

Urządzenie UTM – Opis przedmiotu zamówienia

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 700 tys. jednoczesnych połączeń oraz 32 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 1.7 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 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 1.3 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 650 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.

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 - zaporą 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 łączy WAN

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 umożliwić 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.

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, weryfikacja zgodności konfiguracji z dobrymi praktykami producenta (audyt konfiguracji i polityk urządzenia).



Przełącznik sieciowy (switch zarządzalny) – Opis przedmiotu zamówienia

W ramach postępowania wymagany jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.

Parametry fizyczne platformy

- Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
- Zasilanie AC 230V.
- Maksymalny pobór mocy: 60 W.
- Minimalny zakres temperatury pracy: 0-40°C.

Interfejsy sieciowe - wymagania minimalne

1. Wymagany jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:

a) 48 porty GE RJ-45.

e) 4 porty 10 GE SFP+.

Zarządzanie

- Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
- Wsparcie dla SNMP w wersjach 1-3
- Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
- Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
- Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
- Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
- Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
- Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.

- Automatycznie wykonywane rewizje konfiguracji.

Parametry wydajnościowe

- Przepustowość urządzenia - min. 175 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 250 Mpps.
- Tablica adresów MAC o pojemności co najmniej 32k wpisów.
- Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.

Wymagane funkcje

- Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
- Obsługa Jumbo Frames.
- Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
- Agregacja portów zgodna ze standardem 802.3ad.
- Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.
- Obsługa routingu statycznego.
- Port-mirroring.
- Uwierzytelnianie 802.1x na poziomie portu.
- Uwierzytelnianie 802.1x w oparciu o adres MAC.
- W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).
- W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
- W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
- Obsługa protokołu sFlow.

Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC

1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:
 - Centralne zarządzanie konfiguracją urządzenia
 - Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania
 - Centralne zarządzanie sieciami VLAN.

- Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u
 - Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.
 - Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
 - Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.
 - Automatyczna detekcja i rekomendacje konfiguracji.
 - Przesyłanie logów na zewnętrzny serwer syslog.
 - Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
 - Obsługa białych i czarnych list adresów MAC.
 - Wykrywanie aplikacji komunikujących się w sieci.
2. Musi być możliwe redundantne połączenie z elementami zarządzającymi.
 3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.

Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa

- System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.
- System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.



Access Point – Opis przedmiotu zamówienia

Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.

1. Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych:
 - a. Temperatura 0–50°C,
 - b. Wilgotność 5–90%.
2. Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażona w złącze typu Kensington.
3. Urządzenie musi być wyposażone w trzy niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać co najmniej następujące standardy:
 - a. 2.4 GHz 802.11b/g/n/ax,
 - b. 5 GHz 802.11a/n/ac/ax,
 - c. 6 GHz 802.11ax/be
4. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 24 SSID.
5. Urządzenie musi być wyposażone w moduł BLE.
6. Urządzenie musi być wyposażone w co najmniej jeden interfejs Ethernet (RJ45) wspierający co najmniej szybkości 1G/2.5G/5.0G.
7. Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3at lub zewnętrzny zasilacz. Maksymalne zużycie energii nie może przekraczać 17W przy wykorzystaniu wszystkich funkcji urządzenia.
8. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych:
 - a. Tunnel,
 - b. Bridge,
 - c. Mesh.
9. Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja.
10. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA, WPA2, WPA3, Web Captive Portal, MAC blacklist & whitelist, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST).
11. Interfejs radiowy urządzenia powinien wspierać następujące funkcje:
 - a. MIMO – 2x2,
 - b. Wymagana przepustowość dla poszczególnych modułów radiowych:
 - min. 688 Mbps;
 - min. 2882 Mbps;
 - min. 5765 Mbps;
 - c. Wymagana moc nadawania:
 - min. 23 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm;
 - min. 23 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;
 - min. 22 dBm dla pasma 6GHz z możliwością zmiany co 1dBm
 - d. Wsparcie dla kanałów 20/40/80/160/320MHz,
 - e. Anteny – wbudowane dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz, 5dBi dla pasma 6GHz.

- f. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy.
 - g. Każdy z modułów radiowych musi posiadać możliwość pracy jako dedykowany skaner.
12. Maksymalna deklarowana liczba klientów na każdy moduł radiowy – 512
13. Funkcje dodatkowe:
- a. OFDMA UL i DL
 - b. Spatial Reuse (BSS Coloring)
 - c. UL-MU-MIMO
 - d. DL-MU-MIMO
 - e. Enhanced Target Wake Time (TWT)
 - f. Wbudowany analizator widma
 - g. Wbudowane mechanizmy WIPS/WIDS

Oprogramowanie klasy XDR, EDR – Opis przedmiotu zamówienia

Wymagania ogólne:

1. Licencja musi objąć 30 stanowisk i być dostarczona na okres: 12 miesięcy
2. Zamawiający wymaga wdrożenia rozwiązania w siedzibie zamawiającego oraz szkolenia administrowania w nim co najmniej w zakresie:
 - a. Omówienie z klientem głównych elementów konsoli
 - b. Konfiguracja i pakietów bezpieczeństwa, tworzenie pakietu .MSI
 - c. Konfiguracja profili bezpieczeństwa dla organizacji
 - d. Omówienie modułów Sandbox, Zarządzanie ryzykiem
 - e. Omówienie powiadomień mailowych
 - f. Omówienie incydentów w module EDR/XDR

Wspierane systemy operacyjne

System Operacyjny Windows:

Systemy Operacyjne Komputerów

- Windows 11 October 2024 Update (24H2)
- Windows 11 October 2023 Update (23h2)
- Windows 10 November 2022 Update (22H2)
- Windows 11 September 2022 Update (22H2)
- Windows 11 (initial release)
- Windows 10 November 2021 Update (21H2)
- Windows 10 May 2021 Update (21H1)
- Windows 10 October 2020 Update (20H2)
- Windows 10 May 2020 Update (20H1)
- Windows 10 May 2019 Update (19H1)
- Windows 10 October 2018 Update (Redstone 5)
- Windows 10 April 2018 Update (Redstone 4)
- Windows 10 Fall Creators Update (Redstone 3)
- Windows 10 Creators Update (Redstone 2)

- Windows 10 Anniversary Update (Redstone 1)
- Windows 10 November Update (Threshold 2)
- Windows 10 (initial release)
- Windows 8.1
- Windows 8
- Windows 7 SP1

Windows Tablet oraz systemy wbudowane

Windows 10 IoT Enterprise
Windows Embedded 8.1 Industry
Windows Embedded 8 Standard
Windows Embedded Standard 7
Windows Embedded Compact 7
Windows Embedded POSReady 7
Windows Embedded Enterprise 7

Windows ARM64 desktop

Windows 11 October 2024 Update (24H2)
Windows 10 November 2022 Update (22H2)
Windows 11 September 2022 Update (22h2)
Windows 10 November 2021 Update (21H2)

Systemy operacyjne serwera

Windows Server 2025 64x
Windows Server 2022 Core
Windows Server 2022
Windows Server 2019 Core
Windows Server 2019
Windows Server 2016
Windows Server 2016 Core

Windows Server 2012 R2

Windows Server 2012

Windows Small Business Server (SBS) 2011

Windows Server 2008 R2

Systemy Operacyjne Linux i wersja kernel

Oparte o RPM

RHEL 7.x - 3.10.0 (build 957) 64-bit

RHEL 8.x - 4.18.0 64-bit

RHEL 9.x - 5.14.0 64-bit

Oracle Linux 7.x (UEK) - 4.18.0 64-bit

Oracle Linux 7.x (RHCK) - 3.10.0 build 957 64-bit

Oracle Linux 8.x (UEK) - 5.4.17 / 5.15.0 64-bit

Oracle Linux 8.x (RHCK) – 4.18.0 64-bit

Oracle Linux 9.x (UEK) – 5.15.0 64-bit

Oracle Linux 9.x (RHCK) – 5.14.0 64-bit

CentOS 7.x - 3.10.0 (build 957) 32-bit/64-bit

CentOS 8 Stream - 4.18.0 64-bit

CentOS 9 Stream - 5.14.0 64-bit

Fedora 37 – 40 – wsparcie do wygaśnięcia. 64-bit

AlmaLinux 8.x - 4.18.0 64-bit

AlmaLinux 9.x - 5.14.0 64-bit

Rocky Linux 8.x - 4.18.0 64-bit

Rocky Linux 9.x - 5.14.0 64-bit

CloudLinux 7.x - 3.10 (build 957) 64-bit

CloudLinux 8.x - 4.18.0 64-bit

Miracle Linux 8.x - 4.18.0 64-bit

Kylinv10 RHEL - 4.19.90 64-bit

Oparte o Debian

Debian 9 - 4.9.0 32-bit/64-bit

Debian 10 - 4.19 32-bit/64-bit

Debian 11 - 5.10 32-bit/64-bit

Debian 12 – 6.1.0 64-bit

Ubuntu 16.04.x - 4.8 / 4.10 / 4.13 / 4.15 32-bit/64-bit

Ubuntu 18.04.x - 5.0 / 5.3 / 5.4 64-bit

Ubuntu 20.04.x - 5.4 / 5.8 / 5.11 / 5.13 / 5.15 64-bit

Ubuntu 22.04.x - 5.15 / 5.19 64-bit

Ubuntu 23.04.x – 6.2.0 64-bit

Ubuntu 24.04.x – 6.8.0 64-bit

PopOS 22.04.x – 6.2.6 64-bit

Pardus 21 – 5.10.0 64-bit

Mint 20.x – 5.4.0 64-bit

Mint 21.x – 5.15.0 64-bit

Mint 22.x – 6.8.0.x 64-bit

Zorin OS – 6.5.x 64-bit

Linux Mint Debian Edition 6 – 6.1.x 64-bit

Oparte o SUSE

SLES 12 SP4 - 4.12.14-x 64-bit

SLES 12 SP5 - 4.12.14-x 64-bit

SLES 15 SP1 - 4.12.14-x 64-bit

SLES 15 SP2 - 5.3.18-x 64-bit

SLES 15 SP3 - 5.3.18-x 64-bit

SLES 15 SP4 – 5.14.21 64-bit

SLES 15 SP5 – 5.14.21 64-bit

SLES 15 SP6 – 6.4.x 64-bit

SLED 15 SP4 – 5.14.21 64-bit

openSUSE Leap 15.4 - 15.5 - 5.14.21 64-bit

Cloud based Linux

AWS Bottlerocket 2020.03 - 5.4.x, 5.10.x 64-bit

Amazon Linux v2 - 4.14.x / 4.19.x / 5.10 64-bit

Amazon Linux 2023 – 6.1.x 64-bit

Google COS Milestones 77, 81, 85 - 4.19.112 / 5.4.49 64-bit

Azure Mariner 2 - 5.15 64-bit

Linux dla ARM

Oparte o RPM

RHEL 8.x – 4.18.0-x

RHEL 9.x – 5.14

AlmaLinux 9.x – 5.14

Rocky Linux 9.x – 5.14

Oparte o Debian

Debian 11 – 5.10 / 6.1

Debian 12 – 6.1.0.x

Ubuntu 20.04.x – 5.15

Ubuntu 22.04.x – 5.15 / 5.19

Ubuntu 24.04.x – 6.8.0.x

Oparte o SUSE

SLES 15 SP4 – 5.14.21-x

openSUSE Leap 15.4-15.5 – 5.14.21-x

Oparte o chmurę

Amazon Linux v2 – 5.10

Amazon Linux 2023 - 6.1

Systemy Operacyjne Mac OS X

macOS Sequoia (15.x)

macOS Sonoma (14.x)

macOS Ventura (13.x)

macOS Monterey (12.x)

macOS Big Sur (11.x)



Obsługiwane Środowiska Microsoft Exchange

Security for Exchange wspiera następujące wersje i role Microsoft Exchange:

- Exchange Server 2019 z rolą Edge Transport lub Mailbox
- Exchange Server 2016 z rolą Edge Transport lub Mailbox
- Exchange Server 2013 z rolą Edge Transport lub Mailbox
- Exchange Server 2010 z rolą Edge Transport, Hub Transport lub Mailbox

Security for Exchange jest kompatybilny z Microsoft Exchange Database Availability Groups (DAG).

Ochrona środowisk wirtualnych (SVE)

1. Możliwość zastosowania zewnętrznego silnika skanującego w postaci maszyny wirtualnej.
2. Maszyna wirtualna pełniąca rolę silnika skanującego może być pobrana w formacie:
 - a) OVA
 - b) XVA
 - c) VHD
 - d) VHDX
 - e) VMDK

Środowiska wspierane:

- VMware vSphere and vCenter Server:
 - version 6.5
 - version 6.7, including update 1, update 2a and update 3
 - version 7.0, including update 1, update 2, update 2b, update 2c and update 2d
 - version 8.0, including update 1, update 2
- VMware Horizon/View 7.8, 7.7, 7.6, 7.5, 7.1, 6.x, 5.x
- VMware Workstation 11.x, 10.x, 9.x, 8.0.6
- VMware Player 7.x, 6.x, 5.x
- Citrix Xen Hypervisor: 8.4.
- Citrix Virtual Apps and Desktops 7 1808, 7 1811, 7 1903, 7 1906
- Citrix XenApp and XenDesktop 7.18, 7.17, 7.16, 7.15 LTSR, 7.6 LTSR

- Citrix VDI-in-a-Box 5.x
- Microsoft Hyper-V Server 2008 R2, 2012, 2012 R2, 2016, 2019 or Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019 (including Hyper-V Hypervisor)
- Red Hat Enterprise Virtualization 3.0 (including KVM Hypervisor)
- Oracle VM 3.0
- Oracle VM VirtualBox 5.2, 5.1
- Nutanix Prism with AOS 5.6, 5.5, 5.20 LTS, 5.18 STS, 5.15 LTS, 5.11, 5.10 (Enterprise Edition)
- Nutanix Prism with AHV 20170830.115, 20170830.301, 20170830.395 and 20190916.294 (Community Edition)

Ochrona antywirusowa i antyspyware

Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.

1. Interfejs oraz pomoc techniczna świadczona w języku polskim.
2. Wykrywanie zagrożeń i analiza procesów technikami heurystycznymi.
3. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
4. Wbudowana technologia do ochrony przed rootkitami.
5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
6. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".
7. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
8. Możliwość ustawienia zadania skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu.
9. Możliwość skanowania dysków sieciowych i dysków przenośnych.
10. Skanowanie plików spakowanych i skompresowanych.
11. Ochrona krytycznych kluczy rejestru przed ich wykorzystaniem lub nieautoryzowanym dostępem do nich.
12. Możliwość dodawania wykluczeń na podstawie:

- a) Plik
- b) Folder
- c) Rozszerzenie
- d) Proces
- e) Hash pliku
- f) Hash certyfikatu
- g) Nazwa zagrożenia
- h) Wiersz poleceń
- i) IP/maska

13. Skanowanie poczty opartej o protokoły POP3 i SMTP w czasie rzeczywistym.

14. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie w przeglądarce.

15. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Dodatkowo zdefiniowane są grupy stron przez producenta.

16. Wsparcie przeglądarek Internet Explorer 8+, Mozilla Firefox 30+, Google Chrome 34+, Safari 4+, Microsoft Edge 20+ i Opera 21+ bez konieczności zmian w konfiguracji.

17. Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, RDP, FTPS, SCP/SSH.

18. Program powinien skanować ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.

19. W GUI programu na punkcie końcowym z systemem Windows oraz macOS możliwość wyświetlenia aktualnej wersji produktu i aktualnej wersji silników.

20. W GUI programu na punkcie końcowym z systemem Windows oraz macOS możliwość wyświetlenia, kiedy była przeprowadzana ostatnia aktualizacja z dokładnością co do dnia i godziny.

21. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.

22. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.

23. Administrator musi mieć możliwość ukrycia ikony oprogramowania w obszarze powiadomień systemu Windows.
24. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na punkcie końcowym Windows i macOS.
25. Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet.
26. Oprogramowanie klienckie posiada wbudowaną funkcję do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej.
27. System musi umożliwiać kontrolę dostępu do urządzeń na podstawie interfejsów, do których zostały one podłączone.
28. Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej na podstawie ich wykrycia lub wpisanych ręcznie ID urządzenia lub ID produktu.
29. Funkcja blokowania informacji wysyłanych przez HTTP lub SMTP jak: (adresy e-mail, Piny, Konta bankowe, hasła itp.).
30. Funkcja blokowania wysyłanych informacji konfigurowana zdalnie przez administratora.
31. Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego.
32. Wbudowany IDS.
33. Możliwość wykorzystania funkcji skanowania lokalnego lub hybrydowego ze sprawdzaniem reputacji plików w chmurze.
34. Możliwość tworzenia list sieci zaufanych.
35. Możliwość dezaktywacji funkcji zapory sieciowej.
36. Dodatkowa funkcja ochrony przeciwko znanym zagrożeniom typu ransomware.
37. Użytkownik na punkcie końcowym ma możliwość opóźnienia restartu potrzebnego do zakończenia jednego lub wielu zadań (konfigurowalne w politykach bezpieczeństwa).
38. Komunikacja między konsolą zarządzającą, a punktami końcowymi jest szyfrowana.

39. Wbudowana ochrona przed exploitami wyposażona w minimum 15 różnych technik wykrycia exploitów z możliwością włączenia lub wyłączenia każdej z nich oraz dająca możliwość dodania własnych procesów. Funkcja umożliwia również:

- a) Możliwość wymuszenia funkcji DEP systemu Windows.
- b) Możliwość wymuszenia relokacji modułów (ASLR) dla Windows.

40. Ochrona przed atakami sieciowymi – Mechanizm obronny przed atakującymi próbującymi uzyskać dostęp do systemu poprzez wykorzystanie luk w sieci. Funkcja ta musi obejmować ochronę przed technikami takimi jak:

- Pierwszy dostęp.
- Dostęp do poświadczeń.
- Wykrycie.
- Crimeware.
- Ruch boczny.

41. Ochrona przed ransomware - możliwość wykrywania i blokowania ataków typu ransomware niezależnie od tego czy atak został przeprowadzony lokalnie lub zdalnie na punkcie końcowym oraz utworzenie kopii zapasowej plików w momencie szyfrowania, a w przypadku ataku odzyskanie i przywrócenie ich do pierwotnej lokalizacji. Oprogramowanie musi dać możliwość odzyskania plików na żądanie lub automatycznie, o następujących rozszerzeniach:

3fr, ai, arw, bay, cdr, cer, cr2, crt, crw, dcr, der, dll, dng, doc, docm, docx, dwg, dxf, dxg, eps, erf, exe, indd, jpe, jpeg, jpg, mdf, mef, mrw, nef, nrw, odb, odc, odm, odp, ods, odt, orf, p12, p7b, p7c, pdd, pdf, pef, pem, pfx, ppt, pptm, pptx, psd, pst, ptx, png, r3d, raf, rtf, rw2, rwl, sr2, srf, srw, wb2, wpd, wps, x3f, xlk, xls, xlsb, xlsx, msg, py, ini, xml, msi, cab, tsf, dgn, log, gif, csv, avi, mov, mp4

42. System musi wykrywać podatne sterowniki zainstalowane na punkcie końcowym z Windows i Linux.

43. Agent i usługi oprogramowania antywirusowego zainstalowanego na punkcie końcowym muszą być chronione przed próbami manipulacji i naruszenia ich integralności w systemie Windows.

- 44. Oprogramowanie musi skanować nośniki USB zanim użytkownik zaloguje się do systemu Windows.
- 45. System musi umożliwiać skanowanie oprogramowania układowego UEFI.
- 46. System umożliwia przechwytywanie TLS handshake pozwalając na skanowanie ruchu sieciowego bez konieczności deszyfracji.
- 47. Telemetria - Możliwość przesyłania nieprzetworzonych danych bezpieczeństwa z punktów końcowych z systemem operacyjnym Windows i macOS do SIEM Splunk (wymaga TLS 1.2 lub wyższy) lub z systemem Windows i Linux do serwera Syslog (JSON).
- 48. Oprogramowanie pozwala na skanowanie punktów końcowych pod kątem wyszukiwania wskaźników naruszeń bezpieczeństwa (IOC).



Stacje robocze i serwery

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
3. Jedna wersja instalacyjna na stacje robocze i serwery plików Windows.
4. Oprogramowanie zawiera monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego.
5. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program powinien pytać o hasło.
6. Produkt i zawartość zabezpieczeń powinny być aktualizowane nie rzadziej niż raz na godzinę.
7. Oprogramowanie posiada możliwość raportowania zdarzeń informacyjnych.
8. Oprogramowanie musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju.
9. Oprogramowanie musi posiadać możliwość skanowania jedynie nowych i zmienionych plików.
10. Oprogramowanie posiada możliwość odblokowania ustawień lokalnych konfiguracji na systemach Windows po doinstalowaniu odpowiedniego modułu. Zmiana ustawień zabezpieczona jest hasłem.
11. Po kliknięciu prawym klawiszem myszy na ikonie programu i wybraniu opcji „O programie”, możliwość wyświetlenia danych do pomocy technicznej tj: adres strony pomocy, adres e-mail do administratora ochrony, numer telefonu do administratora ochrony z wyłączeniem systemów Linux.
12. Dla maszyn z systemem Linux możliwość wskazania katalogów, które mogą być chronione w czasie rzeczywistym.

Ochrona Exchange

1. Rozwiązanie musi zapewniać filtrowanie antymalware dla przychodzącego, wewnętrznego i wychodzącego ruchu mailowego.
2. Rozwiązanie musi wspierać skanowanie "na życzenie" oraz skanowanie według harmonogramu dla skrzynek pocztowych i folderów publicznych, w tym możliwość zarówno wykluczenia konkretnych skrzynek bądź folderów publicznych, jak i skanowania tylko emaili z załącznikami bądź emaili otrzymanych w ciągu określonego czasu.
3. Zdolność konfigurowania różnych akcji wykonywanych na plikach zainfekowanych, podejrzanych oraz niemożliwych do przeskanowania.
4. Możliwość skanowania w poszukiwaniu potencjalnie niechcianych aplikacji (PUA).
5. Możliwość skanowania malware wewnątrz archiwów.
6. Rozwiązanie musi zapewniać filtr antyspamowy dla ruchu mailowego, z możliwością dodania do białej listy konkretnych adresów email i domen.
7. Możliwość odpytania serwerów Realtime Blackhole List (RBL) zdefiniowanych przez administratorów i odfiltrowania wiadomości zaklasyfikowanych jako spam bazując na reputacji wysyłającego serwera.
8. Zdolność automatycznego oznaczenia jako spam wiadomości mailowych napisanych przy użyciu alfabetów azjatyckich bądź cyrylicy.
9. Zdolność do wykonania zapytań bazujących na chmurze dla udoskonalonej ochrony przeciw nowemu spamowi.
10. Zdolność do podjęcia różnych akcji na wykrytych mailach ze spamem, takich jak poprzedzanie tematu maila konkretną etykietą, usunięcie, przeniesienie do kwarantanny bądź przekierowanie maila do konkretnej skrzynki pocztowej.
11. Rozwiązanie musi zapewniać funkcjonalności filtrowania zawartości dla przychodzącego, wewnętrznego i wychodzącego ruchu mailowego, bazujące na konkretnym tekście bądź wyrażeniach regularnych zgodnych z tematem maila i/lub jego zawartością.
12. Zdolność do podejmowania różnych akcji na emailach, pasujących do reguł filtrowania treści, takich jak dodawanie prefiksu w postaci taga do tematu maila, usuwanie, wysyłanie do kwarantanny bądź przekierowywanie emaila do konkretnej skrzynki.

Konsola zdalnej administracji

1. System musi umożliwiać centralne zarządzanie i konfigurację ochrony wspieranych stacji roboczych i serwerów.
2. Możliwość integracji wielu domen Active Directory.
3. Możliwość uruchomienia zdalnego skanowania wybranych punktów końcowych.
4. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony punktu końcowego (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania na żądanie, zainstalowanych modułów, ostatniej aktualizacji oraz przypisanej polityki).
5. Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci, analityk bezpieczeństwa lub z ustawieniami niestandardowymi.
6. Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, systemu operacyjnego.
7. Możliwość centralnej aktualizacji punktów końcowych z serwera w sieci lokalnej lub z Internetu.
8. Możliwość wysłania linku instalacyjnego bezpośrednio z poziomu konsoli administracyjnej.
9. Możliwość uruchomienia centralnej konsoli jedynie z poziomu przeglądarki internetowej.
10. Możliwość ręcznego (na żądanie) i automatycznego generowania raportów (według ustalonego harmonogramu) oraz wyeksportowanie ich do formatu: pdf i csv. Również zbiorczo w formie archiwum zip.
11. Raport generowany według harmonogramu z możliwością automatycznego wysłania go do osób zdefiniowanych w tym raporcie.
12. Możliwość generowania raportu co godzinę.
13. Pierwsza aktywacja modułu kontroli urządzeń nie wymaga restartu stacji docelowej.
14. Możliwość dodania etykiety do stacji roboczej.
15. Możliwość dezinstalacji oprogramowania antywirusowego innych firm w trakcie instalacji zdalnej.
16. Możliwość przechowywania kwarantanny maksymalnie 180 dni.

17. Możliwość definiowania, czy pliki z kwarantanny mają być przysyłane do producenta i co ile godzin ma się ta czynność odbywać.
18. Po aktualizacji zawartości bezpieczeństwa opcja automatycznego przeskanowania kwarantanny.
19. Wsparcie techniczne mailowe i telefoniczne w j. polskim od poniedziałku do piątku w godzinach 8:00-16:00. W pozostałych godzinach możliwość bezpośredniego kontaktu z producentem (24/7) w j. angielskim.
20. Po integracji z lokalnym Active Directory możliwość przypisywania polityk automatycznie po zalogowaniu do systemu operacyjnego w zależności od tego jaki użytkownik domenowy się zalogował lub do jakiej grupy domenowej on należy.
21. Możliwość automatycznego przypisywania polityk na podstawie reguły lokalizacji.
Określenie lokalizacji na podstawie:
 - Zakres adresów IP/IP.
 - Adres bramy.
 - Adres serwera WINS.
 - Adres serwera DNS.
 - Połączenie DHCP sufiksów DNS.
 - Punkt końcowy może rozwiązać hosta.
 - Typ sieci.
 - Nazwa hosta.
22. Uwierzytelnienie dwuskładnikowe realizowane przy pomocy aplikacji kompatybilnej ze standardem RFC6238.
23. Możliwość naprawy instalacji agenta z poziomu konsoli.
24. Możliwość utworzenia reguły, która będzie usuwała punkty końcowe z konsoli zarządzającej, jeżeli punkt końcowy nie połączył się z konsolą przez określoną liczbę dni. Funkcja ta pozwala również na określenie wzoru nazw maszyn, które automatycznie będą usuwane oraz na określenie godziny, o której te maszyny będą usuwane.
25. Możliwość wyświetlania adresu MAC dołączonego do nazwy hosta.
26. Możliwość wyświetlenia czy punkt końcowy jest serwerem czy stacją roboczą.

27. Możliwość wyświetlenia informacji czy zainstalowany na punkcie końcowym system operacyjny to Windows, Linux lub MacOS.
28. Możliwość filtrowania punktów końcowych, które były online w ciągu ostatnich 24 godzin, 7 lub 30 dni.
29. Menu tworzenia paczek instalacyjnych musi określać czy dany moduł jest dostępny dla stacji roboczych Windows, Serwerów Windows, Linux, MacOS.
30. Oprogramowanie umożliwia pobranie oddzielnego pakietu instalacyjnego dla systemów MacOS z Intel x86 oraz oddzielnego dla Apple M oraz osobnego pakietu dla systemów Windows z Intel x86 oraz oddzielnego dla architektury ARM.
31. System umożliwia pobieranie plików poddanych kwarantannie z poziomu centralnej konsoli administracyjnej.
32. Możliwość wygenerowania i zapisania logów na stacji roboczej z poziomu konsoli zarządzającej.
33. Możliwość zarządzania ochroną na serwerach Exchange, tworzenie polityk i konfiguracji zdalnej ochrony.
34. Znaczniki punktów końcowych – oprogramowanie musi umożliwiać przypisywanie znaczników (tagów) do punktów końcowych. Przypisywanie musi odbywać się ręcznie lub automatycznie. Musi istnieć możliwość filtrowania punktów końcowych na podstawie kilku wybranych znaczników w jednym czasie.
35. Ochrona proaktywna oparta o maszynowe uczenie, która działa w fazie poprzedzającej wykonanie. Ochrona ta musi wykrywać zagrożenia takie jak:
 - a) Ukierunkowane ataki.
 - b) Podejrzane pliki i ruch w sieci.
 - c) Exploity.
 - d) Ransomware.
 - e) Grayware.
36. Moduł ochrony proaktywnej musi posiadać oddzielne działania jakie będzie podejmował dla plików i oddzielne dla ruchu sieciowego.
37. Moduł ochrony proaktywnej musi działać w trybach, które administrator może dowolnie zmieniać na:

- a) Tolerancyjny.
- b) Normalny.
- c) Agresywny.

38. Zintegrowany sandbox po stronie producenta, który pozwala na analizę pliku:

- a) Plik może zostać wysłany automatycznie ze stacji roboczej, jeżeli oprogramowanie uzna go za podejrzany lub ręcznie z poziomu konsoli przez administratora.
- b) Możliwość ręcznego przesłania archiwum zabezpieczonego hasłem.
- c) Możliwość ręcznego przesłania adresu URL.
- d) W przypadku ręcznego przesłania wielu plików jednorazowo, możliwość detonacji próbek pojedynczo.

39. Wbudowany sandbox musi działać w trybie monitorowania i blokowania.

40. Wbudowany sandbox musi oferować działania naprawcze takie jak dezynfekcja, przeniesienie do kwarantanny lub tylko raportowanie.

41. Wbudowany sandbox musi oferować opcję wstępnego filtrowania plików z kategorii aplikacje, dokumenty, skrypty, archiwa, maile zapisane do pliku, pod kątem podejrzanego zachowania.

42. Wbudowany sandbox musi posiadać opcję, która pozwala na dodanie określonych rozszerzeń do wyjątków, pliki z tym rozszerzeniem nie zostaną przesłane do sandboxa.

43. Minimalny rozmiar pliku jaki może zostać automatycznie przesłany do sandboxa to 1KB.

44. Maksymalny rozmiar pliku jaki może zostać automatycznie przesłany do sandboxa to 50MB.

45. System zarządzania ryzykiem – Zintegrowany z konsolą zarządzającą system, który pozwala oszacować podatność środowiska na atak na podstawie punktów ryzyka. Punkty ryzyka powinny być przydzielane od 0 do 100, gdzie liczba mniejsza stanowi mniejsze ryzyko, a liczba większa większe ryzyko. System ponadto musi posiadać:

- a) Funkcję, która pozwala wyszukiwać podatności ustawień punktów końcowych oraz naprawiać je lub ignorować z podziałem na typ wykrytej konfiguracji:
 - Przeglądarka

-Sieć

-System operacyjny

-Luki

System ponadto musi określać nasilenie zagrożenia wynikłego z wykrytej podatności w oparciu o punkty procentowe oraz posiadać funkcję cofnięcia wprowadzonych zmian w ustawieniach systemów.

- b) System zarządzania ryzykiem powinien określać luki w wykrytym zainstalowanym oprogramowaniu podając przy tym numer CVE tych luk.
- c) System pozwala na śledzenie i wykrywanie ryzykownych działań jakie podejmuje użytkownik na punkcie końcowym wraz z poinformowaniem o liczbie użytkowników, których takie działanie dotyczy oraz jaka jest jego szkodliwość.
- d) System pozwala na skanowanie punktów końcowych pod kątem wykrywania ryzyka na podstawie harmonogramu lub pojedynczo utworzonego zadania.
- e) System pozwala na raportowanie na ile urządzeniach wykryto błędną konfigurację i luki w aplikacjach oraz jaka jest ilość takich podatności i ich szkodliwość wyrażona w procentach.
- f) System pozwala na wykrywanie podatności w oparciu o standardy bezpieczeństwa zgodne z: CISv8, SOC 2, ISO/IEC 27001:2022, GDPR (EU), NIS2 (EU) oraz DORA (EU).
- g) System musi mieć możliwość określenia, które konkretnie zapisy standardów bezpieczeństwa: CISv8, SOC 2, ISO/IEC 27001:2022, GDPR (EU), NIS2 (EU) oraz DORA (EU) nie są spełnione w wyniku wykrytej błędnej konfiguracji.

46. Możliwość scentralizowanego podglądu wykrytych zagrożeń z wszystkich modułów ochrony w jednym miejscu i odfiltrowania ich według daty, kategorii, typu zagrożenia, działań naprawczych i innych.

47. Możliwość ustawienia wymagania zmiany hasła logowania do konsoli co 90 dni.

48. Możliwość zablokowania konta w konsoli, jeżeli użytkownik tego konta podejmował pięć kolejnych prób logowania nieprawidłowym hasłem.

49. Funkcja pojedynczego logowania – Single Sign-on (SSO) przy integracji z Microsoft Azure.

50. Raport podsumowujący - Możliwość podglądu raportu, który streszcza stan środowiska firmowego w ciągu ostatnich 24h, 7 dni lub 30 dni. Z rozróżnieniem na takie sekcje jak:

- a) Zarządzane punkty końcowe.
- b) Ilość zajętych miejsc w licencji z rozróżnieniem na stacje robocze Windows, serwery Windows, macOS, Linux oraz fizyczne punkty końcowe i maszyny wirtualne.
- c) Pięć rodzajów najczęściej blokowanych zagrożeń.
- d) Podział zagrożeń na urządzenia takie jak stacje robocze i serwery.
- e) Status incydentów bezpieczeństwa, które wystąpiły.
- f) Stan modułów punktów końcowych.
- g) Ocena ryzyka firmy.
- h) Zablokowane strony WWW w oparciu o wykryte tam szkodliwe oprogramowanie, phishing, oszustwa.
- i) Zablokowane techniki ataku sieciowego z podziałem na takie jak wczesny dostęp, dostęp do poświadczeń, wykrycie, ruch boczny, crimeware.

51. Możliwość integracji z innymi systemami poprzez API takich elementów bądź sekcji jak:

- a) Firmy
- b) Raporty
- c) Licencjonowanie
- d) Konta
- e) Pakiety
- f) Incydenty
- g) Sieć
- h) Kwarantanna
- i) Integracje
- j) Event Push Service
- k) Polityki

52. Early access – Oprogramowanie musi umożliwiać dobrowolne przystąpienie do darmowych testowych programów wczesnego dostępu. Programy wczesnego dostępu

powinny umożliwiać testowanie najnowszych funkcji oprogramowania, których nie ma jeszcze w wersji końcowej produktu. Uzyskanie dostępu do programu testowego musi być natychmiastowe.

53. Możliwość utworzenia konsoli typu Partner, która pozwala na zarządzanie wieloma firmami z poziomu jednej scentralizowanej konsoli zarządzającej, konsola partnerska musi umożliwiać:

- a) Pobieranie przez partnera plików z kwarantanny podległych firm.
- b) Zarządzanie systemem ochrony firm podrzędnych przez Partnera z jednej konsoli lub tworzenie bezpośrednich dostępów użytkowników dla tych firm.
- c) Odseparowanie przez administratora konsoli podrzędnej od konsoli partnera nadrzędnego.

54. Profil firmy - Możliwość określenia profilu przedsiębiorstwa w konsoli webowej.

Dostępne są kategorie m.in: Lotnictwo, Budownictwo, Edukacja, Służba zdrowia, Handel i inne.

55. System musi umożliwiać wybór trzech poziomów obciążenia procesora dla zadań określonych w harmonogramie skanowania na systemach Linux i macOS.

56. System musi posiadać funkcję wstrzymywania skanowania podczas pracy na baterii.

57. Konsola administracyjna umożliwia zmianę motywu dla interfejsu spośród jasnego, ciemnego lub wybranego automatycznie w oparciu o ustawienia systemowe.

58. System umożliwia tymczasowe wyłączenie wszystkich lub wybranych modułów ochrony na określony czas, który wynosi 15 minut, 30 minut, 1 godzina, 2 godziny, 4 godziny. Po ponownym uruchomieniu ochrony możliwość przeprowadzenia pełnego skanowania.

59. Wbudowany sandbox musi posiadać możliwość przesyłania pliku do analizy z komputera zdalnego za pomocą podanej ścieżki. Wielkość pliku nie może przekraczać 100MB.

60. Filtrowanie wykrytych incydentów bezpieczeństwa m.in. na podstawie:

- a) ID.
- b) Ostatnia aktualizacja.
- c) Status.
- d) Osoba przydzielająca.
- f) Data utworzenia.

- g) Priorytet.
- h) Ocena szkodliwości w skali 0-100.
- i) Podmioty.
- j) Zasoby.
- k) Ostatnia faza killchain.
- l) Wykonane czynności.
- m) Skorelowane incydenty.
- n) Typ incydentu.

61. System umożliwia wygenerowanie i pobranie zestawu informacji z chronionych punktów końcowych w formie archiwum. Funkcja powinna być dostępna dla systemów Windows, Linux oraz macOS. Archiwum musi zawierać co najmniej informacje:

a) Windows

- Logi zainstalowanego agenta.
- Dziennik zdarzeń Windows.
- Informacje o systemie.
- DnsCache.
- Webcache.
- Informacje z głównych katalogów rejestru (SYSTEM, SOFTWARE, DEFAULT, DRIVERS, SAM, SECURITY).
- Harmonogram zadań.
- Historia Powershell (jeśli włączono).

b) Linux

- Podstawowy log pomocy technicznej zainstalowanego agenta.
- Certyfikaty.
- Autorun i usługi.
- Informacje sieciowe.
- Informacje systemowe.
- Zainstalowane pakiety.

c) macOS

- Podstawowy log pomocy technicznej zainstalowanego agenta.

- Autorun.
- Lista procesów.
- Informacje sieciowe.
- Informacje o systemie.

62. Oprogramowanie musi umożliwiać przegląd konfiguracji punktów końcowych w czasie rzeczywistym poprzez tworzenie zapytań pod kątem wykrywania:

- a) historia powłoki.
- b) wczytywanie bibliotek .dll z podejrzanej lokalizacji.
- c) Sesje logowania z użyciem jawnych danych uwierzytelniających.
- d) Arp cache.
- e) Ip forwarding.
- f) Lista zamontowanych nośników.
- g) Konfiguracja ip tables.
- h) Połączenia TLS które używają certyfikatów self-signed.
- i) Używane rozszerzenia w przeglądarce Chrome.
- j) Używane rozszerzenia w przeglądarce Firefox.
- k) Używane rozszerzenia w przeglądarce Safari.
- l) Źródła apt w systemach Linux.
- m) Wyświetlanie zainstalowanych pakietów DEB.
- n) Wyświetlanie zainstalowanych pakietów RPM.
- o) Pakiety Python zainstalowane w systemie.
- p) Lista użytkowników, którzy zostali utworzeni w ciągu ostatnich 30 dni (Linux).
- q) Wykrywanie czy aplikacje zdalnego dostępu są zainstalowane w systemie MacOS.
- r) Wykrywanie czy Kontrola Kont Użytkowników (UAC) jest wyłączona.
- s) Wykrywanie czy SecureBoot jest włączony.
- t) Lista zapamiętanych sieci bezprzewodowych.
- u) Wykrywa, czy zmienił się domyślny folder startowy użytkownika.
- w) Wykrywa, czy zmienił się domyślny folder startowy maszyny.

63. Oprogramowanie musi umożliwiać tworzenie konfigurowalnych reguł, po spełnieniu których może zostać wygenerowany incydent bezpieczeństwa. Funkcja ta powinna:

- a) Oferować opcję podjęcia automatycznych działań po spełnieniu warunków tj.: izolacja punktu końcowego, wygenerowanie archiwum diagnostycznego, przestanie pliku do analizy sandbox, zakończenie procesu i innych.
- b) Automatyczne działania zapobiegawcze są zależne od wyboru kategorii.
- c) Tworzenie reguł musi być określone poprzez wybór operatora np. „to”, „zawiera”, „jest jednym z” itp.
- d) Dotyczyć określonych kryteriów tj. proces, plik, rejestr, połączenia.
- e) Zapewniać możliwość tworzenia zapytań YARA.
- f) Umożliwiać określenie priorytetu kolejności automatyzacji.
- g) Administrator powinien mieć możliwość wyboru poziomu szkodliwości potencjalnie wygenerowanych incydentów (wysokie, średnie i niskie).



EDR-Endpoint Detection and Response

Produkt zapewnia szczegółowe informacje o wykrytych incydentach, interaktywną mapę incydentów i działania naprawcze.

Wspierane systemy operacyjne**A. Systemy desktopowe**

- a) Windows 11 October 2024 Update (24H2)
- b) Windows 11 October 2023 Update (23H2)
- c) Windows 10 November 2022 Update (22H2)
- d) Windows 11 September 2022 Update (22H2)
- e) Windows 11 (initial release)
- f) Windows 10 November 2021 Update (21H2)
- g) Windows 10 May 2021 Update (21H1)
- h) Windows 10 October 2020 Update (20H2)
- i) Windows 10 May 2020 Update (20H1)
- j) Windows 10 May 2019 Update (19H1)
- k) Windows 10 October 2018 Update (Redstone 5)
- l) Windows 10 April 2018 Update (Redstone 4)
- m) Windows 10 Fall Creators Update (Redstone 3)
- n) Windows 10 Creators Update (Redstone 2)
- o) Windows 10 Anniversary Update (Redstone 1)
- p) Windows 10 November Update (Threshold 2)
- q) Windows 10 (initial release)
- r) Windows 8.1
- s) Windows 8
- t) Windows 7 SP1

B. Systemy operacyjne dla serwerów:

- a) Windows Server 2025 64x
- b) Windows Server 2022 Core

- c) Windows Server 2022
- d) Windows Server 2019 Core
- e) Windows Server 2019
- f) Windows Server 2016
- g) Windows Server 2016 Core
- h) Windows Server 2012 R2
- i) Windows Server 2012
- j) Windows Small Business Server (SBS) 2011
- k) Windows Server 2008 R2

C. MacOS:

- a) macOS Sequoia (15.x)
- b) macOS Sonoma (14.x)
- c) macOS Ventura (13.x)
- d) macOS Monterey (12.x)
- e) macOS Big Sur (11.x)

D. Linux

Oparte o RPM

RHEL 7.x - 3.10.0 (build 957) 64-bit

RHEL 8.x - 4.18.0 64-bit

RHEL 9.x - 5.14.0 64-bit

Oracle Linux 7.x (UEK) - 4.18.0 64-bit

Oracle Linux 7.x (RHCK) - 3.10.0 build 957 64-bit

Oracle Linux 8.x (UEK) - 5.4.17 / 5.15.0 64-bit

Oracle Linux 8.x (RHCK) – 4.18.0 64-bit

Oracle Linux 9.x (UEK) – 5.15.0 64-bit

Oracle Linux 9.x (RHCK) – 5.14.0 64-bit

CentOS 7.x - 3.10.0 (build 957) 32-bit/64-bit

CentOS 8 Stream - 4.18.0 64-bit

CentOS 9 Stream - 5.14.0 64-bit

Fedora 37 – 40 – wsparcie do wygaśnięcia. 64-bit

AlmaLinux 8.x - 4.18.0 64-bit

AlmaLinux 9.x - 5.14.0 64-bit

Rocky Linux 8.x - 4.18.0 64-bit

Rocky Linux 9.x - 5.14.0 64-bit

CloudLinux 7.x - 3.10 (build 957) 64-bit

CloudLinux 8.x - 4.18.0 64-bit

Miracle Linux 8.x - 4.18.0 64-bit

Kylinv10 RHEL - 4.19.90 64-bit

Oparte o Debian

Debian 9 - 4.9.0 32-bit/64-bit

Debian 10 - 4.19 32-bit/64-bit

Debian 11 - 5.10 32-bit/64-bit

Debian 12 – 6.1.0 64-bit

Ubuntu 16.04.x - 4.8 / 4.10 / 4.13 / 4.15 32-bit/64-bit

Ubuntu 18.04.x - 5.0 / 5.3 / 5.4 64-bit

Ubuntu 20.04.x - 5.4 / 5.8 / 5.11 / 5.13 / 5.15 64-bit

Ubuntu 22.04.x - 5.15 / 5.19 64-bit

Ubuntu 23.04.x – 6.2.0 64-bit

Ubuntu 24.04.x – 6.8.0 64-bit

PopOS 22.04.x – 6.2.6 64-bit

Pardus 21 – 5.10.0 64-bit

Mint 20.x – 5.4.0 64-bit

Mint 21.x – 5.15.0 64-bit

Mint 22.x – 6.8.0.x 64-bit

Zorin OS – 6.5.x 64-bit

Linux Mint Debian Edition 6 – 6.1.x 64-bit

Oparte o SUSE

SLES 12 SP4 - 4.12.14-x 64-bit

SLES 12 SP5 - 4.12.14-x 64-bit

SLES 15 SP1 - 4.12.14-x 64-bit

SLES 15 SP2 - 5.3.18-x 64-bit

SLES 15 SP3 - 5.3.18-x 64-bit

SLES 15 SP4 – 5.14.21 64-bit

SLES 15 SP5 – 5.14.21 64-bit

SLES 15 SP6 – 6.4.x 64-bit

SLED 15 SP4 – 5.14.21 64-bit

openSUSE Leap 15.4 - 15.5 - 5.14.21 64-bit

Cloud based Linux

AWS Bottlerocket 2020.03 - 5.4.x, 5.10.x 64-bit

Amazon Linux v2 - 4.14.x / 4.19.x / 5.10 64-bit

Amazon Linux 2023 – 6.1.x 64-bit

Google COS Milestones 77, 81, 85 - 4.19.112 / 5.4.49 64-bit

Azure Mariner 2 - 5.15 64-bit

Komponenty EDR

Główne elementy:

1. Sensor EDR, który gromadzi i przetwarza dane dotyczące punktu końcowego i zachowania aplikacji w celu ich raportowania.
2. Analityka Bezpieczeństwa, komponent służący do interpretacji metadanych gromadzonych przez sensor EDR.
3. Możliwość instalacji dodatkowego, dedykowanego agenta z sensorem EDR dla urządzeń z systemem Windows, aby rozszerzyć już zainstalowaną równolegle ochronę świadczoną przez innego producenta oprogramowania antywirusowego.

Wykrywanie podejrzanej aktywności

Monitorowanie zdarzeń na punktach końcowych w poszukiwaniu oznak ataku i wywoływanie incydentów po wykryciu takiej aktywności.

1. Bazowanie na systemach opartych o techniki MITRE ATT&CK i własnej inteligencji.
2. Zgłaszanie naruszeń jako incydent w module EDR.

Badanie incydentów i wizualizacja

1. Produkt zapewnia wsparcie analizy incydentów poprzez dostarczenie narzędzi, które pomagają filtrować, badać i podejmować działania dotyczące wszystkich zdarzeń bezpieczeństwa wykrytych przez czujnik EDR w określonym czasie.
2. Produkt integruje się z bazą wiedzy MITRE ATT&CK i odpowiednio oznacza zdarzenia bezpieczeństwa.
3. Produkt zapewnia zaawansowaną wizualizację zdarzeń bezpieczeństwa z określonymi danymi lub działaniami z następującymi informacjami:
 - a) Karta podsumowująca zawiera przegląd wpływu zdarzenia i szczegółowe informacje o każdym węźle zdarzenia.
 - b) Funkcja osi czasu zbiera informacje o rozwoju zdarzenia bezpieczeństwa w kolejności chronologicznej.
 - c) System gromadzi informacje o działaniach podejmowanych przez produkt w związku ze zdarzeniem bezpieczeństwa.

Incydenty

1. Oprogramowanie pozwala na informowanie o zagrożeniach wykrytych i zablokowanych w formie grafu i chronologicznej linii zdarzeń oraz daje możliwość:
 - a) Filtrowania zdarzeń.
 - b) Zakończenia procesów.
 - c) Dodania procesów do czarnej listy.
 - d) Dodania procesów do białej listy.
 - e) Izolacji hosta.
 - f) Przesłania pliku do Sandbox.

- g) Sprawdzenia informacji o pliku w Google.
 - h) Sprawdzenia informacji o pliku w VirusTotal.
2. Możliwość szybkiego podglądu incydentów za pomocą spersonalizowanych widoków list lub widoku domyślnego.
 3. Możliwość wyświetlenia 10,20,30,50,100 zdarzeń na jednej stronie.
 4. System umożliwia blokowanie na podstawie utworzonych reguł czarnej listy przy pomocy kategorii:
 5. a) Hash MD5 lub SHA256.
 - b) Pełna ścieżka do aplikacji.
 - c) Reguła połączenia.
 6. Możliwość importu reguł czarnej listy dla hash, ścieżek do aplikacji oraz reguł połączeń z pliku CSV.
 7. System musi oferować szeroki zakres filtrowania dodanych reguł blokowania minimum po nazwie pliku, hash pliku, typu hash, ścieżce, protokole porcie/zakresie portów, daty dodania.
 8. Możliwość wygenerowania i wyeksportowania listy incydentów do pliku .csv.

Urządzenie do backupu danych NAS – Opis przedmiotu zamówienia

| Specyfikacja sprzętowa | |
|---|--|
| Procesor | Procesor 64 bit x86 o taktowaniu nie mniejszym niż 2.2 GHz |
| Procesor liczba rdzeni | Nie mniej niż 4 |
| Pamięć RAM | Nie mniej niż 4GB DDR4 |
| Pamięć RAM liczba slotów | Minimum 2 sloty |
| Pamięć RAM - możliwość rozszerzenia | Do urządzenia powinna zostać rozszerzona pamięć RAM do 16 GB |
| Pamięć Flash | Nie mniej niż 5 GB |
| Liczba zatok na dyski twarde | Minimum 8 |
| Obsługiwane dyski twarde | 3.5" oraz 2.5" SATA oraz 2.5" SATA SSD - do urządzenia muszą zostać dostarczone dyski HDD Sata 3,5" o poj. min. 4TB znajdujące się na liście kompatybilności serwera Wraz ze sprzętem powinno być dostarczone 10 dysków, w tym 2 dyski służące jako zapasowe w razie awarii dysku podstawowego |
| Pojemność dysków twardych możliwych do stosowania | do 20 TB |
| Obsługa dysków M2 PCIe | Tak, minimum 2 porty Gen3x1 - do urządzenia muszą zostać dostarczone dwa dyski M.2 500 GB PCI Express 3.0 NVMe, znajdujące się na liście kompatybilności serwera NAS |
| Możliwość podłączenia modułu rozszerzającego | Tak, minimum 2 |
| Porty LAN 2,5 GbE | Minimum 2 RJ-45 |
| Diody LED | Minimum Status, LAN, HDD |
| Porty USB 3.2 Gen2 (10 Gb/s) | Minimum 2 Typ C i 2 Typ A |
| Port PCIe | Tak, minimum 1 Gen3x8 |
| Przyciski | Reset, Zasilanie |
| Typ obudowy | RACK, 2U (szyny powinny być w zestawie) |
| Dopuszczalna temperatura pracy | od 0 do 40°C |
| Wilgotność względna podczas pracy | 5-95% R.H. |
| Zasilanie | Zasilacz redundantny 2 x 300W, 100-240 V |

| Specyfikacja oprogramowania | |
|---|---|
| Agregacja łączy | Tak |
| Obsługiwane systemy plików | Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+ |
| Szyfrowanie wolumenów | Tak, min AES 256 |
| Szyfrowanie dysków zewnętrznych | Tak |
| Zarządzanie dyskami | Pojedynczy Dysk, 0, 1, 5, 6, 10, 50, 60, JBOD, Obsługa Hot Spare per grupa RAID oraz global hot spare Rozszerzanie pojemności Online RAID Migracja poziomów Online RAID HDD S.M.A.R.T. Skanowanie uszkodzonych bloków (pliku) Przywracanie macierzy RAID Obsługa map bitowych Pula pamięci masowej Obsługa migawek Obsługa replikacji migawek |
| Wbudowana obsługa iSCSI | Multi-LUNs na Target Obsługa LUN Mapping & Masking Obsługa SPC-3 Persistent Reservation Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN |
| Zarządzanie prawami dostępu | Ograniczenie dostępnej pojemności dysku dla użytkownika Importowanie listy użytkowników Zarządzanie kontami użytkowników Zarządzanie grupą użytkowników Zarządzanie współdzieleniem w sieci Tworzenie użytkowników za pomocą makr Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL |
| Obsługa Windows AD | Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera LDAP |
| Funkcje backup | Oprogramowanie do tworzenia kopii bezpieczeństwa producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde, |
| Współpraca z zewnętrznymi dostawcami usług chmury | Przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box |

| | |
|---|--|
| Darmowe aplikacje na urządzenia mobilne | Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer / Odtwarzacz muzyki Dostępne na systemy iOS oraz Android |
| Minimum obsługiwane serwery | Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer multimediiów UPnP Serwer pobierania (HTTP / FTP) Serwer Monitoringu |
| VPN | VPN client / VPN server. Obsługa PPTP, OpenVPN |
| Administracja systemu | Połączenia HTTP/HTTPS Powiadamianie przez e-mail (uwierzytelnianie SMTP) Powiadamianie przez SMS Ustawienia inteligentnego chłodzenia DDNS oraz zdalny dostęp w chmurze SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP (USB) Obsługa sieciowej jednostki UPS Monitor zasobów Kosz sieciowy dla CIFS/SMB oraz AFP Monitor zasobów systemu w czasie rzeczywistym Rejestr zdarzeń Całkowity rejestr systemowy (poziom pliku) Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania Możliwość aktualizacji oprogramowania Ustawienia: Back up, przywracania, resetowania systemu |
| Wirtualizacja | Wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android. Dostęp do konsoli maszyn za pośrednictwem przeglądarki z HTML5 Funkcjonalności importu, eksportu, klonowania i wykonywania migawek maszyn wirtualnych. |
| Konteneryzacja | Możliwość uruchomienia wirtualnych kontenerów dla LXD i Docker |

| | |
|---|---|
| Zabezpieczenia | Filtracja IP Ochrona dostępu do sieci z automatycznym blokowaniem Połączenie HTTPS FTP z SSL/TLS (Explicit) Obsługa SFTP (tylko admin) Szyfrowanie AES 256-bit Szyfrowana zdalna replikacja (Rsync poprzez SSH) Import certyfikatu SSL Powiadomienia o zdarzeniach za pośrednictwem Email i SMS |
| Możliwość instalacji dodatkowego oprogramowania | Tak, sklep z aplikacjami; możliwość instalacji z paczek |
| Gwarancja | 3 lata |