierz. Licencja zaoferowanej macierzy powinna umożliwiać podłączanie minimum 8 hostów bez konieczności zakupu dodatkowych licencji. Konieczne jest posiadanie automatycznego, bez interwencji człowieka, rozkładania danych między dyskami poszczególnych typów (tzw. auto-tiering). Dane muszą być automatycznie przemieszczane między różnymi typami dysków. Możliwość wykorzystania dysków SSD jako cache macierzy, możliwość rozbudowy pamięci cache do min. 4TB poprzez dyski SSD. Macierz musi mieć możliwość obsługi CLI API, Redfish/Swordfish REST API
Replikacja	W przypadku macierzy FC lub iSCSI macierz musi mieć możliwość asynchronicznej replikacji danych do drugiej takiej samej macierzy w innej lokalizacji. Do uruchomienia tej funkcjonalności nie powinno być potrzeby użycia licencji z poza oferty
Macierz musi posiadać wsparcie dla oprogramowania	VMware Site Recovery Manager VMware vSphere (ESXi) vCenter VMware Site Recovery Manager Microsoft Hyper-V

	Wsparcie dla systemów Windows 2022, 2019 and 2016 RHEL 8.2 and 7.8 SLES 15.2 and 12.5 VMware 7.0 and 6.7 Citrix XenServer 8.x and 7.x
Certyfikaty	Urządzenie musi być wyprodukowane zgodnie z normą ISO-9001:2015 oraz ISO-14001. Urządzenie musi posiadać deklarację CE.
Oprogramowanie do monitorowania	Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z posiadaną platformą wirtualizacji VMware. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności: • Monitoring: ○ ilość podłączonych oraz rozłączonych systemów ○ stan podłączonych urządzeń ○ informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów ○ Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia ○ informacje o statusie gwarancji dla poszczególnych urządzeń ○ informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń ○ informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. ○ Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych ○ Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. ○ Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. ○ Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. ○ Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. ○ Monitoring parametrów serwerów z informacją o minimum: ▪ Obciążeniu procesora ▪ Zużyciu pamięci RAM ▪ Temperaturze procesorów ▪ Temperaturze powietrza wlotowego ▪ Zużyciu prądu ▪ Zmianach w fizycznej konfiguracji serwera ▪ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ○ Monitoring parametrów pamięci masowych z informacją o minimum: ▪ Opóźnieniach ▪ IOPS ▪ Przepustowości ▪ Utylizacji kontrolerów ▪ Pojemność całkowita i dostępna ▪ Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów. ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ▪ Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata ▪ Informacje o poziomie redukcji danych ▪ Informacje o statusie replikacji oraz snapshotów ○ Monitoring parametrów przełączników sieciowych z informacją o minimum: ▪ Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny ▪ Stanie komponentów: zasilacze, wentylatory

	▪ Podłączonych hostach ▪ Ilości i statusu portów ▪ Utylizacji procesora ▪ Utylizacji poszczególnych portów ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. • Aktualizacja firmware ○ możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiązań HCI, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizacji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania • Raporty ○ Możliwość generowania raportów dla serwerów zawierających informację o: ▪ Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej ▪ Średnim obciążeniu: procesorów, pamięci RAM, IO, ○ Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: ▪ Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji ○ Generowanie raportów do plików CSV i PDF • Cyberbezpieczeństwo ○ Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. ○ Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. ○ Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. ○ Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. • Wspierane urządzenia ○ Urządzenie Producenta dostarczane w ramach postępowania ○ Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) • Wirtualny asystent ○ Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; • Możliwość rozszerzenia funkcjonalności ○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. • Inne Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android
Warunki gwarancji	• 3 lata gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia - zgłoszenia przyjmowane 7 dni w tygodniu w trybie 24/7. • Gwarancja musi obejmować całość rozwiązania nie powinno być tak aby jakaś część tego rozwiązania nie podlegała gwarancji. • Możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta. • Producent musi dawać możliwość rozszerzenia gwarancji do 7-miu lat • Podczas trwania gwarancji producent powinien zapewnić narzędzia i procesy do proaktywnej oceny stanu technicznego oraz automatycznego zgłaszania usterek bez ingerencji człowieka.

	- Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzeń. - Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. - Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, a uszkodzony dysk twardy pozostaje u Zamawiającego. - Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
--	--

6. Macierz do kopii zapasowych

PARAMETR TECHNICZNY	MINIMALNE WYMAGANIA / OPIS SZCZEGÓŁOWY
Typ urządzenia	Serwer NAS (Network Attached Storage) z redundantnym zasilaniem, przeznaczony do montażu w szafie rack 19"
Obudowa	Rack 2U z systemem hot-swap, umożliwiającą wymianę komponentów bez wyłączania urządzenia
Procesor	Intel Celeron czterordzeniowy / czterowątkowy o architekturze 64-bit x86, taktowanie w trybie burst do min. 2,9 GHz, obsługa technologii Intel AES-NI (sprzętowe szyfrowanie)
Architektura procesora	64-bitowa x86
Układ graficzny	Zintegrowany Intel UHD Graphics z obsługą akceleracji sprzętowej
Pamięć RAM zainstalowana	4 GB DDR4 SODIMM
Maksymalna pojemność pamięci RAM	Możliwość rozbudowy do min. 16 GB (2 sloty SODIMM DDR4)
Pamięć Flash	Min. 4 GB z obsługą dual boot OS protection (ochrona systemu operacyjnego)
Liczba zatok dyskowych	12 zatok 3,5" z obsługą dysków SATA 6Gb/s i 3Gb/s
Kompatybilność dysków	Dyski twarde 3,5" SATA, dyski twarde 2,5" SATA, dyski SSD 2,5" SATA
System hot-swap dysków	Tak - wszystkie zatoki z możliwością wymiany dysków na gorąco
Dyski twarde w zestawie	4 sztuki dysków twardych SATA o pojemności min. 8 TB każdy (łącznie min. 32 TB pojemności surowej)
Typ dysków	Dyski klasy NAS lub Enterprise, przeznaczone do pracy ciągłej 24/7
Obsługa cache SSD	Tak - możliwość instalacji dysków cache SSD dla przyspieszenia operacji
Sloty M.2	Opcjonalnie poprzez adapter PCIe
Obsługiwane poziomy RAID	RAID 0, 1, 5, 6, 10, 50, 60 oraz JBOD
Porty sieciowe	Min. 2 porty Ethernet 2,5 Gigabit (2.5GbE/1GbE/100M/10M) z obsługą Jumbo Frame
Wake on LAN	Tak
Slot PCIe	Min. 1 slot PCIe Gen 3 x2 dla kart rozszerzeń (np. karta sieciowa, adapter M.2)

Porty USB 3.2 Gen 2	Min. 2 porty USB 3.2 Gen 2 Type-A (10Gbps)
Porty USB 2.0	Min. 2 porty USB 2.0
Port HDMI	1 port HDMI 1.4b z obsługą rozdzielczości 4K
Wskaźniki LED	Wskaźniki statusu dla każdego z 12 dysków, status systemu, LAN, ekspansja, zasilanie
Przyciski	Przycisk Power, przycisk Reset
Zasilacz	Redundantne zasilacze (2 sztuki) o mocy min. 300W każdy, 100-240V, obsługa hot-swap
Pobór mocy w trybie uśpienia dysków	Nie więcej niż 40W
Pobór mocy w trybie pracy	Typowo nie więcej niż 75W przy pełnym obciążeniu dyskami
Chłodzenie	Min. 2 wentylatory o średnicy 80mm, 12VDC z automatyczną regulacją obrotów
System ostrzeżeń	Buzzer ostrzegający o zdarzeniach systemowych
Temperatura pracy	Zakres od 0°C do 40°C
Temperatura przechowywania	Zakres od -20°C do 70°C
Wilgotność względna	5-95% bez kondensacji
System operacyjny	Dedykowany system operacyjny producenta z interfejsem webowym do zarządzania
Obsługa wirtualizacji	Wsparcie dla aplikacji wirtualizacyjnych i kontenerów
Obsługa iSCSI	Tak - funkcjonalność IP-SAN
Maksymalna liczba jednoczesnych połączeń CIFS	Min. 1500 połączeń przy maksymalnej konfiguracji pamięci RAM
Protokoły sieciowe	Min. SMB/CIFS, AFP, NFS, FTP, WebDAV, iSCSI
Obsługa chmury	Integracja z publicznymi usługami chmurowymi oraz możliwość synchronizacji danych
Funkcje bezpieczeństwa	Szyfrowanie sprzętowe AES-NI, obsługa protokołów szyfrowanych (HTTPS, SSH), kontrola dostępu, firewall
Aplikacje i usługi	System aplikacji rozszerzających funkcjonalność: backup, replikacja, surveillance, multimedia, bazy danych, serwer WWW
Obsługa HDMI	Możliwość lokalnego wyświetlania treści i obsługi interfejsu poprzez port HDMI
Gwarancja	Min. 3 lata gwarancji producenta
Akcesoria w zestawie	Kabel zasilający (min. 2 szt.), zatrzaski montażowe do szafy rack, instrukcja obsługi, płyta z oprogramowaniem utilities
Normy i certyfikaty	CE, FCC, BSMI, RoHS oraz inne certyfikaty bezpieczeństwa i kompatybilności elektromagnetycznej wymagane prawem
Producent i model referencyjny	QNAP TS-1264U-RP-4G lub równoważny o parametrach nie gorszych niż opisane powyżej

1. Oferent może zaoferować urządzenie równoważne o parametrach nie gorszych niż opisane w powyższej specyfikacji.

2. W przypadku oferowania urządzenia równoważnego, Oferent zobowiązany jest wykazać spełnienie wszystkich wymaganych parametrów technicznych poprzez załączenie stosownej dokumentacji technicznej producenta.
3. Dyski twarde muszą być fabrycznie nowe, pochodzić z autoryzowanego kanału dystrybucji i być objęte pełną gwarancją producenta dysków.
4. Urządzenie musi być dostarczone w oryginalnym, nienaruszonym opakowaniu producenta wraz z wszystkimi akcesoriami standardowo dostarczany przez producenta.
5. Zamawiający wymaga, aby oferowane rozwiązanie umożliwiało rozbudowę o dodatkowe dyski twarde oraz zwiększenie pamięci RAM zgodnie z parametrami maksymalnymi określonymi przez producenta.

7. Oprogramowanie do kopii zapasowych

- Oprogramowanie może być dostarczane w dwóch scenariuszach:
 - Cloud(Software as Service),
 - On-premise.
- Istnieje możliwość migracji w obie strony pomiędzy środowiskiem on-premise oraz cloud.
- Interfejs systemu dostępny jest w języku:
 - polskim,
 - angielskim,
- Oprogramowanie nie preferuje platformy sprzętowej, nie jest profilowane pod konkretnego dostawcę sprzętu serwerowego oraz pamięci masowych,
- Oprogramowanie może być uruchomione w kontenerze docker,
- Możliwość instalacji oraz uruchomienia serwera zarządzania na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy:
 - Debian: 9+
 - Ubuntu: 16.04+
 - Fedora: 29+
 - CentOS: 7+
 - RHEL: 6+
 - openSUSE: 15+
 - SUSE Enterprise Linux (SLES): 12 SP2+
 - Windows Client: 7, 8.1, 10 (1607+)
 - Windows Server: 2008 R2+,
- System wykonuje kopię własnej bazy danych, która umożliwia odtworzenie wszystkich ustawień i całej konfiguracji,
- Oprogramowanie działa w architekturze wykluczającej pojedynczy punkt awarii(awaria jednego z komponentów nie spowoduje przestoju),

Wsparcie techniczne:

- Pomoc techniczna w językach:
 - polskim,
 - angielskim.
- Materiały samopomocowe:
 - Baza wiedzy:
 - polski,
 - angielski

Zarządzanie:

- Zarządzanie całością działania systemu (backup, przywracanie)z poziomu jednej konsoli webowej,
- Zarządzanie całym systemem poprzez dashboardy,
- Gradacja uprawnień kont administratorów z poziomu panelu zarządzającego,
- System posiada wbudowane predefiniowane zadania backupowe,
- System umożliwia tworzenie zadań backupowych w oparciu o kalendarz.
- Automatyczne oraz ręczne uruchamianie kopii zapasowych zgodnie z ustalonym harmonogramem,

- Automatyczne oraz ręczne uruchamianie procesu przywracania zgodnie z ustalonym harmonogramem,
- Monitorowanie postępu działania zadania,
- Posiada system powiadamiania poprzez e-mail o zdarzeniach w następujących przypadkach:
 - Zadanie zostało zakończone pomyślnie,
 - Zadanie zostało zakończone z ostrzeżeniami,
 - Zadanie zostało zakończone z błędem,
 - Zadanie zostało anulowane,
 - Zadanie nie zostało uruchomione.
- System generuje alerty na konsoli WEB w przypadku zaistnienia określonego zdarzenia systemowego.
- Możliwość zdefiniowania okna backupowego dla każdego z zadań,
- Oprogramowanie posiada wbudowany menadżer haseł do przechowywania kluczy szyfrujących oraz poświadczeń do magazynów,
- System pozwala na klonowanie planów kopii zapasowych,
- System umożliwia reset hasła administratora w przypadku jego utraty,
- Oprogramowanie umożliwia definiowanie retencji według schematów:
 - GFS(Grandfather-Father-Son),
 - FIFO(First-In, First-Out).
- Oprogramowanie umożliwia tworzenie kont użytkowników nie będących administratorami,
- Konta użytkowników mogą być tworzone poprzez import pliku CSV,
- Oprogramowanie umożliwia tworzenie grup urządzeń,
- Oprogramowanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera(urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera(urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów).
- System pozwala na zarządzanie multi-tenantowe - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.:
 - System Administrator,
 - Backup operator,
 - Restore operator,
 - Viewer.

Składowanie danych:

- Oprogramowanie jest systemem multi-storageowym i umożliwia tworzenie wielu repozytoriów danych jednocześnie,
- System umożliwia składowanie danych:
 - Lokalnie:
 - Zasób SMB,
 - Zasób NFS,
 - Zasób ISCSI,
 - Zasób S3,
 - Katalog zabezpieczonego urządzenia.
 - W chmurze:
 - Amazon Web Service,
 - Magazyn zgodny z S3,
 - Dostarczanej przez producenta.
- System pozwala na zdefiniowanie zapasowej ścieżki repozytorium, na wypadek niedostępności głównej lokalizacji,
- System oferuje mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.
- System umożliwia replikację danych między magazynami.

Odtwarzanie:

- Odtwarzanie granularne:
 - Pojedynczych plików z kopii obrazu dysku,
 - Pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365,

- Wykorzystanie funkcjonalności Bare Metal Restore(kopii zapasowej całego dysku - łącznie z partycjami i danymi startowymi) dla odtwarzania systemu po awarii, wsparcie dostępne jest dla systemów:
 - Windows: 7+,
 - Windows Server: 2008 R2+,
- Odtwarzanie Bare metal Restore może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika.
- Uruchamianie procesu Bare Metal Restore odbywa się z bootowalnej płyty CD lub pendrive'a,
- Oprogramowanie umożliwia odtwarzanie systemu w scenariuszach: P2P, P2V, V2P, V2V.
- Oprogramowanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie(VHD, VHDX, VMDK),
- Odtwarzanie zasobów plikowych bez praw dostępu(tzw. ACL),
- Odtwarzanie zasobów plikowych z prawami dostępu,
- Przywracanie plików pomiędzy systemami operacyjnymi(np. odtwarzanie danych plikowych Linux na systemie Windows),
- Odtwarzanie danych według harmonogramu,
- Przywracanie danych z określonego urządzenia/użytkownika,
- Przywracanie kopii z wybranego magazynu.
- Przywracanie danych Microsoft 365:
 - do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku:
 - pst,
 - mbox.
 - do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji),
- System posiada możliwość nieodwracalnego kasowania danych,
- Przywracanie repozytoriów GIT:
 - Przywracanie pomiędzy hostingami repozytoriów(GitHub/BitBucket),
 - przywracanie między kontami.

Backup:

- Wykonywanie pełnych, różnicowych, przyrostowych kopii zapasowych, a także backupu syntetycznego dla:
 - Systemów operacyjnych:
 - Alpine 3.10+,
 - Debian: 9+,
 - Ubuntu: 16.04+,
 - Fedora: 29+,
 - CentOS: 7+,
 - RHEL: 6+,
 - openSUSE: 15+,
 - SUSE Enterprise Linux(SLES): 12 SP2+,
 - macOS: 10.13+,
 - Windows: 7, 8.1, 10(1607+),
 - Windows Server: 2008 R2+,
 - Środowisk wirtualnych:
 - Hyper-V,
 - VMware: 6.7+.
 - Repozytoriów GIT:
 - GitHub,
 - Bitbucket.
- Wykonywanie pełnych, różnicowych oraz przyrostowych oraz logów transakcyjnych kopii zapasowych dla:
 - Baz danych:
 - Microsoft SQL,
 - MySQL,
 - PostgreSQL,
 - Firebird,
 - Dowolnych innych przez podpięcie skryptów pre/post.

- Szyfrowanie danych wykonywana po stronie stacji roboczej za pomocą algorytmu AES w trybie CBC z kluczem szyfrującym o długości:
 - 128 bit,
 - 192 bit,
 - 256 bit.
- Kompresja danych wykonywana po stronie stacji roboczej za pomocą algorytmów:
 - ZStandard,
 - LZ4.
- Oprogramowanie umożliwia zarządzanie poziomem kompresji,
- Wykonywanie kopii zapasowej otwartych plików(VSS),
- System umożliwia uruchamianie skryptów przed i po backupie,
- System umożliwia uruchamianie skryptów po wykonaniu migawki VSS,
- System umożliwia automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku błędów,
- Backup jednego oraz wielu dysków/całego systemu operacyjnego(Windows) ze wsparciem dla partycji MBR oraz GPT,
- Backup plikowy,
- Oprogramowanie realizuje funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie dyskowe,
- Oprogramowanie umożliwia konsolidację wersji kopii zapasowych,
- Oprogramowanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia,
- Oprogramowanie pozwala na automatyczne uruchomienie kopii zapasowej podczas zamykania systemu operacyjnego.
- Oprogramowanie pozwala na backup zaszyfrowanych partycji.

GIT

- Oprogramowanie zapewnia wsparcie dla repozytoriów lokalnych oraz zdalnych(dostępnych w usługach zewnętrznych),
- Oprogramowanie umożliwia zabezpieczenie metadanych repozytoriów(w zależności od zabezpieczanej usługi m.in.: issues, pull requests, actions/pipelines, wiki).

Licencjonowanie:

- Sposób licencjonowania opiera się na:
 - Ilości serwerów/endpointów- dla fizycznych urządzeń,
 - Ilości fizycznych hostów - dla środowisk wirtualnych,
 - Ilości repozytoriów - dla GIT.
- **Licencje powinny pozwalać na wieczyste zabezpieczenie:**
 - 5 fizycznych serwerów bez wirtualizacji.
- Wsparcie techniczne:
 - Świadczone jest w języku polskim, bezpośrednio przez główną siedzibę producenta,
 - Zapewnia dostęp do aktualizacji oprogramowania,
 - Umożliwia korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego,
 - Obowiązuje przez okres minimum **12 miesięcy**.

8. Agregat prądotwórczy

A. Stan techniczny i tożsamość urządzenia

1. Agregat fabrycznie nowy, nieużywany, niewystawowy, wyprodukowany nie wcześniej niż 12 miesięcy przed dostawą.
2. Trwałe oznaczenie producenta, modelu oraz numeru seryjnego umieszczone na tabliczce znamionowej.

B. Parametry pracy zespołu prądotwórczego

3. Moc znamionowa ciągła (PRIME) min. 18–20 kVA.
4. Moc maksymalna awaryjna (STANDBY) min. 20–22 kVA.
5. Zespół trójfazowy, napięcie wyjściowe 400/230 V, częstotliwość 50 Hz.

6. Prędkość znamionowa pracy silnika: 1500 obr./min.

7. Współczynnik mocy ($\cos \phi$): 0,8.

C. Silnik i zabezpieczenia

8. Silnik wysokoprężny, czterosuwowy, chłodzony cieczą.

9. Układ automatycznej regulacji prędkości obrotowej.

10. Automatyczne zabezpieczenia przed: niskim ciśnieniem oleju, nadmierną temperaturą, przekroczeniem dopuszczalnej prędkości obrotowej.

D. Prądnica

11. Prądnica synchroniczna, bezszczotkowa.

12. Stabilizacja napięcia poprzez AVR.

13. Tolerancja wahań napięcia: maks. $\pm 1\%$.

E. Panel sterowania

14. Możliwość ręcznego i automatycznego uruchamiania zespołu.

15. Wyświetlane parametry: napięcie, prąd, częstotliwość, temperatura, ciśnienie oleju, licznik motogodzin.

16. Sygnalizacja stanów alarmowych i awaryjnych.

17. Wyprowadzenia sygnałów do współpracy z układem SZR/ATS.

F. Wyposażenie i eksploatacja

18. Akumulator rozruchowy + fabryczna ładowarka podtrzymująca.

19. Zbiornik paliwa min. 50–80 l, zapewniający min. 8–10 h pracy przy 75% obciążenia.

20. Podkłady antywibracyjne / rama nośna.

21. Wersja wyciszona (jeżeli wymagana) z poziomem hałasu ≤ 72 dB(A) w odległości 7 m.

22. Możliwość podłączenia uziemienia ochronnego.

G. Dokumentacja i szkolenie

23. Dokumentacja techniczna w języku polskim.

24. Instrukcja obsługi, katalog części i materiały eksploatacyjne.

25. Szkolenie użytkowników min. 2 godziny.

H. Instalacja i uruchomienie

26. Transport, wniesienie, posadowienie i wypoziomowanie agregatu.

27. Wykonanie pełnego podłączenia do instalacji elektrycznej i uziemiającej obiektu.

28. Wykonanie prac zgodnie z polskim prawem, normami PN-EN, Prawem energetycznym i Prawem budowlanym.

29. Wykonanie wymaganych zgłoszeń i formalności wobec OSD (jeżeli dotyczy).

30. Wykonanie próbnego uruchomienia i testu obciążeniowego min. 60 min.

31. Przekazanie protokołu odbioru i dokumentacji powykonawczej.

9. Licencja oprogramowania antywirus z modułem EDR

Ochrona antywirusowa niżej wymienionego systemu monitorowana i zarządzana z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową.

Od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, do prawidłowego działania wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli znajdującej się na serwerach producenta.

Instalacja agenta ochrony antymalware możliwa jest na wspieranych systemach Windows, Mac oraz Linux.

Wspierane przeglądarki internetowe do obsługi konsoli zarządzającej:

- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari

Zarówno konsola jak i oprogramowanie antywirusowe do ochrony stacji roboczych oraz serwerów posiada Polski interfejs użytkownika.

Ten sam agent zainstalowany na systemach Windows umożliwia rozbudowę funkcjonalności o system EDR i mechanizm zarządzania ekspozycją na atak (Exposure Management) – aktywacja dodatkowych funkcji uzależniona jest tylko od posiadanej licencji, automatycznie aktywowana w momencie jej dodania i nie wymaga reinstalacji agenta w środowisku oraz posiadania osobnej konsoli zarządzającej.

Funkcjonalności systemu mogą różnić się w zależności od platformy na jakiej zainstalowany jest agent ze względu na ich ograniczenia, jednak chronione platformy są zarządzane z tej samej konsoli zarządzającej

Opis technologii

1. Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanowania heurystycznego, modułu skanującego nośniki wymienne, monitora ruchu http oraz modułu wykrywającego rootkity.
2. Rozwiązanie posiada wbudowany mechanizm ochrony przed zagrożeniami typu ransomware.
3. Rozwiązanie wspiera technologię Antimalware Scan Interface (AMSI)
4. Rozwiązanie umożliwia wybór plików do skanowania – wszystkich plików lub tylko plików o określonych rozszerzeniach.
5. W momencie wykrycia infekcji rozwiązanie automatycznie stara się wyleczyć plik, a jeśli nie jest to możliwe przenosi go do bezpiecznego folderu kwarantanny.
6. Rozwiązanie posiada możliwość ręcznej reakcji na wykryte zagrożenie, w takim przypadku pozwala na: wyleczenie pliku, usunięcie, przeniesienie do kwarantanny, zmiany nazwy, zablokowania.
7. Rozwiązanie chroni plik systemowy HOSTS przed nieautoryzowanymi zmianami.
8. Rozwiązanie posiada mechanizmy skanujące dyski sieciowe.
9. Skanowanie dysków sieciowych jest możliwe dla dowolnych operacji na takich zasobach lub tylko przy wykonywaniu znajdujących się tam plików.
10. Rozwiązanie posiada możliwość tworzenia wykluczeń dla mechanizmów ochrony w czasie rzeczywistym, w tym co najmniej dla: plików, folderów, procesów.
11. Rozwiązanie posiada mechanizm ochrony ruchu http chroniący użytkownika przed malware oraz phishingiem.
12. Istnieje możliwość stworzenia wykluczenia dla wskazanej aplikacji, tak aby nie skanowała ona ruchu http.
13. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie przez wywołanie funkcji w interfejsie lokalnym oprogramowania.
14. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
15. Rozwiązanie posiada możliwość dystrybuowania aktualizacji baz definicji wirusów oraz aktualizacji oprogramowania zainstalowanego na stacji końcowej, za pomocą serwera pośredniczącego.
16. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej do nowej wersji, następuje w sposób automatyczny, niewidoczny dla użytkownika końcowego.
17. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej nie wymaga dodatkowych czynności konfiguracyjnych ze strony administratora systemu i następuje automatycznie w momencie udostępnienia takiej aktualizacji przez producenta.
18. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli zarządzania.
19. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej w określone dni i godziny tygodnia i miesiąca.
20. Rozwiązanie posiada możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli lub lokalnie przez określonego klienta.
21. Rozwiązanie posiada możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.
22. Rozwiązanie posiada możliwość wywołania procesu skanowania z niskim priorytetem, co pozwala na skanowanie z użyciem mniejszej ilości zasobów systemowych.
23. Rozwiązanie posiada możliwość wywołania skanowania uwzględnionych rozszerzeń a także ich wykluczanie.
24. Rozwiązanie posiada możliwość skanowania urządzeń przenośnych takich jak pendrive, dyski zewnętrzne itp.
25. Skanowanie dysków przenośnych może odbywać się w sposób automatyczny bez wiedzy użytkownika, automatycznie z wyświetleniem podsumowania skanowania użytkownikowi oraz z możliwością zablokowania opcji przerwania skanowania przez użytkownika końcowego.

26. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie.
27. Rozwiązanie posiada funkcję skanowania na żądanie pojedynczych plików, katalogów, napędów przy pomocy skrótu w menu kontekstowym
28. Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).
29. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
30. Rozwiązanie posiada heurystyczną technologię do wykrywania nowych, nieznanych wirusów.
31. Umożliwia wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware”, „adware”, „keylogger”, „dialer”, „trojan”, „rootkit”.
32. Posiada mechanizm wykrywania nowych i nieznanych zagrożeń (0-day), bazujący na technologii chmurowej, analizującej podejrzane pliki wykonywalne.
33. Rozwiązanie posiada technologię wykrywania nowych i nieznanych zagrożeń typu 0-day, technologia ta powinna w głównej mierze bazować na metadanych na temat analizowanego pliku. Pliki sklasyfikowane jako bezpieczne, nie są wysyłane do analizy w infrastrukturze producenta.
34. Rozwiązanie posiada technologię wykrywania nowych i nieznanych zagrożeń, która w przypadku podejrzanych plików umożliwia automatyczne ładowanie ich do systemu sandbox, utrzymywanego w infrastrukturze dostawcy oprogramowania antywirusowego w celu przeprowadzenia dodatkowej strukturalnej i behawioralnej analizy podejrzanego pliku.
35. Rozwiązanie posiada możliwość wyłączenia mechanizmu automatycznego przesyłania podejrzanych plików do dodatkowej analizy przez producenta.
36. Rozwiązanie posiada możliwość umieszczenia oprogramowania typu „spyware”, „adware”, „keylogger”, „dialer”, „trojan” w kwarantannie.
37. Rozwiązanie posiada możliwość obsługi plików skompresowanych obejmującego najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX.
38. Rozwiązanie posiada możliwość logowania historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów jest możliwy z poziomu GUI aplikacji jak i konsoli centralnego zarządzania.
39. Rozwiązanie automatycznie powiadamia użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona.
40. Rozwiązanie posiada możliwość wyłączenia powiadomień dla użytkowników stacji końcowej o wykrytych zagrożeniach.
41. Rozwiązanie posiada możliwość wyłączenia interfejsu użytkownika oprogramowania zainstalowanego na stacji końcowej.
42. Rozwiązanie umożliwia blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.
43. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez system reputacyjny producenta.
44. Rozwiązanie posiada możliwość instalacji dodatku do przeglądarki internetowej (Google Chrome, Mozilla FireFox, MS Edge) pozwalającego na wyświetleniu graficznej informacji o reputacji witryny, która pojawia się w wynikach wyszukiwania w wyszukiwarkach internetowych.
45. Rozwiązanie jest wyposażone w mechanizm ochrony przeglądarki internetowej, w tym analizujący uruchamiane skrypty ActiveX i pobierane pliki.
46. Rozwiązanie posiada możliwość ochrony podczas przeglądania sieci Internet na podstawie badania reputacji witryn.
47. Rozwiązanie umożliwia blokowanie dostępu do kategorii witryn WWW skatalogowanych przez systemy producenta.
48. Oprogramowanie zapewnia co najmniej 30 kategorii klasyfikacji witryn WWW.
49. Użytkownik podczas próby przejścia na witrynę znajdującą się w zablokowanej przez Administratora kategorii, jest powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej.
50. Rozwiązanie umożliwia blokowanie witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS.
51. Rozwiązanie posiada wbudowany mechanizm zabezpieczenia połączenia do witryn skategoryzowanych przez producenta jako „bankowość elektroniczna”.

52. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie blokuje możliwość uruchamiania od strony chronionego hosta poleceń cmd oraz skryptów.
53. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie automatycznie blokuje zdalny dostęp do hosta za pomocą takich narzędzi jak pulpit zdalny, TeamViewer, LogMein, VNC itp.
54. Kontrola połączenia umożliwia zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora – administrator ma możliwość tworzenia własnej listy takich witryn.
55. Rozwiązanie posiada wbudowaną funkcję, która po zakończeniu sesji z witrynami sklasyfikowanymi jako „bankowość elektroniczna” czyści zawartość schowka systemowego.
56. Rozwiązanie posiada funkcję zarządzania zaporą ogniową (tzw. personal firewall) wbudowaną w system Windows, z opcją definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup.
57. Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.
58. Rozwiązanie pozwala na tworzenie własnych reguł w oparciu co najmniej o: kierunek komunikacji sieciowej, protokół sieciowy oraz możliwość wyboru akcji zezwolenia lub zablokowania wskazanej komunikacji.
59. Rozwiązanie posiada możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej).
60. Rozwiązanie umożliwia stworzenie zestawów reguł do natychmiastowego zastosowania, które zablokują komunikację sieciową w celu izolacji hosta na żądanie administratora.
61. Rozwiązanie jest wyposażone w mechanizm aktualizacji aplikacji (patch management), umożliwiającą instalację dostępnych poprawek dla systemu operacyjnego oraz aplikacji na nim zainstalowanych.
62. Mechanizm aktualizacji aplikacji (patch management) nie wymaga instalowania dodatkowych agentów oprócz agenta AV.
63. Moduł aktualizacji aplikacji, okresowo skanuje aplikacje zainstalowane na stacji roboczej i umożliwia ich aktualizację do najnowszych wersji.
64. Moduł aktualizacji aplikacji pełni rolę mechanizmu łatającego podatności i instalującego aktualizacje oprogramowania, a nie jedynie pasywnego skanera luk w bezpieczeństwie aplikacji.
65. Administrator posiada możliwość określenia, kiedy i jakie aktualizacje mają zostać zainstalowane automatycznie.
66. Administrator posiada możliwość uruchomienia aktualizacji dla systemu operacyjnego jak i aplikacji znajdujących się na nim na żądanie dla wybranych lub wszystkich hostów.
67. Mechanizm aktualizacji aplikacji umożliwia automatyczne wyświetlenie komunikatu użytkownikowi od strony hosta o konieczności zamknięcia danej aplikacji, tak aby proces aktualizacji mógł się zakończyć.
68. W przypadku gdy instalacja aktualizacji dla systemu operacyjnego lub innej aplikacji wymaga restartu hosta w celu jej zastosowania, administrator posiada możliwość wymuszenia automatycznego restartu, wymuszenia restartu po określonej liczbie godzin, lub wyświetlenia komunikatu użytkownikowi o konieczności restartu.
69. Administrator konsoli zarządzającej ma możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji.
70. Mechanizm aktualizacji aplikacji (patch management) nie wymaga uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces.
71. Administrator ma możliwość zdefiniowania aplikacji, które nie podlegają aktualizacji, poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej.
72. Rozwiązanie umożliwia wyświetlenie w GUI od strony chronionego hosta informacji o brakujących poprawkach dla systemu lub aplikacji i umożliwienie, ich instalacji przez użytkownika końcowego.
73. System centralnego zarządzania prezentuje niezaktualizowane aplikacje występujące na wszystkich chronionych hostach lub listę nieaktualizowanego oprogramowania dla pojedynczej stacji końcowej.
74. Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.
75. Mechanizm kontroli urządzeń zewnętrznych wspiera m.in. urządzenia takie jak: pamięci masowe, napędy CD/DVD, modemy, porty COM i LTP, drukarki, czytniki kart pamięci, kamery, urządzenia bluetooth.
76. Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączania do stacji końcowej.
77. Lista urządzeń zaufanych jest tworzona co najmniej w oparciu o nazwę urządzenia i identyfikator sprzętowy.

78. Rozwiązanie posiada możliwość blokady zapisywania plików na zewnętrznych dyskach USB urządzenia takie są wówczas dostępne w trybie tylko do odczytu.
79. Mechanizm kontroli urządzeń umożliwia blokadę uruchamiania plików wykonywalnych z nośników pamięci. Blokada ta pozwala na korzystanie z pozostałych danych zapisanych na takich nośnikach.
80. Rozwiązanie posiada opcję zabezpieczenia hasłem możliwości deinstalacji agenta przez użytkownika końcowego.
81. Zmiany w konfiguracji mogą być dokonywane przez użytkownika końcowego tylko dla poszczególnych funkcji aplikacji wskazanych przez administratora w profilu.
82. Rozwiązanie posiada wbudowany mechanizm przywracania plików zaszyfrowanych przez zagrożenia typu ransomware.
83. Mechanizm w swoim działaniu wykorzystuje własną technologię producenta, nie inne technologie takie jak Volume Shadow Copy Service (VSS)
84. W przypadku wykrycia szkodliwego działania ransomware, moduł blokuje aktywność szkodliwego procesu oraz przywraca pliki, które zostały zaszyfrowane do oryginalnej formy i lokalizacji.
85. Moduł przywracania plików zaszyfrowanych może działać w trybie monitorowania, bez podejmowania reakcji.
86. Administrator ma możliwość wskazania własnego folderu, do którego będą kopiowane pliki tworzonej kopii zapasowej plików.
87. Administrator posiada możliwość określenia maksymalnej wielkości pliku, którego kopia zapasowa będzie tworzona przez moduł przywracania.
88. *Rozwiązanie jest wyposażone w dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware niezależnie od pozostałych modułów ochrony. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.*
89. *Moduł posiada możliwość pracy w trybie monitorowania (bez blokowania) przekazując administratorowi informacje dotyczące prób modyfikacji plików w chronionych folderach.*
90. *Administrator posiada możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.*
91. *Istnieje możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną antyransomware.*
92. *Rozwiązanie potrafi automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz daje możliwość wskazania zaufanych aplikacji przez administratora.*
93. *Rozwiązanie posiada funkcjonalność kontroli uruchamianych aplikacji.*
94. *Tryb kontroli aplikacji umożliwia uruchomienie wszystkich aplikacji, uruchomienie i monitorowanie wszystkich aplikacji, blokowanie niezauważanych aplikacji*
95. *Istnieje możliwości blokowania, zezwolenia lub monitorowania aplikacji w oparciu, co najmniej o docelowy identyfikator SHA1,SHA256, lokalizację pliku, wersję pliku, nazwę aplikacji, wielkość pliku, wydawcę, ważność podpisu cyfrowego aplikacji.*
96. *Tworzone reguły dotyczyć mogą czynności: uruchomienia aplikacji, ładowania modułu, uruchomienia instalatora, dostępu do pliku.*
97. *Na wspieranych systemach Windows rozwiązanie pozwala na zdalne wywołanie procesu szyfrowania za pomocą funkcji BitLocker wbudowanej w system operacyjny.*
98. *Administrator posiada w momencie konfiguracji procesu szyfrowania, możliwość wymuszenia od strony użytkownika ustanowienia dodatkowego zabezpieczenia w postaci kodu PIN*
99. *Rozwiązanie posiada możliwość przekazywania do konsoli administracji zdalnej kluczy odzyskiwania funkcji BitLocker*
100. *Rozwiązanie pozwala na zdalne uruchomienie procesu deszyfrowania wcześniej zaszyfrowanych dysków systemowych.*
101. *Administrator w konsoli zarządzającej posiada dostępne informacje dotyczące stanu zaszyfrowania dysków systemowych.*
102. *Rozwiązanie pozwala na uzyskiwanie informacji pochodzących z dziennika systemu Windows dotyczących między innymi: Czyszczenia dziennika audytu, zablokowania konta użytkownika, utworzenia konta użytkownika, zmiany konta użytkownika, błędnych prób logowania użytkownika, wystąpienia błędu krytycznego (BSOD)*
103. *Administrator ma możliwość wyboru, które z informacji pochodzących z dziennika systemu Windows mają być przekazywane do konsoli zarządzającej.*

104. Rozwiązanie pozwala na wygenerowanie pliku za pomocą którego administrator może wywołać zdalne połączenie za pomocą usług Microsoft RDP (Remote Desktop).
105. Wygenerowany plik może być otwarty i wykorzystany do zdalnego połączenia za pomocą Microsoft Terminal Services Client (MSTSC), Microsoft Remote Desktop i innych wspierających usług i aplikacji.

Centralna administracja

1. Portal zarządzający jest dostępny w języku polskim.
2. Poza językiem polskim konsola wspiera języki: angielski, niemiecki, francuski, hiszpański, fiński, włoski.
3. Logowanie do konsoli umożliwia wykorzystanie mechanizmów wieloskładnikowego uwierzytelniania (2FA) dla kont posiadających dostęp do konsoli zarządzającej.
4. Mechanizm 2FA służący zabezpieczeniu dostępu do konsoli zarządzającej w swoim działaniu wykorzystuje mechanizmy: powiadomień SMS, oraz tokenów jednorazowych generowanych w aplikacjach mobilnych (np. Google Authenticator, Microsoft Authenticator).
5. Komunikacja pomiędzy portalem centralnego zarządzania a stacjami roboczymi odbywa się w formie zaszyfrowanej.
6. W celu korzystania z centralnej administracji, od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli zarządzającej znajdującej się na serwerach producenta.
7. Interfejs zarządzania posiada funkcję wyświetlania monitów o zbliżającym się zakończeniu licencji, a także powiadomienia o zakończeniu licencji.
8. Interfejs jest wyposażony w panel kontrolny zawierający podsumowanie stanu bezpieczeństwa organizacji w postaci graficznych wykresów.
9. Wykresy są interaktywne, tzn., że po wybraniu interesującego elementu, następuje przekierowanie do zawierającego bardziej szczegółowe dane menu.
10. Rozwiązanie posiada dedykowaną zakładkę zawierającą informację o wszystkich hostach posiadających zainstalowane oprogramowanie do ochrony, w tym: ich nazwy, status ochrony, przypisany profil bezpieczeństwa.
11. Istnieje możliwość eksportu listy wszystkich hostów do pliku CSV.
12. Administrator ma możliwość wglądu w szczegóły zgłaszającego się hosta, w których zawarte są informacje dotyczące: ostatniego połączenia do konsoli zarządzającej, wersji zainstalowanego produktu, systemu operacyjnego, stanu ochrony, akcji związanych z wykrytymi zagrożeniami i skanowaniami.
13. Administrator ma możliwość z poziomu szczegółów klienta, uruchomienia skanowania antywirusowego, instalacji aktualizacji dla aplikacji i systemu operacyjnego, przypisania profilu, usunięcia urządzenia, zmiany klucza subskrypcji, odizolowania hosta od sieci i pobrania pliku diagnostycznego.
14. Komputery nie nawiązujące komunikacji z konsolą zarządzającą mogą być automatycznie usuwane z listy po określonym przez administratora czasie - co najmniej 60 dni.
15. Rozwiązanie posiada dodatkową zakładkę zawierającą informacje dotyczącą brakujących aktualizacji dla zainstalowanych aplikacji i systemu operacyjnego.
16. Istnieje możliwość posortowania i filtrowania brakujących poprawek pod względem ich poziomu krytyczności.
17. Informacje dotyczące brakujących poprawek dla aplikacji i systemu operacyjnego zawierają liczbę i typ hostów, na których został wykryty brak danej poprawki.
18. Po wskazaniu danej poprawki administrator posiada możliwość jej instalacji na wskazanych komputerach lub na wszystkich komputerach i serwerach, dla których dana poprawka została wydana.
19. Administrator ma możliwość wglądu w historię instalowanych poprawek na chronionych hostach.
20. Rozwiązanie posiada moduł raportujący w którym wyświetlane są informacje dotyczące stanu ochrony, infekcji malware, instalowanych aplikacji.
21. Raporty mogą być tworzone zgodnie z harmonogramem i wysyłane na wskazane adresy email.
22. Rozwiązanie posiada wbudowany mechanizm zarządzania subskrypcjami, z możliwością dodawania nowych kluczy licencyjnych.
23. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.

24. Portal zarządzający umożliwia dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu EDR, mechanizmów zarządzania podatnościami, ochrony usług Microsoft 365.
25. Dodanie klucza licencyjnego skutkuje aktywacją zawartości dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym.
26. Rozwiązanie ma możliwość definiowania różnych profili ustawień dla chronionych urządzeń z poziomu portalu zarządzającego.
27. Profile mogą być przypisane do pojedynczych hostów lub do grup.
28. Profile mogą być automatycznie przypisywane do hostów spełniających określone warunki w tym: adresy IP, DNS, nazwa WINS, przynależność do AD.
29. W przypadku automatycznego przypisywania profili, system pozwala na automatyczne dodawanie tagów dla hostów które otrzymają dany profil konfiguracyjny.
30. Istnieje możliwość porównania 2 profili konfiguracyjnych w celu wyświetlenia różnic pomiędzy nimi.
31. Rozwiązanie pozwala administratorowi podczas tworzenia profili wskazanie funkcjonalności, które mogą być zmieniane przez użytkownika od strony chronionego hosta – możliwość wprowadzanych zmian jest do określenia dla poszczególnych funkcji programu oraz całości konfiguracji.
32. Z poziomu portalu zarządzającego istnieje możliwość pobrania plików instalacyjnych, wykorzystywanych do instalacji agenta na objętych licencją hostach.
33. Pliki instalacyjne mają posiadać plików .EXE, .MSI .MPKG, .DEB, .RPM w zależności od platformy i typu systemu na jakich ma zostać zainstalowany agent.
34. Tworzone profile muszą dawać administratorowi możliwość blokowania ustawień konfiguracyjnych aplikacji zainstalowanych od strony stacji roboczych w celu uniemożliwienia ich modyfikacji przez lokalnego użytkownika.
35. Administrator posiada możliwość wyświetlenia dodatkowych szczegółów dotyczących chronionych hostów.
36. Administrator posiada do wyboru ponad 100 różnych dodatkowych informacji, które mogą być widoczne w tym co najmniej: wersji BIOS, identyfikatora CPU, ilości rdzeni procesora, wolnej ilości miejsca na dysku, informacji o fakcie wykorzystania systemu operacyjnego Windows, który osiągnął cykl end of life, aktywnego wygaszacza ekranu, zalogowanego konta administracyjnego.
37. Portal zarządzający pozwala na zarządzanie oprogramowaniem instalowanym na urządzeniach mobilnych (smartphony) w przypadku posiadania odpowiedniej licencji.
38. Konsola posiada możliwość definiowania wielu kont administratorów o różnych poziomach dostępu.
39. W ramach posiadanych licencji istnieje możliwość przenoszenia oprogramowania w ramach danego klucza subskrypcji z jednej stacji roboczej na inną.
40. Konsola posiada wbudowane narzędzie umożliwiające wygenerowanie podsumowania zdarzeń bezpieczeństwa z okresu ostatnich 7 dni.
41. Narzędzie w swoim działaniu wykorzystuje mechanizmy sztucznej inteligencji.
42. Wygenerowane podsumowanie zdarzeń bezpieczeństwa dostępne jest w języku wykorzystywanym w konsoli
43. Korzystanie z narzędzia nie wymaga posiadania dodatkowej licencji.
- 44.

System EDR zarządzany z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową.

Od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, do prawidłowego działania wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli znajdującej się na serwerach producenta.

Ten sam agent zainstalowany na systemach Windows umożliwia rozbudowę funkcjonalności o system EPP i mechanizm zarządzania ekspozycją na atak (Exposure Management) – aktywacja dodatkowych funkcji uzależniona jest tylko od posiadanej licencji, automatycznie aktywowana w momencie jej dodania i nie wymaga reinstalacji agenta w środowisku oraz posiadania osobnej konsoli zarządzającej.

Rozwiązanie posiada polski interfejs użytkownika centralnej konsoli zarządzania oraz agenta instalowanego na stacji końcowej oraz serwerze.

1. Oprogramowanie instalowane na stacjach końcowych i serwerach, zwane dalej agentem, ma możliwość współpracy z każdym oprogramowaniem antywirusowym dostępnym na rynku.
2. Agent instalowany na stacjach końcowych i serwerach posiada możliwość instalacji z wykorzystaniem mechanizmów dystrybucji oprogramowania Active Directory.
3. Agent instalowany na stacjach końcowych i serwerach posiada możliwość ręcznej instalacji, bez wykorzystania zewnętrznych systemów dystrybucji oprogramowania.
4. Oprogramowanie nie wymaga restartu systemu operacyjnego po dokonaniu aktualizacji oprogramowania agenta monitorującego na stacjach końcowych i serwerach.
5. Dane zebrane przez agenta instalowanego na stacjach końcowych są przesyłane w trybie ciągłym, szyfrowanym protokołem HTTPS, do centrum przetwarzania danych producenta, w celu wykrywania niebezpiecznych zdarzeń.
6. Agent instalowany na stacjach końcowych i serwerach monitoruje i zbiera informacje na temat co najmniej następujących zdarzeń:
 - dostęp do pliku;
 - tworzenie nowego procesu;
 - nawiązane połączenia sieciowe;
 - wpisy dziennika systemu, niezbędne do wykrycia naruszeń bezpieczeństwa;
 - zawartość skryptów uruchamianych na monitorowanej stacji.
7. W celu zmniejszenia obciążenia stacji końcowych wszystkie procesy związane z analizą zebranych danych oraz wykrywaniem podejrzanych zdarzeń odbywają się w centrum przetwarzania danych producenta, a nie na monitorowanej stacji końcowej.
8. Dane zbierane przez agenta instalowanego na stacjach końcowych, przed wysłaniem do centrum przetwarzania danych, są kompresowane w celu optymalizacji wykorzystania łączy sieciowych.
9. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, z centrum przetwarzania danych producenta, odbywa się jedynie z wykorzystaniem protokołów HTTP oraz HTTPS.
10. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, wspiera komunikację za pomocą serwera pośredniczącego http (http proxy).
11. W przypadku braku dostępu do sieci Internet, na monitorowanej stacji, która skutkuje brakiem możliwości przesłania danych zebranych przez agenta do centrum przetwarzania danych producenta, dane zebrane na stacji końcowej są buforowane i przesłane do analizy od razu po uzyskaniu przez agenta dostępu do sieci Internet.
12. Dane zbierane przez agentów na stacjach końcowych i serwerach są, przechowywane i przetwarzane na obszarze Europejskiej Wspólnoty Gospodarczej.
13. Rozwiązanie na bazie zebranych danych generuje detekcje, które stanowią powiązane ze sobą podejrzane zdarzenia, zebrane przez agentów ze stacji roboczych i serwerów.
14. Detekcje są generowane za pomocą statycznych reguł, przygotowanych przez producenta, jak również przy wykorzystaniu mechanizmów uczenia maszynowego uwzględniających specyfikę pracy środowiska informatycznego.
15. Detekcje są generowane w czasie rzeczywistym na podstawie danych zebranych i przesłanych przez agentów uruchomionych na stacjach końcowych i serwerach w środowisku informatycznym.
16. Detekcje widoczne są w konsoli zarządzającej w postaci graficznych diagramów, przedstawiających wykryte anomalie i powiązania pomiędzy biorącymi udział w detekcji elementami.
17. Rozwiązanie posiada możliwość filtrowania zdarzeń biorących udział w detekcji w zależności od poziomu ryzyka – od poziomu informacyjnego do zdarzeń o charakterze krytycznym.
18. Każda detekcja zawiera co najmniej następujące informacje:
 - Lista urządzeń na których rozwiązanie zarejestrowało podejrzane zdarzenia.
 - Data i czas wystąpienia podejrzanych zdarzeń.
 - Listę podejrzanych zdarzeń zidentyfikowanych przez rozwiązanie.
 - Opis dla każdego z podejrzanych zdarzeń, wyjaśniający, dlaczego dane zdarzenie zostało uznane za podejrzane.
 - Sumę kontrolną (co najmniej SHA1) plików, które zostały uznane za podejrzane.
 - Poziom ryzyka, określający istotność danej detekcji.
 - Typ detekcji, określający techniki ataku, które zostały wykryte podczas tworzenia detekcji (np. nieuprawnione podniesienie uprawnień, połączenia z sieciami C&C, nieuprawnione wykonanie skryptu).

19. Zdarzenia, występujące w detekcjach, które wskazują na wykorzystanie znanej techniki ataku na systemy informatyczne, zawierają odnośniki do ogólnodostępnych materiałów opisujących zastosowanie tych technik (np. matryca MITRE ATT&CK).
20. Zdarzenia, występujące w detekcjach, które odnoszą się do plików oraz aplikacji uruchomionych na monitorowanych komputerach, zawierają odnośniki do ogólnodostępnej bazy reputacji, pozwalającej sprawdzić reputację tych plików (np. VirusTotal).
21. Rozwiązanie umożliwia oznaczanie wygenerowanych detekcji jako błędne.
22. Oznaczenie detekcji jako błędnej, musi powodować, automatyczne identyfikowanie przyszłych takich samych detekcji i odpowiednie ich oznaczenie w interfejsie centralnego zarządzania.
23. Rozwiązanie posiada możliwość stworzenia archiwum zawierającego dodatkowe informacje dotyczące hosta, na którym wystąpiła detekcja w celu przeprowadzenia analizy śledczej incydentu.
24. Rozwiązanie pozwala na dodanie własnego komentarza przy wykrytej detekcji.
25. Rozwiązanie umożliwia wykupienie usługi pozwalającej na przesłanie detekcji do laboratorium producenta w celu analizy, zwrotnie administrator otrzymuje szczegółowy raport przygotowany przez analityka dotyczący incydentu.
26. Rozwiązanie pozwala na przesłanie wiadomości e-mail informującej o wygenerowaniu nowej detekcji w systemie.
27. Rozwiązanie pozwala na izolację sieciową komputerów przez administratora.
28. Rozwiązanie umożliwia tworzenie reguł automatycznej izolacji stacji roboczych i serwerów, jeśli zostaną one uwzględnione w wygenerowanych detekcjach.
29. Rozwiązanie umożliwia wykonanie zdalnie reakcji na chronionym hoście w tym co najmniej pozwala na: pobranie plików, pobranie historii PowerShell, pobranie wpisów dziennika zdarzeń, pobranie dziennika ochrony antywirusowej, pobranie informacji o wpisach rejestru systemowego, pobranie informacji o MBR, wylistowanie procesów, wylistowanie informacji z systemowego harmonogramu zadań, wylistowanie usług, umożliwia zatrzymanie procesu lub wątku, umożliwia usuwanie plików, usług, wartości rejestru systemowego oraz zadań systemowego harmonogramu zadań.
30. Rozwiązanie umożliwia tworzenie raportów
31. Rozwiązanie wspiera dostęp do danych na temat utworzonych detekcji za pomocą interfejsu REST API, na potrzeby integracji z innymi systemami zabezpieczającymi.
32. Konsola centralnego zarządzania, oferuje interfejs w języku Polskim.
33. Konsola zarządzająca wyposażona jest w panel kontrolny (dashboard) w którym administrator ma możliwość weryfikacji stanu bezpieczeństwa organizacji.
34. Rozwiązanie umożliwia wyszukanie zdarzeń napływających do konsoli co najmniej w oparciu o: PID nowego procesu, SHA-1 nowego procesu, nazwę procesu, ścieżkę, nazwę procesu docelowego, docelową ścieżkę, typ zdarzenia, nazwę systemu, typ systemu, wersję systemu, adres IP źródłowy oraz zdalny, port lokalny oraz port zdalny, wartość klucza rejestru.
35. Konsola wyposażona w dedykowaną zakładkę zawierającą listę urządzeń posiadających zainstalowanego agenta systemu EDR.
36. Lista urządzeń posiadających zainstalowanego agenta systemu EDR zawiera informacje dotyczące: nazwy hosta, adresu IP, poziomu ważności, przypisanego profilu, systemu operacyjnego, informacji o ostatnim podłączeniu oraz aktualnym statusie.
37. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.
38. Portal zarządzający umożliwia dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu EPP, mechanizmów zarządzania ekspozycją na atak (Exposure Management).
39. Dodanie klucza licencyjnego skutkuje aktywowaniem zawartości zakładki obsługującej dany produkt w portalu zarządzającym.
40. Rozwiązanie posiada wbudowane narzędzie pozwalające na stworzenie podsumowania incydentu na podstawie dostępnych danych.
41. Narzędzie umożliwiające stworzenie podsumowania incydentu w swoim działaniu wykorzystuje mechanizmy sztucznej inteligencji.
42. Generowane podsumowanie incydentu dostępne jest w języku wykorzystywanym w konsoli zarządzającej.
43. Rozwiązanie pozwala na wykupienie dodatkowych usług monitorowa oraz monitorowania i reakcji (MDR) na incydenty dla systemu EDR, które realizowane są przez zespoły bezpieczeństwa producenta rozwiązania.
44. Wykupienie usługi nie ogranicza administratorowi dostępu do konsoli zarządzającej i nie wymaga reinstalacji agentów.