Załącznik nr 2b

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA
CZĘŚĆ IV – DOSTAWY SPRZĘTOWE

1. Zakup i dostawa UTM

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy 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 4 administratorów do poszczególnych instancji systemu.
System musi wspierać 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 – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:

- 10 portami Gigabit Ethernet RJ-45.

2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 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 nie mniej niż 6 Gbps.
5. 7. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps.
6. 8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps.
7. 9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.

Funkcje Systemu Bezpieczeństwa:

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

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system

Polityki, Firewall

13. 2. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
14. 3. System musi zapewniać 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.

15. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
16. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
17. Element systemu realizujący funkcję Firewall musi integrować 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
- Google Cloud Platform (GCP).
- OpenStack.
- VMware NSX.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:

- Wsparcie dla IKE v1 oraz v2.
- Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
- Obsługa protokołu Diffie-Hellman grup 19 i 20.
- Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
- 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.
- Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
- Mechanizm „Split tunneling" dla połączeń Client-to-Site.

2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:

- Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.

- Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
- Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
- Routingu statycznego.
- Policy Based Routingu.
- Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Funkcje SD-WAN

1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.

3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać 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) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać 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. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
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 powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W przypadku kiedy usługa logowania i raportowania realizowana jest w chmurze, wykonawca musi dostarczyć stosowne licencje upoważniające do składowania logów przez okres co najmniej jednego roku.
3. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
4. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.

5. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

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

e) Licencja na usługę realizowaną w chmurze na okres 12 miesięcy umożliwiająca logowanie i raportowanie z czasem retencji logów minimum 1 rok.

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres min. 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Rozszerzone wsparcie serwisowe AHB/SOS

b) System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres [x] miesięcy.

c) Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 8x5 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 8x5 Oferent winien przedłożyć dokumenty:

- Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
- Certyfikat ISO 9001 podmiotu serwisującego.

2. <u>Przełącznik sieciowy (24 porty)</u>

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: 30 W.

- Minimalny zakres temperatury pracy: 0-40°C.

Interfejsy sieciowe - wymagania minimalne

1. Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:
   a) 24 porty GE RJ-45.
   e) 4 porty 10 GE SFP+.

Zarządzanie

- Wbudowany 1 port konsoli szeregowej do pełnego zarządzania.
- 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. 125 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 190 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.

Gwarancja oraz wsparcie

1. System musi być objęty serwisem gwarancyjnym producenta przez okres min. 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. ******* Stosujemy przy wsparciu 24x7 *******

Rozszerzone wsparcie serwisowe

1. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ******* Następnym Dniu Roboczym /w ciągu 8 godzin ******* od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres [x] miesięcy.

2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie ******* 8x5 / 24x7 ******* przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim ******* 8x5 / 24x7 *******. Oferent winien przedłożyć dokumenty:

- Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
- Certyfikat ISO 9001 podmiotu serwisującego.

3. <u>Przełącznik sieciowy /48 port/</u>

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^{o}C.

Interfejsy sieciowe - wymagania minimalne

1. Wymaganym 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.
- Musi być możliwe redundantne połączenie z elementami zarządzającymi.

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.

Gwarancja oraz wsparcie

System musi być objęty serwisem gwarancyjnym producenta przez okres min. 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. ******* Stosujemy przy wsparciu 24x7 *******

Rozszerzone wsparcie serwisowe

- System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ******* Następnym Dniu Roboczym /w ciągu 8 godzin ******* od momentu

potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres [x] miesięcy.

- Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie ******* 8x5 / 24x7 ******* przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim ******* 8x5 / 24x7 *******. Oferent winien przedłożyć dokumenty:
- Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
- Certyfikat ISO 9001 podmiotu serwisującego.

4. Urządzenia do backupu

Specyfikacja sprzętowa – dostawa serwerów NAS – 6 szt	
Procesor	Procesor 64 bit x86 o takowaniu nie mniejszym niż 2.2 GHz
Procesor liczba rdzeni	Nie mniej niż 4
Pamięć RAM	Nie mniej niż 8GB (oryginalne kości producenta lub oficjalne zamienniki z listy kompatybilności)
Pamieć RAM liczba slotów	Minimum 2 sloty
Pamięć RAM - możliwość rozszerzenia	Nie mniej niż do 64GB
Pamięć Flash	Nie mniej niż 5 GB
Liczba zatok na dyski	Minimum 8 zatok 3,5"
Obsugiwane dyski	3.5" HDD SATA oraz 2.5" HDD SATA oraz 2.5" SATA SSD
Wbudowane w urządzenie interfejsy na dyski M2	Wymagane min. 2 x M2 PCIe Gen3x1
Możliwość stosowania dysków twardych o pojemności	do 18TB
Możliwość podłączenia modułu rozszerzającego	Tak, co najmniej 2
Porty LAN 2,5 GbE	Minimum 2 RJ-45
Porty LAN 10 Gbe	Możliwość rozszerzenia poprzez kartę PCIe
Diody LED	Minimum Status, LAN, HDD
Porty USB 3.2 Gen2	Minimum 4
Port PCiE	Tak, minimum 2 Gen3x4
Przyciski	Reset, Zasilanie
Typ obudowy	Tower
Dopuszczalna temperatura	od 0 do 40˚C

pracy	
Wilgotność względna podczas pracy	5-95% R.H.
Zasilanie	Max. 250 W
Specyfikacja oprogramowania	
Obsługa dwóch systemów operacyjnych	Możliwość wyboru w trakcie inicjalizacji urządzenia systemu operacyjnego opartego na systemach plików EXT4 lub ZFS
Wymagania dla systemu operacyjnego opartego o system plików EXT4	
Agregacja łączy	Tak
Obsługiwane systemy plików	Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+, exFAT
Możliwość podłączenia karty WLAN na USB	Tak
Szyfrowanie udziałów	Tak, min AES 256
Szyfrowanie dysków zewnętrznych	Tak
Zarządzanie dyskami	Pojedynczy Dysk, 0, 1, 5, 6, 10, 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 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 plików 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 Dostępne na systemy iOS oraz Android
Minimum obsługiwane serwery	Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer multimediów UPnP Serwer pobierania (Bittorrent / 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 System plików dziennika Całkowity rejestr systemowy (poziom pliku) Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania automatyczna Możliwość aktualizacji oprogramowania ręcznie Ustawienia systemu: Kopia, Przywracanie, Resetowanie
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	Tak, sklep z aplikacjami; możliwość instalacji z paczek

oprogramowania	
Gwarancja	2 lata
Dyski (64 szt.)	
Kompatybilność	Kompatybilne z oferowanym urządzeniem (lista kompatybilności)
Pojemność	8TB
Technologia	HDD
Interfejs	SATA
Przepustowość Interfejsu	6Gb/s
Prędkość obrotowa [RPM]	7200
Format	3.5"
Pamięć podręczna (MB)	256
|Fizyczna wielkość sektora	512E
Rodzaj enkrypcji	SE
Stan	nowy
Gwarancja	2 lata, pozostawienie dysków u klienta w razie awarii
Specyfikacja wdrożenia	
Wdrożenie	-Inicjalizacja urządzenia - Konfiguracja puli pamięci oraz grup RAID - Konfiguracja sieci - Konfiguracja użytkowników i grup - Utworzenie folderów udostępnionych - Instalacja pakietów bezpieczeństwa - Zaawansowana konfiguracja migawek - Konfiguracja replikacji danych lub backupu - Uruchomienie dowolnych, dodatkowych usług na urządzeniu - Weryfikacja poprawności działania urządzenia

5. Wymagania dotyczące agregatu prądotwórczego

- agregat fabrycznie nowy wyprodukowany na terenie UE,
- rok produkcji 2021 lub 2022,
- agregat w obudowie wyciszonej, odpornej na warunki atmosferyczne,
- model agregatu G0110IVGR z układem SZR (Samoczynne Załączenie Rezerwy),
- moc znamionowa min: 100 kVA,
- silnik diesel produkcji UE,
- układ automatycznego podgrzewania paliwa,
- regulator obrotów silnika – elektroniczny,
- panel kontrolny G 545, j) maksymalne wymiary: 2350 mm x 1000 mm x 1600mm (dł x szer x wys), k) zbiornik paliwa minimum 190 l wykonany z tworzywa z wanną retencyjną,
- poziom hałasu, maksymalnie 61 dB(A) z 7 metrów,
- przycisk wyłączenia awaryjnego,
- konstrukcja prądnicy: samowzbudna, bezszczotkowa,
- częstotliwość 50 Hz,
- napięcie znamionowe - 230/400 V,
- klasa izolacji H, r) automatyczny regulator napięcia – elektroniczny AVR,
- gwarancja minimum 24 miesiące z limitem 3 000 motogodzin.

6. Macierz

Obudowa RACK 2U powinna pozwalać na zamontowanie 12 dysków 3.5". 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.

Kontrolery
W każdym z kontrolerów powinno być dostępne cztery porty iSCSI w standardzie SFP28 pracujące z prędkością do 25GB. Należy dodać cztery kable SFP28 do SFP28 25GB długości co najmniej 2m przeznaczone przez producenta do pracy z tym urządzeniem.

Dyski
W macierzy powinny być zainstalowane co najmniej sześć dysków co najmniej 12TB SAS wymienialne podczas pracy macierzy oraz sześć dysków co najmniej 1.92TB SSD SAS 24GB/s wymienialne podczas pracy macierzy. Macierz ma mieć możliwość rozbudowy do co najmniej 8PB z użyciem zainstalowanych kontrolerów

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 miedzy rożnymi 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 wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001. Urządzenie musi posiadać deklarację CE.

Warunki gwarancji

Minimum 2 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 5-miu lat. W przypadku naprawy dysku - uszkodzony dysk zostaje u klienta. Podczas trwania gwarancji producent powinien zapewnić narzędzia i procesy do proaktywnej oceny stanu technicznego oraz automatycznego zgłaszania usterek bez ingerencji człowieka. Powinna być możliwość skorzystania z pomocy wsparcia producenta za pomocą komunikatora np. messenger, teams, WhatsApp. Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje 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. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

7. Serwer

Element konfiguracji	Wymagania minimalne
Obudowa	Maksymalnie 2U RACK 19 cali (wraz z szynami montażowymi oraz ramieniem do prowadzenia kabli) Możliwość wyposażenia serwera w zamykany, zdejmowany panel przedni chroniący przed nieuprawionym dostępem do dysków Możliwość wyposażenia serwera w czujniki otwarcia obudowy współpracującego z BIOS/UEFI.
Procesor	Minimum 1 procesor 12-rdzeniowy, x86 - 64 bity, Intel Xeon Silver 4510 2.4GHz 12c lub równoważny procesor 12-rdzeniowy, Płyta główna wspierająca zastosowanie procesorów od 8 do 60 rdzeniowych, mocy do min. 350W i taktowaniu CPU do min. 3.6GHz.
Liczba procesorów	Min. 1 procesor
Pamięć operacyjna	128 GB RDIMM DDR5 4800 MT/s w modułach o pojemności 32GB każdy. Płyta główna z minimum 32 slotami na pamięć i umożliwiająca instalację do minimum 8TB.
Sloty rozszerzeń	3 aktywne gniazda PCI-Express generacji 5, w tym min. 3 slot x16 (szybkość slotu – bus width) pełnej wysokości (full height). Możliwość rozbudowy do 6 slotów PCI-Express generacji 5.

Dysk twardy	Zatoki dyskowe gotowe do zainstalowania 8 dysków SFF typu Hot Swap, NVMe/SAS/SATA/SSD, 2,5” i opcja rozbudowy/rekonfiguracji o dodatkowe 8 dysków typu Hot Swap, NVMe/SAS/SATA/SSD, 2,5”.. Zainstalowane minimum 5 dysków 1,92 TB NVMe
Kontroler	Serwer wyposażony w kontroler sprzętowy z min. 4GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę 16 napędów dyskowych NVMe/SAS oraz obsługujący poziomy: RAID 0/1/10/5/50/6/60. Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD jednocześnie
Interfejsy sieciowe	Minimum 4 wbudowane porty Ethernet 100/1000 Mb/s RJ-45 z funkcją Wake-On-LAN, wsparciem dla PXE, które nie zajmują gniazd PCIe opisanych w sekcji „Sloty rozszerzeń”.
Karta graficzna	Zintegrowana karta graficzna
Porty	4 x USB 3.0 (w tym 1 port wewnętrzny) 1x VGA Możliwość rozbudowy o: - dodatkowy port typu DisplayPort dostępny z przodu serwera - port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45
Napęd	Możliwość instalacji wewnętrznego napędu DVD-ROM lub DVD-RW
Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 1000W.
Karta/moduł zarządzający	Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia mininmalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność:

	• monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe • wparcie dla agentów zarządzających oraz możliwość pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP • dostęp do karty zarządzającej poprzez - dedykowany port RJ45 z tyłu serwera lub - przez współdzielony port zintegrowanej karty sieciowej serwera dostęp do karty możliwy - z poziomu przeglądarki webowej (GUI) - z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP) - z poziomu skryptu (XML/Perl) - poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface) • wbudowane narzędzia diagnostyczne • zdalna konfiguracji serwera(BIOS) i instalacji systemu operacyjnego • obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie • wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników • przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough) • obsługa zdalnego serwera logowania (remote syslog) • wirtualna zadalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów CD/DVD i USB i i wirtualnych folderów • mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie • funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności • monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji • konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping)

	• zdalna aktualizacja oprogramowania (firmware) • zarządzanie grupami serwerów, w tym: - tworzenie i konfiguracja grup serwerów - sterowanie zasilaniem (wł/wył) - ograniczenie poboru mocy dla grupy (power caping) - aktualizacja oprogramowania (firmware) - wspólne wirtualne media dla grupy • możliwość równoczesnej obsługi przez 6 administratorów • autentykacja dwuskładnikowa (Kerberos) • wsparcie dla Microsoft Active Directory • obsługa SSL i SSH • enkrypcja AES/3DES oraz RC4 dla zdalnej konsoli • wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API • wsparcie dla Integrated Remote Console for Windows clients • możliwość autokonfiguracji sieci karty zarządzającejj (DNS/DHCP)
Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	Microsoft Windows Server 2019, 2022 Ubuntu 22.04 LTS Red Hat Enterprise Linux (RHEL) 8.6 oraz 9.0 SUSE Linux Enterprise Server (SLES) 15 SP4 VMware ESXi 7.0 U3, 8.0, 8.0U1
Wsparcie techniczne	Min. 2-letnia gwarancja producenta w miejscu instalacji z pozostawieniem uszkodzonych dysków w miejscu instalacji Czas reakcji w miejscu instalacji w ciągu 4h od zgłoszenia usterki. Możliwość zgłaszania awarii w trybie 24x7. Wsparcie techniczne realizowane jest przez serwis producenta oferowanego serwera.
Inne	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja zgodności CE.

System operacyjny	1 x Microsoft Windows 2022 server standard 50 x Licencja CAL user do serwera Microsoft Windows 2022 server

PRACE DO WYKONANIA	1	szt
Dostawa i integracja ze środowiskiem sieciowym UG Czorsztyn	1	szt
Instalacja i konfiguracja środowiska wirtualizacyjnego HYPERV	1	szt
Instalacja i konfiguracja serwera domenowego oraz Active Directory	1	szt
Instalacja i konfiguracja serwera aplikacyjnego zgodnie z wymaganiami aplikacji wykorzystywanych w UG Czorsztyn	1	szt
Migracja i uruchomienie aplikacji systemu zarządzania jednostką administracji publicznej Ratusz wykorzystywanym w UG Czorsztyn (aplikacje podatkowe, finansowe, opłatowe)	1	szt

8. Zakup i dostawa dodatkowych 15 licencji specjalistycznego oprogramowania do zabezpieczenia przed ransomware dzięki technologi EDR (Endpoint Detection and Response)

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.

Rozwiązanie dla ochrony antywirusowej stacji roboczych wspiera następujące systemy operacyjne:

- Microsoft Windows 7 z dodatkiem SP1
- Microsoft Windows 8.1
- Microsoft Windows 10
- Microsoft Windows 11

- macOS 11 "Big Sur"
- macOS 10.15 "Catalina"
- macOS 10.14 "Mojave"

Rozwiązanie dla ochrony antywirusowej systemów serwerowych wspiera następujące systemy operacyjne:

- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Microsoft Windows Server 2022

Wspierane przeglądarki internetowe do obsługi konsoli zarządzającej:

- Microsoft Internet Explorer
- 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 podatnościami – 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

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.

Rozwiązanie posiada wbudowany mechanizm ochrony przed zagrożeniami typu ransonmware.
Rozwiązanie wspiera technologię Antimalware Scan Interface (AMSI)
Rozwiązanie umożliwia wybór plików do skanowania – wszystkich plików lub tylko plików o określonych rozszerzeniach.
W momencie wykrycia infekcji rozwiązanie automatycznie stara się wyleczyć plik a jeśli nie jest to możliwe przenosi go do bezpiecznego folderu kwarantanny.
Rozwiązanie posiada możliwość ręcznej reakcji na wykryte zagrożenie, w takim przypadku pozwala na: wyleczenie pliku, usunięcie, przeniesienie do kwarantanny, zmiany nazwy, zablokowania.
Rozwiązanie chroni plik systemowy HOSTS przed nieautoryzowanymi zmianami.
Rozwiązanie posiada mechanizmy skanujące dyski sieciowe.
Skanowanie dysków sieciowych jest możliwe dla dowolnych operacji na takich zasobach lub tylko przy wykonywaniu znajdujących się tam plików.
Rozwiązanie posiada możliwość tworzenia wykluczeń dla mechanizmów ochrony w czasie rzeczywistym, w tym co najmniej dla: plików, folderów, procesów.
Rozwiązanie posiada mechanizm ochrony ruchu http chroniący użytkownika przed malware oraz phishingiem.
Istnieje możliwość stworzenia wykluczenia dla wskazanej aplikacji, tak aby nie skanowała ona ruchu http.
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.
Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
Rozwiązanie posiada możliwość dystrybuowania aktualizacji baz definicji wirusów oraz aktualizacji oprogramowania zainstalowanego na stacji końcowej, za pomocą serwera pośredniczącego.
Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej do nowej wersji, następuje w sposób automatyczny, niewidoczny dla użytkownika końcowego.
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.
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.

Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej w określone dni i godziny tygodnia i miesiąca.

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.

Rozwiązanie posiada możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.
Rozwiązanie posiada możliwość wywołania procesu skanowania z niskim priorytetem, co pozwala na skanowanie z użyciem mniejszej ilości zasobów systemowych.
Rozwiązanie posiada możliwość wywołania skanowania uwzględnionych rozszerzeń a także ich wykluczanie.
Rozwiązanie posiada możliwość skanowania dysków przenośnych takich jak pendrive, dyski zewnętrzne itp.
Skanowanie dysków przenośnych może odbywać się w sposób automatyczny bez wiedzy użytkownika, automatycznie z wyświetleniem podsumowania skanowania użytkownikowi
Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie.
Rozwiązanie posiada funkcję skanowania na żądanie pojedynczych plików, katalogów, napędów przy pomocy skrótu w menu kontekstowym
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).
Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
Rozwiązanie posiada heurystyczną technologię do wykrywania nowych, nieznanych wirusów.
Umożliwia wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan", „rootkit".
Posiada mechanizm wykrywania nowych i nieznanych zagrożeń (0-day), bazujący na technologii chmurowej, analizującej podejrzane pliki wykonywalne (przez pliki wykonywalne rozumie się co najmniej: aplikacje, interpretowalną zawartość Flash, Sliverlight, skrypty oraz makra dokumentów pakietu Office).
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.
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.
Rozwiązanie posiada możliwość wyłączenia mechanizmu automatycznego przesyłania podejrzanych plików do dodatkowej analizy przez producenta.
Rozwiązanie posiada możliwość umieszczenia oprogramowania typu „spyware", „adware", „keylogger", „dialer", „trojan" w kwarantannie.

Rozwiązanie posiada możliwość obsługi plików skompresowanych obejmującego najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX.
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.
Rozwiązanie automatycznie powiadamia użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona.
Rozwiązanie posiada możliwość wyłączenia powiadomień dla użytkowników stacji końcowej o wykrytych zagrożeniach.
Rozwiązanie posiada możliwość wyłączenia interfejsu użytkownika oprogramowania zainstalowanego na stacji końcowej.
Rozwiązanie umożliwia blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.
Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez system reputacyjny producenta.
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.
Rozwiązanie jest wyposażone w mechanizm ochrony przeglądarki internetowej, w tym analizujący uruchamiane skrypty ActiveX i pobierane pliki.
Rozwiązanie posiada możliwość ochrony podczas przeglądania sieci Internet na podstawie badania reputacji witryn.
Rozwiązanie umożliwia blokowanie dostępu do kategorii witryn WWW skatalogowanych przez systemy producenta.
Oprogramowanie zapewnia co najmniej 30 kategorii klasyfikacji witryn WWW.
Użytkownik podczas próby przejścia na witrynę znajdująca się w zablokowanej przez Administratora kategorii, jest powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej.
Rozwiązanie umożliwia blokowanie witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS.
Rozwiązanie posiada wbudowany mechanizm zabezpieczenia połączenia do witryn skategoryzowanych przez producenta jako „bankowość elektroniczna” poprzez uniemożliwienie nawiązania nowych sesji do niezaufanych hostów na czas połączenia z bankiem.
W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie blokuje możliwość uruchamiania od strony chronionego hosta poleceń cmd oraz skryptów.

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.
Kontrola połączenia umożliwia zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora – administrator ma możliwość tworzenia własnej listy takich witryn.
Rozwiązanie posiada wbudowaną funkcję, która po zakończeniu sesji z witrynami sklasyfikowanymi jako „bankowość elektroniczna" czyści zawartość schowka systemowego.
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.
Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.
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.
Rozwiązanie posiada możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej).
Rozwiązanie umożliwia stworzenie zestawów reguł do natychmiastowego zastosowania, które zablokują komunikację sieciową w celu izolacji hosta na żądanie administratora.
Rozwiązanie jest wyposażone w mechanizm aktualizacji aplikacji (patch managment), umożliwiający instalację dostępnych poprawek dla systemu operacyjnego oraz aplikacji na nim zainstalowanych.
Mechanizm aktualizacji aplikacji (patch managment) nie wymaga instalowania dodatkowych agentów oprócz agenta AV.
Moduł aktualizacji aplikacji, okresowo skanuje aplikacje zainstalowane na stacji roboczej i umożliwia ich aktualizację do najnowszych wersji.
Moduł aktualizacji aplikacji pełni role mechanizmu łatającego podatności i instalującego aktualizacje oprogramowania, a nie jedynie pasywnego skanera luk w bezpieczeństwie aplikacji.
Administrator posiada możliwość określenia, kiedy i jakie aktualizacje mają zostać zainstalowane automatycznie.
Administrator posiada możliwość uruchomienia aktualizacji dla systemu operacyjnego jak i aplikacji znajdujących się na nim na żądanie dla wybranych lub wszystkich hostów.
Mechanizm aktualizacji aplikacji umożliwia automatyczne wyświetlenie komunikatu użytkownikowi od strony hosta o konieczności zamknięcia danej aplikacji, tak aby proces aktualizacji mógł się zakończyć.
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.
Administrator konsoli zarządzającej ma możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji.
Mechanizm aktualizacji aplikacji (patch managment) nie wymaga uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces.
Administrator ma możliwość zdefiniowania aplikacji, które nie podlegają aktualizacji, poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej.
Rozwiązanie umożliwia wyświetlenie w GUI od strony chronionego hosta informacji o brakujących poprawkach dla systemu lub aplikacji i umożliwienie, ich instalacji przez użytkownika końcowego.
System centralnego zarządzania prezentuje niezaktualizowane aplikacje występujące na wszystkich chronionych hostach lub listę nieaktualizowanego oprogramowania dla pojedynczej stacji końcowej.
Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.
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.
Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączania do stacji końcowej.
Lista urządzeń zaufanych jest tworzona co najmniej w oparciu o nazwę urządzenia i identyfikator sprzętowy.
Rozwiązanie posiada możliwość blokady zapisywania plików na zewnętrznych dyskach USB urządzenia takie są wówczas dostępne w trybie tylko do odczytu.
Mechanizm kontroli urządzeń umożliwia blokadę uruchamiania plików wykonywalnych z nośników pamięci. Blokada ta pozwala na korzystanie z pozostałych danych zapisanych na takich nośnikach.
Rozwiązanie posiada możliwość zabezpieczenia zmian w konfiguracji przez użytkownika końcowego przy wykorzystaniu hasła.
Zmiany w konfiguracji mogą być dokonywane przez użytkownika końcowego tylko dla poszczególnych funkcji aplikacji wskazanych przez administratora w profilu.
Rozwiązanie posiada możliwość przekazywania do konsoli administracji zdalnej kluczy odzyskiwania funkcji Bitlocker
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.
Moduł posiada możliwość pracy w trybie monitorowania (bez blokowania) przekazując administratorowi informacje dotyczące prób modyfikacji plików w chronionych folderach.

Administrator posiada możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.
Istnieje możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną antyransomware.
Rozwiązanie potrafi automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz daje możliwość wskazania zaufanych aplikacji przez administratora.
Rozwiązanie posiada funkcjonalność kontroli uruchamianych aplikacji.
Tryb kontroli aplikacji umożliwia uruchomienie wszystkich aplikacji, uruchomienie i monitorowanie wszystkich aplikacji, blokowanie niezaufanych aplikacji.
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.
Tworzone reguły dotyczyć mogą czynności: uruchomienia aplikacji, ładowania modułu, uruchomienia instalatora, dostępu do pliku.

Centralna administracja

1. Portal zarządzający jest dostępny w języku polskim.
2. Komunikacja pomiędzy portalem centralnego zarządzania a stacjami roboczymi odbywa się w formie zaszyfrowanej.
3. 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.
4. Interfejs zarządzania posiada funkcję wyświetlania monitów o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.
5. Interfejs jest wyposażony w panel kontrolny zawierający podsumowanie stanu bezpieczeństwa organizacji w postaci graficznych wykresów.
6. Wykresy są interaktywne, tzn. że po wybraniu interesującego elementu, następuje przekierowanie do zawierającego bardziej szczegółowe dane menu.
7. Rozwiązanie posiada dedykowaną zakładkę zawierającą informację o wszystkich hostach posiadających zainstalowane oprogramowanie do ochrony, w tym: ich nazwy, status ochrony, przypisany profil bezpieczeństwa.
8. Istnieje możliwość eksportu listy wszystkich hostów do pliku CSV.
9. Administrator ma możliwość wglądu w szczegóły zgłaszającego się hosta, w których zawarte są informacje dotyczące: ostatniego podłączenia do konsoli zarządzającej, wersji zainstalowanego produktu, systemu operacyjnego, stanu ochrony, akcji związanych z wykrytymi zagrożeniami i skanowaniami.
10. 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.

11. Komputery nie nawiązujące komunikacji z konsolą zarządzającą mogą być automatycznie usuwane z listy po określonym przez administratora czasie - co najmniej 60 dni.
12. Rozwiązanie posiada dodatkową zakładkę zawierającą informacje dotyczącą brakujących aktualizacji dla zainstalowanych aplikacji i systemu operacyjnego.
13. Istnieje możliwość posortowania i filtrowania brakujących poprawek pod względem ich poziomu krytyczności.
14. Informacje dotyczące brakujących poprawek dla aplikacji i systemu operacyjnego zawierają liczbę i typ hostów na których został wykryty brak danej poprawki.
15. Po wskazaniu danej poprawki administrator posiada możliwość jej instalacji na wskazanych komputerach lub na wszystkich komputerach i serwerach, dla których dana poprawka została wydana.
16. Administrator ma możliwość wglądu w historię instalowanych poprawek na chronionych hostach.
17. Rozwiązanie posiada moduł raportujący w którym wyświetlane są informacje dotyczące stanu ochrony, infekcji malware, instalowanych aplikacji.
18. Raporty mogą być tworzone zgodnie z harmonogramem i wysyłane na wskazane adresy email.
19. Rozwiązanie posiada wbudowany mechanizm zarządzania subskrypcjami, z możliwością dodawania nowych kluczy licencyjnych.
20. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.
21. 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.
22. Dodanie klucza licencyjnego skutkuje pojawieniem się dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym.
23. Rozwiązanie ma możliwość definiowania różnych profili ustawień dla chronionych urządzeń z poziomu portalu zarządzającego.
24. Profile mogą być przypisane do pojedynczych hostów lub do grup.
25. Istnieje możliwość porównania 2 profili konfiguracyjnych w celu wyświetlenia różnic pomiędzy nimi.
26. 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.

27. Z poziomu portalu zarządzającego istnieje możliwość pobrania plików instalacyjnych, wykorzystywanych do instalacji agenta na objętych licencją hostach.
28. Pliki instalacyjne mają posiadać plików .EXE, .MSI, .MPKG, .DEB, .RPM w zależności od platformy i typu systemu na jakich ma zostać zainstalowany agent.
29. Tworzone profile muszą dają administratorowi możliwość blokowania ustawień konfiguracyjnych aplikacji zainstalowanych od strony stacji roboczych w celu uniemożliwienia ich modyfikacji przez lokalnego użytkownika.
30. Portal zarządzający pozwala na zarządzanie oprogramowaniem instalowanym na urządzeniach mobilnych (smartphony) w przypadku posiadania odpowiedniej licencji.
31. Konsola posiada możliwość definiowania wielu kont administratorów o różnych poziomach dostępu.
32. W ramach posiadanych licencji istnieje możliwość przenoszenia oprogramowania w ramach danego klucza subskrypcji z jednej stacji roboczej na inną.

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 podatnościami – 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 możliwość instalacji agenta monitorowania na stacjach roboczych z co najmniej następującymi systemami operacyjnymi:

- Microsoft Windows 7 z dodatkiem SP1
- Microsoft Windows 8.1 (32-bit i 64-bit)
- Microsoft Windows 10
- Microsoft Windows 11
- MacOS 11 “Big Sur”
- MacOS 10.15 “Catalina”
- MacOS 10.14 “Mojave”

Rozwiązanie posiada możliwość instalacji agenta monitorowania na serwerach z co najmniej następującymi systemami operacyjnymi:

- Microsoft® Windows Server 2012
- Microsoft® Windows Server 2016
- Microsoft® Windows Server 2019
- Microsoft® Windows Server 2022

Wspierane przeglądarki internetowe:

- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari

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. Maksymalna ilość wysyłanych danych przez agenta uruchomionego na stacji roboczej z systemami Windows nie przekracza 25MB na 24 godziny.

10. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, z centrum przetwarzania danych producenta, odbywa się jedynie z wykorzystaniem protokołów HTTP oraz HTTPS.
11. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, wspiera komunikację za pomocą serwera pośredniczącego http (http proxy).
12. 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.
13. Dane zbierane przez agentów na stacjach końcowych i serwerach są, przechowywane i przetwarzane na obszarze Europejskiej Wspólnoty Gospodarczej.
14. Rozwiązanie na bazie zebranych danych generuje detekcje, które stanowią powiązane ze sobą podejrzane zdarzenia, zebrane przez agentów ze stacji roboczych i serwerów.
15. Detekcje są generowane za pomocą statycznych reguł, przygotowanych przez producenta, jak również przy wykorzystaniu mechanizmów uczenia maszynowego uwzględniających specyfikę pracy środowiska informatycznego.
16. Detekcje są generowane w czasie rzeczywistym na podstawie danych zebranych i przesłanych przez agentów uruchomionych na stacjach końcowych i serwerach w środowisku informatycznym.
17. Detekcje widoczne są w konsoli zarządzającej w postaci graficznych diagramów, przedstawiających wykryte anomalie i powiązania pomiędzy biorącymi udział w detekcji elementami.
18. Detale dotyczące detekcji przedstawiane są w postaci drzewa zawierającego szczegółowe informacje dotyczące poszczególnych elementów biorących udział w wykrytej anomalii.
19. Rozwiązanie posiada możliwość filtrowania zdarzeń biorących udział w detekcji w zależności od poziomu ryzyka – od poziomu informacyjnego do zdarzeń o charakterze krytycznym.
20. 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).

21. 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).
22. 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).
23. Rozwiązanie umożliwia oznaczanie wygenerowanych detekcji jako błędne.
24. Oznaczenie detekcji jako błędnej, musi powodować, automatyczne identyfikowanie przyszłych takich samych detekcji i odpowiednie ich oznaczenie w interfejsie centralnego zarządzania.
25. Rozwiązanie posiada możliwość stworzenia archiwum zawierającego dodatkowe informacje dotyczące hosta, na którym wystąpiła detekcja w celu przeprowadzenia analizy śledczej incydentu.
26. Rozwiązanie pozwala na dodanie własnego komentarza przy wykrytej detekcji.
27. Rozwiązanie umożliwia wykupienie usługi pozwalającej na przesłanie detekcji do laboratorium producenta w celu analizy, zwrotnie administrator otrzymuje szczegółowy raport przygotowany przez analityka dotyczący incydentu.
28. Rozwiązanie monitoruje aplikacje uruchomione na stacjach roboczych i serwerach i oznacza aplikacje zidentyfikowane jako szkodliwe lub potencjalnie niebezpieczne dla użytkownika.
29. Rozwiązanie pozwala na przesłanie wiadomości e-mail informującej o wygenerowaniu nowej detekcji w systemie.
30. Rozwiązanie pozwala na izolację sieciową komputerów przez administratora.
31. Rozwiązanie umożliwia tworzenie reguł automatycznej izolacji stacji roboczych i serwerów, jeśli zostaną one uwzględnione w wygenerowanych detekcjach.
32. 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.
33. Rozwiązanie umożliwia tworzenie raportów zawierających co najmniej listę wygenerowanych detekcji, wraz z ich opisem, za zadany okres.
34. Rozwiązanie pozwala na eksport raportów, w postaci plików PDF.
35. Rozwiązanie wspiera dostęp do danych na temat utworzonych detekcji za pomocą interfejsu REST API, na potrzeby integracji z innymi systemami zabezpieczającymi.
36. Konsola centralnego zarządzania, oferuje interfejs w języku Polskim.
37. Konsola zarządzająca wyposażona jest w panel kontrolny (dashboard) w którym administrator ma możliwość weryfikacji stanu bezpieczeństwa organizacji.

38. 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.
39. Konsola wyposażona w dedykowaną zakładkę zawierającą listę urządzeń posiadających zainstalowanego agenta systemu EDR.
40. 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.
41. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.
42. Portal zarządzający umożliwia dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu EPP, mechanizmów zarządzania podatnościami, ochrony usług Microsoft 365.
43. Dodanie klucza licencyjnego skutkuje pojawieniem się dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym.

9. Dyski do serwera Qnap w ilości 6 sztuk

Dyski musza być klasy serwerowej (enterprise)

- Dyski SATA 6 Gbit/s, **8 TB**
- Obroty minimalnie 7200 / min
- Dyski musza posiadać MTTF (MTBF) nie mniejszy niż 2 000 000h
- Pojemność pamięci cache minimum 256 MB
- Znamionowe roczne obciążenie pracą 550TB (rocznie)
- Parametr maksymalnej utrzymywanej prędkość przesyłu danych (deklarowana przez producenta dysków) :dla technologii sektorowej 512e: 248 MiB/s - dla pojemności 8TB

Gwarancja 2 lata, gwarancja musi zawierać opcje pozostawienie dysków w razie awarii przez cały okres trwania gwarancji.

Opisy do wymagań ogólnych

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć 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. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.