Załącznik nr 2 B do SWZ Szczegółowy opis przedmiotu zamówienia

I. Ogólne warunki realizacji:

1. W ramach zadania Wykonawca dostarczy sprzęt i oprogramowanie wyszczególnione w niniejszym dokumencie oraz dokona wdrożenia zgodnego z opisem w sekcji „Wdrożenie".

2. Wymagania ogólne dla dostarczanego sprzętu i oprogramowania (dotyczy wszystkich systemów opisanych w tym dokumencie):

- Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów z obszaru Unii Europejskiej;
- Niedopuszczalne są produkty prototypowe, nie dopuszcza się urządzeń długotrwale magazynowanych oraz pochodzących z programów wyprzedażowych producenta. Urządzenia nie mogą się znajdować się na liście „end-of-sale" oraz „end-of-support" producenta;
- Zamawiający wymaga, by dostarczone urządzenia były nowe (tzn. wyprodukowane nie dawniej, niż na 6 miesięcy przed ich dostarczeniem, przy czym w przypadku zasilacza UPS data produkcji ma być nie dawniej niż 1 miesiąc przed jego dostarczeniem) oraz by nie były używane (przy czym Zamawiający dopuszcza, by urządzenia były rozpakowane i uruchomione przed ich dostarczeniem wyłącznie przez Wykonawcę i wyłącznie w celu weryfikacji działania urządzenia, przy czym jest zobowiązany do poinformowania Zamawiającego o zamiarze rozpakowania sprzętu, a Zamawiający ma prawo inspekcji sprzętu przed jego rozpakowaniem);
- Zamawiający wymaga, by dostarczone licencje na oprogramowanie i systemy operacyjne były nowe i nie były nigdy wcześniej aktywowane czy używane na innych urządzeniach;
- Musi posiadać stosowny pakiet usług gwarancyjnych świadczonych przez producenta sprzętu (lub autoryzowany serwis) kierowanych do użytkowników z obszaru Rzeczpospolitej Polskiej;
- Całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne producentów sprzętu;
- Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji w formie papierowej lub elektronicznej;
- Do każdego urządzenia musi być dostarczony komplet nośników umożliwiających odtworzenie oprogramowania zainstalowanego w urządzeniu;
- Wymagane jest utrzymanie świadczeń gwarancyjnych (przez producenta urządzeń lub jego autoryzowaną placówkę serwisową) także w przypadku bankructwa Wykonawcy niemożliwości ich wypełnienia przez Wykonawcę (np. w przypadku jego bankructwa);
- Wykonawca zapewnia i zobowiązuje się, że korzystanie przez Zamawiającego z dostarczonych produktów nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich;
- Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V ±10%, 50Hz;
- Wszystkie urządzenia zostaną dostarczone z niezbędnym okablowaniem zasilającym i transmisyjnym;
- Wszystkie dostarczone w ramach niniejszego postępowania programy komputerowe muszą zostać zarejestrowane przez Wykonawcę;

- W cenę musi być wliczony koszt dostawy - transportu;
- Wykonawca zapewni dostawę do wskazanej lokalizacji w siedzibie Zamawiającego w dni powszednie w godzinach 8-15;
- Zamawiający opisując przedmiot zamówienia przy pomocy określonych norm, aprobat czy specyfikacji technicznych i systemów odniesienia dopuszcza rozwiązania równoważne opisywanym. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów uwiarygodniających te rozwiązania;
- Rozwiązanie równoważne musi pozwalać na zrealizowanie zakładanego przez Zamawiającego celu poprzez parametry wydajnościowe i funkcjonalne.

II. Wdrożenie:

Instalacja i wdrożenie UTM w PSP Chróścice oraz w Gminnym Ośrodku Pomocy Społecznej

1. Wykonawca przygotuje i omówi koncepcję konfiguracji z administratorem sieci Zamawiającego.
2. Wykonawca będzie uzgadniał z Zamawiającym harmonogram dostawy i montażu.
3. Wdrożenia nowych urządzeń UTM musi uwzględniać aspekt współpracy/integracji z innymi systemami i urządzeniami (typu przełączniki, Active Directory) będących w posiadaniu Zamawiającego. Dodatkowo każda zmiana w koncepcji musi być każdorazowo uzgadniana z administratorem sieci.
4. Wykonawca zamontuje urządzenia w szafie rack Zamawiającego uwzględniając wszelkie aspekty związanie z montażem tego typu urządzeń przewidzianych przez producenta dostarczanych rozwiązań.
5. Wdrożenie firewalla na styku z siecią Internet w zakresie minimum:
   a. rejestracja i aktualizacja do najnowszej stabilnej wersji OS (o ile wymagane jest to przez producenta),
   b. podłączenie i konfiguracja redundantnego łącza WAN,
   c. konfiguracja routingu,
   d. konfiguracja polityk bezpieczeństwa (reguły dostępu dla ruchu z Internetu, do Internetu) zgodnie z wytycznymi ze strony Zamawiającego,
   e. konfiguracja filtracji stron WWW na podstawie kategorii oraz treści,
   f. konfiguracja, dostępu zdalnego SSL VPN (VPN Client, portal WebVPN) dla 2 kont,
   g. integracja systemu firewall z dostarczanymi przełącznikami,
   h. integracja systemu firewall z posiadanymi przełącznikami Zamawiającego.
6. Wykonawca dodatkowo skonfiguruje dla jednego administratora logowanie do systemu z wykorzystaniem MFA. Zamawiający dopuszcza wykorzystanie ścieżki: Email, sms, token.
7. Wykonawca omówi z Zamawiającym stan końcowy konfiguracji, przedstawi zmiany naniesione na urządzeniu i w porozumieniu z Zamawiającym dopracuje szczegółowość konfiguracji.
8. Przeprowadzenie szkolenia z obsługi sprzętu dla administratorów min w zakresie:
   · Firewall konfiguracja:

- Polityki firewall
- Polityki ochrony DOS
- Zarządzanie pasmem
- Profile utm konfiguracja:
- Antivirus
- Web filter
- Dns filter
- Application control
- Interusion prevention
- VPN konfiguracja:
- SSL-VPN
- IPSEC dialup
- IPSEC SITE-TO-SITE
- Logowanie / alertowanie / debugowanie
- Przekazanie dokumentacji powdrożeniowej.

Wdrożenie serwer:

1. Wykonawca będzie uzgadniał z Zamawiającym harmonogram dostawy i montażu.
2. Wdrożenie nowych urządzeń - serwery i zasilacze awaryjne musi uwzględniać aspekt współpracy/integracji z innymi systemami i urządzeniami (typu przełączniki, Active Directory) będących w posiadaniu Zamawiającego.
3. Wykonawca zamontuje urządzenia w szafie rack Zamawiającego uwzględniając wszelkie aspekty związanie z montażem tego typu urządzeń przewidzianych przez producenta dostarczanych rozwiązań.
4. Wykonawca dostarczy wszystkie niezbędne kable do połączenia dostarczonych urządzeń ze sobą i siecią Zamawiającego.
5. Konfiguracja RAID z dysków w serwerze
6. Instalacja, aktywacja i aktualizacja dostarczonego systemu operacyjnego
7. Zamawiający wymaga uruchomienia oraz przetestowania środowiska wirtualnego, co najmniej w zakresie:
   a. Przygotowanie serwerów do instalacji oprogramowania wirtualizacyjnego – aktualizacja oprogramowania układowego do najnowszych stabilnych wersji oferowanej przez producenta,
   b. Instalacja oprogramowania wirtualizacyjnego na dostarczonych serwerach,
   c. Instalacja najnowszych poprawek do środowiska wirtualizacyjnego oferowanych przez producenta oprogramowania wirtualizacyjnego oraz przez producenta serwerów,
   d. Konfiguracja i podłączenie serwerów wirtualizacyjnych do zasobu dyskowego,
   e. Konfiguracja i podłączenie serwerów wirtualizacyjnych do sieci LAN Wnioskodawcy. Zamawiający wymaga, aby każdy z serwerów wirtualizacyjnych był podłączony do sieci LAN, co najmniej taką liczbą portów, by w przypadku niedostępności (awarii) n-(n-1) ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) był zachowany dostęp do sieci LAN,
   f. Konfiguracja sieci w infrastrukturze wirtualnej,
   g. Przygotowanie koncepcji wirtualizacji fizycznych maszyn,
   h. Instalacja i konfiguracja oprogramowania zarządzającego środowiskiem wirtualnym,
   i. Migracja istniejącej infrastruktury do środowiska wirtualnego,

j. Konfiguracja uprawnień w środowisku wirtualizacyjnym – integracja z usługą katalogową,
k. Konfiguracja powiadomień o krytycznych zdarzeniach (email).

8. Instalacja oprogramowania baz danych, oprogramowania antywirusowego, oprogramowania zarządzania zasilaczem UPS (wraz z konfiguracją i testowaniem działania zasilacza UPS
9. Przeprowadzenie instruktażu stanowiskowego z konfiguracji oraz „dobrych praktyk" w zakresie stosowanej technologii (dla 1 administratora min. 3 godziny), w trakcie którego będą poruszone poniższe zagadnienia:
   - tworzenie i konfiguracja wirtualnych dysków
   - tworzenie i konfiguracja maszyn wirtualnych
   - zarządzanie migawkami maszyn wirtualnych
   - import maszyn wirtualnych
   - skalowania maszyn wirtualnych
   - replikacja oraz odzyskiwanie po awarii
10. Przekazanie dokumentacji powdrożeniowej.
11. Testy funkcjonalne.

Przełączniki sieciowe oraz Acces Pointy

1. Montaż przełączników w miejscu wyznaczonym przez zamawiającego
2. Podstawowa konfiguracja przełączników
3. Konfiguracja interfejsów sieciowych przełączników

Segmentacja sieci z użyciem UTM i przełączników sieciowych

Wdrożenie oprogramowania do tworzenia i zarządzania kopiami bezpieczeństwa

1. Instalacja konsoli zarządzającej
2. Instalacja oprogramowania na urządzeniach końcowych
3. Konfiguracja miejsca docelowego dla backupu urządzeń końcowych
4. Konfiguracja oprogramowania zgodnie z wymaganiami zamawiającego
5. Testy funkcjonalne

Wdrożenie serwera NAS w Gminnym Ośrodku Pomocy Społecznej

1. Aktualizacja firmware
2. Konfiguracja RAID
3. Konfiguracja ustawień sieciowych
4. Instalacja dysków
5. Testy funkcjonalne

UPS

Podłączenie do przygotowanej instalacji elektrycznej przez Autoryzowany Serwis Producenta uwzględniające podłączenie wejścia zasilania do BYPASS, podłączenie BYPASS do UPS, podłączenie wyjścia do BYPASS, dostawa, pierwsze uruchomienie, szkolenie z obsługi.

Testy powdrożeniowe

Po dokonaniu całości wdrożenia należy:

a) Przeprowadzić testy poprawności działania całej infrastruktury;

b) Przygotować dokumentację powykonawczą zawierająca listę dostarczonego sprzętu wraz z numerami seryjnymi i opisem konfiguracji poszczególnych elementów systemów.

III. Sprzęt:

Szkoła Chrościce

1. Access Point (4 szt.) - serwis i gwarancja 2 lata

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

Parametry:

1. Obudowa urządzenia musi umożliwiać montaż na ścianie wewnątrz budynku lub umożliwiać posadowienie na biurku za pomocą odpowiedniej podstawki i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych:
    1. Temperatura 0–50°C,
    2. Wilgotność 10–90%.
2. Urządzenie musi być dostarczone z elementami mocującymi do ściany. 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 następujące standardy:
    1. 2.4 GHz 802.11b/g/n,
    2. 5 GHz 802.11a/n/ac/ax,
    3. Skaner 2.4GHz i 5GHz
4. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 16 SSID.
5. Urządzenie musi być wyposażone w moduł BLE.
6. Urządzenie musi być wyposażone w co najmniej w cztery interfejsy Ethernet 10/100/1000 Base-TX,
7. Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3at lub zewnętrzny zasilacz.
8. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych:
    1. Tunnel,
    2. Bridge,
    3. Mesh.
9. Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja.
10. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA-PSK, WPA-TKIP, WPA2-AES, WPA3, Web Captive Portal, MAC blacklist & whitelist, 802.11i, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, PEAP, EAP-FAST, EAP-SIM, EAP-AKA).
11. Interfejs radiowy urządzenia powinien wspierać następujące funkcje:
    1. MIMO – 2x2,
    2. Maksymalna przepustowość dla poszczególnych modułów radiowych:
        1. 574 Mbps;
        2. 1200 Mbps;

3. Wymagana moc nadawania:
    1. min. 25 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm;
    2. min. 21 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;
4. Wsparcie dla 802.11n 20/40Mhz HT,
5. Wsparcie dla kanałów 80MHz,
6. Anteny – wbudowane dla nadajników standardu 802.11 o zysku min. 4dBi.
7. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy,
8. Maksymalna deklarowana liczba klientów per moduł radiowy:
    1. 512;
    2. 512;

12. Funkcje dodatkowe:
    1. OFDMA UL i DL
    2. Spatial Reuse (BSS Coloring)
    3. UL-MU-MIMO 802.11ax
    4. DL-MU-MIMO
    5. Enhanced Target Wake Time (TWT)

Gwarancja oraz wsparcie

Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji oraz być objęte minimum dwuletnim serwisem gwarancyjnym producenta, 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.

2. UTM (1 szt.)

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.
5. 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. 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. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.

8. 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

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. 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.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
5. 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 18000 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 5000 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 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.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.

4. 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:

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

Gwarancja oraz wsparcie

Gwarancja: System musi być objęty minimum dwuletnim serwisem gwarancyjnym producenta, 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.

3. Switch zarządzalny (2 szt.) z serwisem na 2 lata

Przełącznik sieciowy

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

W celu realizacji bezpiecznej infrastruktury teleinformatycznej, wymaganym jest dostarczenie przełącznika oraz innych elementów funkcjonalnych, współpracujących z oferowanym systemem bezpieczeństwa UTM.

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

System musi być objęty minimum dwuletnim serwisem gwarancyjnym producenta, 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.

Gminny Ośrodek Pomocy Społecznej (GOPS)

1. Serwer NAS (1 szt.)

Procesor	4-rdzenie/4-wątki,

	Architektura procesora 64-bitowy x86
Wbudowana pamięć RAM	8 GB
Rodzaj pamięci	On-board DDR4
Wbudowana pamięć flash	4 GB
Liczba zainstalowanych dysków tw.	2 dyski, dyski muszą znajdować się na liście kompatybilności oferowanego serwera NAS
Pojemność zainstalowanych dysków	2TB
Typ dysku	HDD
Obsługa hot-swap dysków	Tak
RAID	Tak
Poziomy RAID	0,1
Architektura sieci	GigabitEthernet
Interfejs sieciowy	2 x 10/100/1000/2500 Mbit/s
Gniazda we/wy	1 x HDMI
	2 x USB 2.0
	2 x RJ-45 LAN
	2 x USB 3.1
Liczba wentylatorów	1
Wentylator	7 cm
Obudowa	Tower
Gniazda rozszerzeń	1 x PCIe 3.0 x 2
Zasilanie	Zasilacz 65W, 100-240 V

2. UTM z licencją na 2 lata (1 szt.)

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.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:

- 5 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 5 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 4 Gbps.
5. 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 Gbps.

6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 600 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 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

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. 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.

3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
5. 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 18 000 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 5 000 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 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.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. 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:
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.

Gwarancja oraz wsparcie

Gwarancja: System musi być objęty minimum dwuletnim serwisem gwarancyjnym producenta 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.

Urząd Gminy w Dobrzeniu Wielkim

1. Zasilacz UPS (1 szt.)

PARAMETR	WYMAGANIA MINIMALNE
Moc wyjściowa	15kVA/15kW
Topologia	VFI-SS-111
Sprawność całkowita dla Pmax (dla VFI)	<93%
Sprawność całkowita dla Pmax (dla ECO)	>98%
Chłodzenie	wymuszone, wewnętrzne wentylatory
Temperatura przechowywania	0 ÷ +40 °C
Temperatura pracy	+10 ÷ +40 °C
Stopień ochrony	IP20
PROSTOWNIK	
Zakres napięcia wejściowego	173 ÷ 485 V AC ± 2 %
Zakres częstotliwości wejściowej	45 ÷ 55 Hz ± 1 Hz
Współczynnik mocy PF (bez zewnętrznych układów kompensujących, realizowane za pomocą układu prostownika)	> 0,99
Moc bierna pojemnościowa (bez zewnętrznych układów kompensujących, realizowane za pomocą układu prostownika)	0 var
Współczynnik tg φ (bez zewnętrznych układów kompensujących, realizowane za pomocą układu prostownika)	< 0,4
Zniekształcenia prądu wejściowego THDi (bez zewnętrznych układów filtrujących, realizowane za pomocą układu prostownika)	< 3%
FALOWNIK	

Znamionowe napięcie wyjściowe	3x400 V AC
Częstotliwość napięcia wyjściowego	Synchroniczne z siecią / 50Hz ± 0,1 Hz
Regulacja statyczna napięcia	< 1 %
Zniekształcenia napięcia wyjściowego THDu	< 2% dla Pmax (liniowe)
	< 5 % (nieliniowe wg PN EN 62040-3)
Współczynnik szczytu CF	5:1
Praca ze 100% asymetrią obciążenia wyjścia (100% obciążenia jednej fazy przy zerowym obciążeniu pozostałych)	wymagana
Przeciążalność	130% - 10min / 160% - 1min / 300% 100ms
CZAS PRACY	
Czas pracy z baterii	minimum 25 minut dla obciążenia 12,052 kW
akumulatory	akumulatory o pojemności nie mniejszej niż 7Ah, akumulatory szczelne bezobsługowe, zainstalowane wewnątrz UPS, o projektowanej żywotności minimum 3-5 lat
WYPOSAŻENIE	
Sygnalizacja	akustyczno-diodowa, wyświetlacz LCD z menu w języku polskim
Interfejs komunikacyjny	RS232, RS485, USB, SNMP, bezpotencjałowe wyjścia programowalne (min. 4), wejścia sterujące (min. 4)
EPO	wymagane / standard NC
Oprogramowanie	oprogramowanie w języku polskim do zarządzania i monitorowania pracy UPS
	wymagane wsparcie producenta (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów.

	możliwość edycji nazw urządzeń na liście monitorowanych zasilaczy UPS
	wsparcie dla systemów Linux, Windows oraz wirtualizacji Hyper-V, Vmware, XenServer
Koła transportowe z minimum dwoma kołami skrętnymi umożliwiającymi swobodne przemieszczanie urządzenia	wymagane
WYPOSAŻENIE DODATKOWE	
Zewnętrzny bezprzerwowy układ obejściowy tzw. BY-PASS pozwalający na naprawę, konserwację lub wymianę akumulatorów w UPSie bez przerwy w zasilaniu podłączonych urządzeń.	wymagane
PARAMETRY MECHANICZNE	
Wymiary UPS (wys. X szer. X gł.)	nie większe niż 900 x 440 x 860 mm
Masa zasilacza	nie większa niż 280 kg
GWARANCJA / SERWIS	
Gwarancja	Możliwość rozszerzenia gwarancji do 60 miesięcy na elektronikę.
Przeglądy gwarancyjne	minimum 1 przegląd gwarancyjny realizowany przez serwis producenta uwzględniający: pomiary napięcia i prądy we/wy UPS, wykonanie rozładowania kontrolnego niezależnym obciążeniem z pomiarem czasu podtrzymania, pomiar rezystancji wewnętrznej oraz napięć akumulatorów
Czas naprawy	max. 14 dni roboczych
Serwis	Autoryzowany serwis producenta zlokalizowany w Polsce

	W przypadku braku możliwości dokonania naprawy w miejscu instalacji urządzenia - oferent dostarczy i podłączy w tym samym dniu sprzęt zastępczy o nie gorszych parametrach niż oferowany
	Serwis realizowany w systemie on-site (w miejscu zainstalowania UPSa)
USŁUGI	
Instalacja oraz uruchomienie Zasilacza UPS w miejscu wskazanym przez zamawiającego	wymagane
Instalacja zewnętrznego układu bypass w miejscu wskazanym przez zamawiającego	wymagane
szkolenie z obsługi Zasilacza UPS	wymagane
POZOSTAŁE	
Certyfikaty / dokumenty / oświadczenia producenta sprzętu (załączyć do oferty)	ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania - należy dołączyć do oferty dokument potwierdzający spełnienie wymagań
	deklaracja CE wystawiona w oparciu o obowiązujące normy (LVD, EMC)
	Wymagane dołączenie do oferty karty katalogowej oferowanego sprzętu
	Do każdego zasilacza UPS wymagane dołączenie dokumentu potwierdzającego realizację gwarancji lub przeglądów przez serwis producenta (zapis w karcie gwarancyjnej lub oświadczenie producenta)
	dostarczane urządzenie (UPS) będzie fabrycznie nowe, wyprodukowane nie wcześniej, niż na 1 miesiąc przed ich dostarczeniem

	sprzęt i oprogramowanie będzie pochodzić z autoryzowanego kanału sprzedaży

2. Serwer (1 szt.)

Obudowa	Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2,5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
Procesor	Zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.6GHz każdy, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 168 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. Płyta główna powinna obsługiwać CPU do 64 rdzeni.
RAM	Minimum 128GB DDR5 ECC RDIMM 4800MT/s, w minimum 4 kościach w celu zwiększenia wydajności oferowanego rozwiązania. Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1.5TB pamięci RAM.
Funkcjonalność pamięci RAM	Demand Scrubbing, Patrol Scrubbing, Permanent Fault Detection (PFD) lub równoważne.
Gniazda PCI	- minimum 1x slot PCIe 16x generacji 4 - minimum 2x slot PCIe 8x generacji 4

Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez zainstalowanie karty w wymaganych slotach PCIe).
Dyski twarde	Możliwość instalacji dysków SATA/SAS. Zainstalowane 4 dyski SSD SATA o pojemności min. 1.92TB, 6Gb, 2,5“ Hot-Plug. Konfiguracja RAID 5. Możliwość zainstalowania karty wyposażonej w dwa dyski M.2 NVMe o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1.
Kontroler RAID	Zainstalowany sprzętowy kontroler dysków SAS/SATA z 8GB cache z podtrzymaniem oraz funkcjonalnością RAID 0,1,10,5,6,50,60.
Wbudowane porty	4 x USB z czego nie mniej niż 1x USB 3.0, 2x VGA
Zasilacze	Redundantne, Hot-Plug min. 700W każdy.
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panelu zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
Diagnostyka	Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze.

System operacyjny/System wirtualizacji	Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze. System musi być objęty licencją dostępową (o ile wymagania licencyjne producenta oprogramowania tego wymagają) dla 50 Użytkowników/Urządzeń Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy. 1) Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 3) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. 4) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 9) Wbudowane wsparcie instalacji i pracy na wolumenach, które: a) pozwalają na zmianę rozmiaru w czasie pracy systemu, b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,

	c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d) umożliwiają zdefiniowanie list kontroli dostępu (ACL). 10) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 11) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 12) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 13) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 14) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 15) Dostępne dwa rodzaje graficznego interfejsu użytkownika: a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 16) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 17) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 18) Mechanizmy logowania w oparciu o: a) Login i hasło, b) Karty z certyfikatami (smartcard), c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 19) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.. 20) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).

	21) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 22) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 23) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 24) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 25) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1. c) Zdalna dystrybucja oprogramowania na stacje robocze. d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: i. Dystrybucję certyfikatów poprzez http ii. Konsolidację CA dla wielu lasów domeny, iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,

	iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. f) Szyfrowanie plików i folderów. g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. i) Serwis udostępniania stron WWW. j) Wsparcie dla protokołu IP w wersji 6 (IPv6), k) Wsparcie dla algorytmów Suite B (RFC 4869), l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych. iii. Obsługi 4-KB sektorów dysków iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) 26) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 27) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).

	28) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 29) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 30) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. 31) Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: ● zdalny dostęp do graficznego interfejsu Web karty zarządzającej; ● zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); ● szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; ● możliwość podmontowania zdalnych wirtualnych napędów; ● wirtualną konsolę z dostępem do myszy, klawiatury; ● wsparcie dla IPv6; ● wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; ● możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; ● możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; ● integracja z Active Directory; ● możliwość obsługi przez dwóch administratorów jednocześnie; ● wsparcie dla dynamic DNS; ● wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. ● możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001. Serwer musi posiadać deklarację CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów, Microsoft Windows 2019, Microsoft Windows 2022.

Warunki gwarancji	3 lata gwarancji producenta, realizowana w miejscu instalacji, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Firma serwisująca musi posiadać ISO 9001:2008 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
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

3. Switch zarządzalny (2 szt.) z serwisem na 2 lata

Przełącznik sieciowy

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

Zamawiający jest w posiadaniu rozwiązania Fortinet model FortiGate-60F. W ramach rozbudowy istniejącego systemu, której celem jest rozszerzenie mechanizmów bezpieczeństwa o warstwę dostępową, wymaganym jest dostarczenie przełącznika oraz innych elementów funkcjonalnych, współpracujących z istniejącym rozwiązaniem Fortigate, o następujących parametrach:

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. 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.

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

System musi być objęty minimum dwuletnim serwisem gwarancyjnym producenta, 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.

4. Access Point (1 szt.) z serwisem na 2 lata

Access Point

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 wyposażone w złącze typu Kensington.
3. Urządzenie musi być wyposażone w trzy niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy:
    a. 2.4 GHz 802.11b/g/n,
    b. 5 GHz 802.11a/n/ac/ax,
    c. Skaner 2.4GHz i 5GHz
4. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 16 SSID.
5. Urządzenie musi być wyposażone w moduł BLE.
6. Urządzenie musi być wyposażone w dwa interfejsy Ethernet 10/100/1000 Base-TX,
7. Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3at lub zewnętrzny zasilacz.
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-PSK, WPA-TKIP, WPA2-AES, WPA3, Web Captive Portal, MAC blacklist & whitelist, 802.11i, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, PEAP, EAP-FAST, EAP-SIM, EAP-AKA).
11. Interfejs radiowy urządzenia powinien wspierać następujące funkcje:
    a. MIMO – 2x2,

b. Maksymalna przepustowość dla poszczególnych modułów radiowych:

   i. 574 Mbps;

   ii. 1201 Mbps;

c. Wymagana moc nadawania:

   i. min. 23 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm;

   ii. min. 22 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;

d. Wsparcie dla 802.11n 20/40Mhz HT,

e. Wsparcie dla kanałów 80MHz,

f. Anteny – wbudowane dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz.

g. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy,

h. Maksymalna deklarowana liczba klientów per moduł radiowy:

   i. 512;

   ii. 512;

12. Funkcje dodatkowe:

a. OFDMA UL i DL

b. Spatial Reuse (BSS Coloring)

c. UL-MU-MIMO 802.11ax

d. DL-MU-MIMO

e. Enhanced Target Wake Time (TWT)

Gwarancja oraz wsparcie

Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji oraz być objęte minimum dwuletnim serwisem gwarancyjnym producenta 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.

5. Dyski do NAS

Zamawiający jest w posiadaniu rozwiązania NAS w postaci NAS QNAP NAS TS-832PXU-RP-4G. W ramach rozbudowy istniejącego systemu należy dostarczyć dyski o parametrach nie gorszych niż w tabeli poniżej:

Obudowa 3.5,

Pojemność 2TB,

Interfejs SATA/600,

Prędkość obrotowa 7200RPM,

Pamięć 128MB cache

Dysk musi znajdować się na liści kompatybilności posiadanego modelu NAS

6. Oprogramowanie do Backupu

Zarządzanie i magazyny

1. Produkt dostępny w polskiej wersji językowej.
2. Konsola zarządzająca dostępna z poziomu przeglądarki internetowej
3. System musi umożliwiać tworzenie kopii zapasowych na poziomie dysków
4. System musi umożliwiać tworzenie kopii zapasowych na poziomie plików i folderów
5. System musi umożliwiać replikację kopii zapasowych do wielu lokalizacji docelowych
6. System musi umożliwiać tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT
7. System musi umożliwiać współpracę z usługą kopiowania woluminów w tle (VSS) firmy Microsoft
8. Możliwość zdefiniowania limitu przepustowości sieciowej z jakiej ma korzystać oprogramowanie backupowe
9. System zarządzania nie może być oparty o relacyjne bazy danych.
10. Rozwiązanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju w procesie tworzenia kopii zapasowej).
11. Rozwiązanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera (urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera (urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów).
12. Aplikacje klienckie powinny wysyłać dane z kopii zapasowej bezpośrednio na wskazany magazyn – serwer backupu/usługa zarządzania, ani żaden inny element Systemu, nie powinien brać udziału w przesyłaniu danych.
13. Rozwiązanie musi być systemem multi-storage-owym i umożliwia tworzenie wielu repozytoriów danych jednocześnie również na innych środowiskach jako przestrzeń do replikacji danych.

14. System musi oferować mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.
15. Rozwiązanie w warstwie sprzętowej powinno bazować na standardowych komponentach architektury x86, bez powiązania i poleganiu na komponentach wyłącznie jednego dostawy (tzw. "no propietary vendor lock").
16. System pozwala administratorowi na ustawienie dowolnego harmonogramu replikacji danych pomiędzy dowolnymi wspieranymi magazynami.
17. System musi umożliwiać wykonywanie kopii obrazu dysku, kopii plików i katalogów oraz kopii maszyn wirtualnych bez ich zatrzymywania z zachowaniem stuprocentowej integralności i spójności danych wewnątrz wykonanej kopii zapasowej.
18. Rozwiązanie musi realizować funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie.
19. Rozwiązanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia.
20. System musi umożliwiać automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku wystąpienia błędu.
21. Rozwiązanie powinno umożliwiać klonowanie planów kopii zapasowych, planów replikacji oraz planów testowego odtwarzania maszyn wirtualnych
22. Rozwiązanie powinno umożliwiać uruchamianie przy zadaniach backupu dowolnych skryptów PRE/POST oraz po wykonaniu migawki VSS.
23. System powinien umożliwiać definiowanie tzw. okna backupowego dla każdego z zadań w celu umożliwienia zarządzania obciążeniem sieci i uwzględnienia okien serwisowych występujących u Zamawiającego.
24. System musi automatycznie dodawać do polityki i harmonogramu tworzenia backupów nowe źródła / maszyny wirtualnych, dodane do bieżącego środowiska (automatyzacja oparta na polityce tworzenia kopii).
25. Rozwiązanie musi udostępniać możliwość podglądu postępu działania dowolnego zadania, w tym zadania wykonywania kopii zapasowych, odtwarzania danych, testowego odtwarzania danych, usuwania danych oraz zadania odświeżania zajętości magazynu na dane.
26. Rozwiązanie musi posiadać system powiadamiania poprzez e-mail oraz Slack o zdarzeniach w następujących przypadkach: zadanie zostało zakończone pomyślnie, zadanie zostało zakończone z ostrzeżeniami, zadanie zostało zakończone z błędem, zadanie zostało anulowane, zadanie nie zostało uruchomione.
27. System powinien umożliwiać wysyłanie powiadomień o statusie wykonanych zadań na dowolne adresy webhook, podawane przez użytkownika,
28. Oferowane rozwiązanie musi być dobrane pod względem wydajności w oparciu o najlepsze praktyki producenta.
29. Rozwiązanie musi być wyskalowane, dobrane pod względem wymaganej funkcjonalności i wydajności stosownie do ilości zabezpieczanych danych i obiektów z uwzględnieniem przyrostu danych (serwery, maszyny wirtualne, bazy danych itp.) zgodnie z opisem w zapytaniu ofertowym.
30. Wydajność oferowanej konfiguracji musi być taka, aby wszystkie funkcje systemu były dostępne w chwili wdrożenia (np. deduplikacja, kompresja, instancja workerów i browserów, replikacja, testowe odtwarzanie maszyn wirtualnych).

31. System pozwala na zmniejszenie rozmiaru przechowywanych i przesyłanych danych poprzez usuwanie zduplikowanych bloków danych ze źródła kopii pomiędzy wszystkimi źródłami w obrębie wszystkich kopii na magazynie danych.
32. Proces deduplikacji musi być możliwy dla każdego z typów obsługiwanych magazynów.
33. Proces deduplikacji nie może wymagać instalacji żadnych dodatkowych komponentów, które będą pośredniczyły w zapisie danych z deduplikowanych
34. Proces deduplikacji nie może posiadać pojedynczego punktu awarii, tym samym musi być dostępny jednocześnie na każdym wspieranym magazynie na dane - również replikacyjnych. Awaria jednego z magazynów na dane nie może wpłynąć na integralność deduplikatów, jak i tablicy deduplikatów na innym magazynie.
35. Proces deduplikacji realizowany jest blokiem o stałej wielkości, którego wielkość może zostać ustalona na etapie wdrożenia rozwiązania zgodnie z najlepszymi praktykami producenta.
36. Proces szyfrowania kopii zapasowych nie może ograniczać procesu deduplikacji w ramach tego samego klucza szyfrującego.
37. Kompresja kopii zapasowych musi obsługiwać jeden z wymienionych algorytmów: LZ4, ZStandard. Dodatkowo, musi umożliwiać określenie szczegółowego poziomu kompresji, w tym: niski, średni, wysoki.
38. Instalacja, modyfikacja ustawień, polityki tworzenia kopii zapasowej systemu nie może wymagać przerwania pracy lub restartu systemu.
39. System musi pozwalać na automatyczne aktualizacje oprogramowania.
40. System musi być w stanie kompresować i szyfrować zabezpieczone dane w systemach NAS.
41. System musi pozwalać na uruchomienie kontenerów Docker w dowolnych urządzeniach NAS w celu ich zabezpieczenia.
42. System tworzenia kopii zapasowej musi przechowywać dane w sposób zapewniający ich niezmienność (tzw. "resilience"), dzięki czemu kopie zapasowe nie będą mogły zostać nadpisane lub zmodyfikowane przez cały okres ich przechowywania, retencji.
43. System zarówno będzie przechowywać dane w kopii zapasowej w postaci zaszyfrowanej jak też ruch wewnątrz systemu również musi być szyfrowany.
44. Archiwum długoterminowych kopii zapasowych musi być szyfrowane, a odzyskiwanie z archiwum obsługiwane z tego samego interfejsu użytkownika, co inne przywracanie dane.
45. System musi mieć mechanizmy chroniące przejęcie konta administratora oraz umożliwiać definiowanie dodatkowych uprawnień dla każdej z predefiniowanych ról użytkowników.
46. System musi pozwalać na gradację uprawnień administratorów - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.: system operator, backup operator, restore operator, viewer. Dla każdej z tych ról system musi umożliwiać przypisywanie dodatkowych uprawnień, w tym możliwość zablokowania usuwania danych.
47. Rozwiązanie musi posiadać możliwość nieodwracalnego usuwania danych z magazynu na dane w momencie spełnienia dodatkowych wymogów.
48. W sytuacji, gdyby podstawowe urządzenie tworzenia kopii zapasowej było niedostępne, system musi posiadać możliwość przywrócenia z archiwum za pomocą innej instancji systemu dostarczonej przez tego samego producenta. tzn. archiwum musi zawierać wszystkie informacje konieczne do odzyskania.

49. Rozwiązanie musi umożliwiać uruchomienie konsoli w chmurze producenta zlokalizowanej na terenie Polski, w celu umożliwienia dostępu do środowiska zarządzania kopiami zapasowymi w przypadku czasowej niedostępności środowiska lokalnego.
50. System kopii zapasowej musi umożliwiać dostęp do konsoli administracyjnej z wielu stacji roboczych.
51. System kopii zapasowej musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
52. System powinien posiadać predefiniowane schemat tworzenia kopii zapasowych: Custom, Basic, G-F-S, Forever incremental,
53. Rozwiązanie musi obsługiwać kontrolę dostępu opartą na rolach (RBAC).
54. Możliwość składowania utworzonych kopii zapasowych na magazynach chmurowych Amazon AWS, Azure, Wasabi, Google Cloud Storage, Backblaze B2, magazyny zgodne z S3.
55. Możliwość składowania utworzonych kopii zapasowych na udziałach sieciowych po protokole smb, nfs, iscsi, katalog lokalny
56. Zarządzanie i odzyskiwanie danych z kopii musi odbywać się z tego samego interfejsu użytkownika (konsoli), niezależnie od tego, gdzie znajduje się kopia zapasowa (w chmurze AWS, Azure, GCP, w Data Center czy w usłudze typu SaaS).
57. Czas przechowywania kopii zapasowej (retention time) systemu backupu nie może być zmieniony np. poprzez manipulowanie wskazaniami zegara serwera NTP w celu szybszego ich wyekspirowania - tzn. czasy przechowywania kopii zapasowych nie będą zależne od wskazań zegara czasu serwera NTP, ale będą wykorzystywać technologię, która mierzy upływ czasu.
58. Możliwość generowania raportów dobowych w oparciu o harmonogram
59. Produkt musi posiadać możliwość zapisu kopii zapasowych do magazynu chmurowego dostarczanego bezpośrednio przez producenta oprogramowania (datacenter musi być zlokalizowane na terenie Polski)
60. Produkt musi posiadać możliwość zdefiniowania maksymalnej liczby równocześnie backupowanych urządzeń w ramach jednego planu backupowego, niezależnie od typu urządzenia (np. stacja robocza, serwer, maszyna wirtualna)
61. Możliwość wyświetlenia szczegółowych informacji o chronionym urządzeniu takich jak: CPU, RAM, System operacyjny, Adres IP.
62. Produkt musi posiadać możliwość zdefiniowania poziomu obciążenia magazynu, po osiągnięciu którego zostanie wysłane powiadomienia e-mail. (poziom definiowany indywidualnie dla każdego magazynu)

Wspierane systemy

Możliwość instalacji oraz uruchomienia agenta backupowego na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy:

- Alpine 3.10+,
- Debian: 9+,
- Ubuntu: 16.04+,

- Fedora: 29+,
- centOS: 7+,
- RHEL: 6+,
- openSUSE: 15+,
- SUSE Enterprise Linux(SLES): 12 SP2+,
- macOS: 10.13+,
- Windows: 7, 8.1, 10(1607+),
- Windows Server: 2008 R2+,

- Środowisk wirtualnych:
- Hyper-V 2016+,
- VMware: 6.7+.

Możliwość instalacji oraz uruchomienia serwera zarządzania na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy:

- Debian: 9+
- Ubuntu: 16.04+
- Fedora: 29+
- centOS: 7+
- RHEL: 6+
- openSUSE: 15+

SUSE Enterprise Linux (SLES): 12 SP2+

Windows Client: 7, 8.1, 10 (1607+)

Windows Server: 2012 R2+,

Środowiska fizyczne i bazy danych

1. Rozwiązanie powinno umożliwiać tworzenie grup urządzeń w celu automatyzacji procesów podczas pracy z urządzeniami.

2. Produkt musi posiadać możliwość tworzenia zadań dla grupy urządzeń oraz dla wybranych urządzeń.
3. Rozwiązanie musi pozwalać na automatyczne wyłączenie stacji roboczej po wykonaniu kopii zapasowej.
4. Rozwiązanie backupowe musi pozwalać na zabezpieczanie zaszyfrowanych partycji min. BitLocker, Veracrypt, TrueCrypt, Eset Endpoint Encryption.
5. System jest niezależny od wersji Microsoft SQL i musi umożliwiać przywracanie danych SQL dla tej samej lub nowszej wersji.
6. System musi obsługiwać również narzędzia RMAN firmy Oracle do tworzenia kopii zapasowych i odzyskiwania. Dodatkowo system musi obsługiwać funkcję przyrostowego scalania danych.
7. System kopii zapasowej musi wspierać odtwarzanie pojedynczych plików z systemów Windows oraz Linux.
8. W przypadku niedostępności źródła danych, system musi oczekiwać na powrót dostępności źródła danych przez określony przez administratora okres. W przypadku braku powrotu dostępności źródła, system musi podjąć ustaloną przez administratora liczbę prób kontynuacji kopii. W przypadku powrotu źródła danych system musi kontynuować zadanie backupu od momentu, w którym wystąpiła niedostępność źródła - system nie może rozpoczynać zadania od punktu początkowego i rozpoczynać przesyłania kopii od zera. W przypadku braku powrotu źródła danych system powinien zakończyć zadanie błędem.
9. Odtwarzanie Bare Metal Restore w Systemie może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika.
10. Rozwiązanie powinno umożliwiać uruchamianie procesu Bare Metal Restore z dowolnego bootowalnego nośnika danych.
11. Rozwiązanie powinno wspierać odtwarzanie danych w scenariuszach P2P, P2V, V2P, V2V.
12. Rozwiązanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie (RAW, VHD, VHDX, VMDK).
13. Rozwiązanie musi umożliwiać odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL) oraz z prawami dostępu. Funkcjonalność ta musi być możliwa do skonfigurowania przez administratora na etapie konfiguracji procesu przywracania danych.
14. Rozwiązanie musi umożliwiać przywracanie plików pomiędzy różnymi systemami operacyjnymi i systemami plików (np. odtwarzanie danych plikowych Linux na systemie Windows).

Środowiska wirtualne

1. System musi wspierać kopię w trybie application-aware dla wszystkich wspieranych wirtualizatorów.
2. System musi umożliwiać wykonywanie kopii maszyn wirtualnych z zastosowanie zaawansowanych metod transportu (HotAdd, SAN, LAN), w tym metodami LAN-Free, tj. takimi, które podczas wykonywania backupu nie obciążają interfejsów sieciowych maszyn wirtualnych.
3. System kopii zapasowej musi wykorzystywać mechanizmy Change Block Tracking oraz Replica Change Tracking dla wspieranych przez producenta platformach wirtualizacyjnych.

4. Rozwiązanie producenta musi być certyfikowane przez dostawcę platformy wirtualizacyjnej, tj. producent musi uczestniczyć w programie Technology Alliance Partner.
5. System kopii zapasowej musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage-u użytego do przechowywania kopii zapasowych.
6. Dla środowiska vSphere i Hyper-V rozwiązanie powinno umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).
7. System kopii zapasowej musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere.
8. System kopii zapasowej musi umożliwiać weryfikację odtwarzalności wirtualnych maszyn według własnego harmonogramu w dowolnym środowisku.

Aplikacje SaaS

1. Ochrona z tej samej konsoli dla Microsoft 365 minimum na poziomie, skrzynek pocztowych, onedrive, kontaktów, kalendarza.
2. Rozwiązanie musi umożliwiać przywracanie danych Microsoft 365: do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku .pst oraz do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji)
3. System musi umożliwiać granularne odtwarzanie danych, tj. pojedynczych plików z kopii obrazu dysku oraz pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365.
4. System musi umożliwiać zabezpieczanie środowisk Git, w tym GitHub, GitLab oraz Bitbucket wraz z metadanymi
5. System musi umożliwiać odtworzenie dowolnego środowiska Git w dowolnym innym środowisku Git, tzw. odtwarzanie crossowe.
6. System musi umożliwiać zabezpieczenie metadanych zebranych wokół repozytorium w ramach zabezpieczanego środowiska Git.
7. System musi umożliwiać odtwarzanie metadanych repozytorium Git do dowolnego innego środowiska Git w przypadku chęci odtworzenia repozytorium.
8. System musi umożliwiać zabezpieczenie środowisk Jira
9. System musi umożliwiać odtworzenie środowiska Jira do chmury lub środowiska lokalnego.
10. System musi umożliwiać zabezpieczenie środowisk Jira

Licencjonowanie i wsparcie techniczne

1. Wszystkie linie supportu muszą być obsługiwane w języku polskim.
2. Wsparcie techniczne musi być świadczone bezpośrednio przez główną siedzibę producenta.
3. Możliwość zgłaszania ticketów supportowych bezpośrednio z poziomu interfejsu zarządzania w formie czatu.

4. Producent wraz z rozwiązaniem musi udostępnić materiały samopomocowe w j. polskim (minimum dostęp do bazy wiedzy, materiałów wideo oraz kart produktów)
5. Wsparcie techniczne musi umożliwiać korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego.
6. Licencje w ramach rozwiązania powinny pozwalać na zabezpieczenie określonej przez Zamawiającego ilości hostów w obrębie wspieranych przez System środowisk.
7. Licencje powinny być dostępne w opcji wieczystej.
8. Dostęp do wsparcia technicznego producenta powinno obowiązywać przez okres dwóch lat.
9. Sposób licencjonowania opiera się na:

    - ilości serwerów/endpointów - dla fizycznych urządzeń,
    - ilości socketów w hostach - dla środowisk wirtualnych,
    - ilość repozytoriów - dla GIT.
    - Licencje powinny umożliwiać zabezpieczenie w wersji **wieczystej**
    - 11 stacji roboczych,
    - 2 serwerów fizycznych bez wirtualizacji,
    - Nielimitowanej ilości maszyn wirtualnych w obrębie 2 fizycznych serwerów stanowiących podstawy do wirtualizacji (łącznie 4 sockety)

Anty-ransomware i bezpieczeństwo

1. System plików rozwiązania musi być odporny na ataki Ransomware (zapewnić ochronę przed szyfrowaniem end-to-end, kopie zapasowe nie mogą być nadpisywane - "niezmienny system plików").
2. System powinien umożliwiać wykorzystanie wbudowanego menadżera haseł do przechowywania wszelkich sekretów (haseł, danych dostępowych, kluczy szyfrujących) wykorzystywanych przez System
3. System powinien umożliwiać przywrócenie hasła głównego administratora w przypadku jego utraty.
4. W ramach systemu, komunikacja pomiędzy hostem źródłowym, a magazynem powinna odbywać się tylko i wyłącznie bezpośrednio pomiędzy agentem backupu, a magazynem. Komunikacja nie może przechodzić przez serwer backupu, ani żaden inny komponent, którego awaria sparaliżowałaby działanie Systemu. System nie może posiadać pojedynczego punktu awarii.
5. System musi działać w zgodzie z regułą Zero-knowledge Encryption. Oznacza to, że wszelkie sekrety muszą być przechowywane w centralnym Managerze Haseł w postaci zaszyfrowanej algorytmem AES i być udostępniane agentowi dopiero w momencie rozpoczęcia wykonywania kopii zapasowej. Sekrety nie mogą być przechowywane w konfiguracji agenta na zabezpieczanym urządzeniu.

7. Oprogramowanie BitDefender - Licencja na okres 24.09.2025 – czerwiec 2026

Bitdefender GravityZone Business Security Enterprise

System Operacyjny Windows:

Systemy Operacyjne Komputerów

Pełne wsparcie:

- Windows 11 October 2023 Update (23h2)
- Windows 11
- Windows 10
- Windows 8.1
- Windows 8
- Windows 7 SP1

Systemy operacyjne serwera

Pełne wsparcie

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 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 9x - 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 36 – 38 – 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 6 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

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 – 5.15.0 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

openSUSE Leap 15.2 - 15.4 - 5.3.18 / 5.14.x 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

Ubuntu 20.04.x – 5.15

Ubuntu 22.04.x – 5.15 / 5.19

Oparte o SUSE

SLES 15 SP4 – 5.14.21-x

openSUSE Leap 15.4 – 5.14.21-x

Oparte o chmurę

Amazon Linux v2 – 5.10

Amazon Linux 2023 - 6.1

Systemy Operacyjne Mac OS X

macOS Sonoma (14.x)

macOS Ventura (13.x)

macOS Monterey (12.x)

macOS Big Sur (11.x)

macOS Catalina (10.15)

macOS Mojave (10.14)

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) VMDK

Środowiska wspierane:

- VMware vSphere and vCenter Server versions:
  - 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: 7.1 (with the XS71ECU2060 hotfix), 8.2.
- 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

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami
2. Pomoc techniczna, interfejs oraz dokumentacja dostarczona i świadczona w języku polskim.
3. Wykrywanie zagrożeń i analiza procesów technikami heurystycznymi
4. Powiadomienia z modułu sprawdzającego procesy są wzbogacone o ścieżkę i identyfikator procesu nadrzędnego, a także o wiersz poleceń, który uruchomił proces. Jeśli ma to miejsce te dane są również przesyłane za pośrednictwem Syslog.
5. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
6. Wbudowana technologia do ochrony przed rootkitami.
7. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.

8. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".
9. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
10. Możliwość skanowania dysków sieciowych i dysków przenośnych.
11. Skanowanie plików spakowanych i skompresowanych.
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 i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express.
14. Skanowanie i oczyszczanie poczty przychodzącej POP3 "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
15. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
16. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
17. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Dodatkowo zdefiniowane są grupy stron przez producenta.

18. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.

19. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać.

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

21. Program skanuje ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.

22. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program będzie pytał o hasło.

23. Po kliknięciu prawym klawiszem myszy na ikonie programu i wybraniu opcji: O programie" możliwość zdefiniowania przez administratora danych do pomocy technicznej jak: adres strony pomocy, adres e-mail do administratora ochrony, numer telefonu do administratora ochrony.

24. W GUI programu na punkcie końcowym możliwość wyświetlenia aktualnej wersji produktu i aktualnej wersji silników.

25. W GUI programu możliwość wyświetlenia, kiedy była przeprowadzana ostatnia aktualizacja z dokładnością co do dnia i sekundy jej uruchomienia.

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

27. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.

28. Praca programu musi być niezauważalna dla użytkownika.

29. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na stacji roboczej.

30. Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet.

31. Oprogramowanie klienckie posiada wbudowana funkcje do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej.

32. Możliwość odblokowania ustawień programu po wpisaniu hasła.

33. Oprogramowanie posiada możliwość odblokowania ustawień lokalnych konfiguracji po doinstalowaniu odpowiedniego modułu.

34. Wbudowany moduł kontroli urządzeń (możliwość blokowania całkowitego dostępu do urządzeń, podłączenia tylko do odczytu i w zależności do jakiego interfejsu w komputerze zostanie podłączone urządzenie).

35. Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej, na podstawie wykrytych urządzeń lub wpisanych ręcznie ID urządzenia lub ID produktu.

36. Funkcja Ochrony danych umożliwia blokowanie wysyłanych przez http lub smtp jak: (adresy e-mail, Piny, Konta bankowe, hasła itp.

37. Funkcja Ochrony danych konfigurowana zdalnie przez administratora.

38. Jedna wersja instalacyjna na stacje robocze i serwery plików Windows.

39. Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego.

40. Wbudowany IDS

41. Możliwość zainstalowania silnika pełnego, lekkiego ze sprawdzaniem reputacji plików w chmurze lub wykorzystanie dodatkowej maszyny wirtualnej która przejmie rolę silnika skanującego.

42. Maszyna, która przejmuję rolę silnika skanującego musi działać w trybach redundancji lub równej dystrybucji.

43. Aktualizacja maszyny skanującej musi obejmować oddzielną aktualizację nowych funkcji, ulepszeń, poprawek oraz oddzielną aktualizację systemu operacyjnego urządzenia wirtualnego.

44. Możliwość tworzenia list sieci zaufanych.

45. Możliwość dezaktywacji funkcji zapory sieciowej.

46. Możliwość ustawienie skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu.

47. Dodatkowa funkcja ochrony przeciwko znanym zagrożeniom typu ransomware.

48. Mechanizm, który wspiera powrót do ostatnich działających wersji produktu oraz sygnatur w przypadku wdrożenia wadliwej aktualizacji.

49. Użytkownik na punkcie końcowym ma możliwość opóźnienia restartu potrzebnego do zakończenia jednego lub wielu zadań (konfigurowalne w politykach bezpieczeństwa)

50. Automatyczne zezwolenie na dostęp dla użytkowników Active Directory z grupy security groups

51. Wymuszenie połączenia szyfrowanego dla punktów końcowych Windows oraz Linux do serwera zarządzającego.

52. 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 wykrywać błędne konfiguracje oraz naprawiać je lub ignorować z podziałem na typ błędnej konfiguracji:

-Ochrony przeglądarki internetowej

-Sieć i poświadczenia

-Błędna konfiguracja systemu operacyjnego

System ponadto musi określać nasilenie tych błędnych konfiguracji w oparciu o punkty procentowe.

    b) System zarządzania ryzykiem który powinien wykrywać luki w aplikacjach podając przy tym numer CVE tych luk.

    c) System, który pozwala na śledzenie i wykrywanie niezwyczajnych działań jakie podejmuje użytkownik na punkcie końcowym wraz z poinformowaniem ilu użytkowników takie działanie dotyczy oraz jakie jest jego nasilenie.

    d) System pozwala na skanowanie punktów końcowych pod kątem wykrywania ryzyka na podstawie harmonogramu lub pojedynczo utworzonego zadania.

    e) System pozwala na raportowanie na ilu urządzeniach wykryto błędną konfigurację i luki w aplikacjach oraz jaka jest ilość takich podatności i ich nasilenie wyrażone w procentach.

    f) System pozwala na raportowanie u ilu użytkowników wykryto podejrzane działania oraz jakie jest ich nasilenie

53. 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)

Uwaga: Ta warstwa zabezpieczeń dotyczy systemów opartych na systemie Windows.

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

-Wczesny dostęp

-Dostęp do poświadczeń

-Wykrycie

-Crimeware

55. 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 a w przypadku ataku odzyskanie i przywrócenie ich do pierwotnej lokalizacji.

Formaty plików jakie mogą być odzyskane:

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

Oprogramowanie daje możliwość odzyskania plików na żądanie lub automatycznego odzyskiwania.

56. Ochrona proaktywna oparta o maszynowe uczenie która działa w fazie poprzedzającej wykonanie, ochrona ta musi wy wykrywać zagrożenia takie jak:

    a) Ukierunkowane ataki

    b) Podejrzane pliki i ruch w sieci

    c) Exploity

    d) Ransomware

    e) Grayware

57. Moduł ochrony proaktywnej musi posiadać oddzielne działania jakie będzie podejmował dla plików i oddzielne dla ruchu sieciowego

58. Moduł ochrony proaktywnej musi działać w trybach, które administrator może dowolnie zmieniać na:

    a) Tolerancyjny

    b) Normalny

    c) Agresywny

59. 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 przesłania archiwum zabezpieczonego hasłem

    c) Możliwość przesłania adresu URL

    d) W przypadku przesłania wielu plików jednorazowo, możliwość detonacji próbek pojedynczo.

60. Wbudowany sandbox musi działać w trybie monitorowania i blokowania

61. Wbudowany sandbox musi oferować działania naprawcze takie jak dezynfekcja lub przeniesienie do kwarantanny

62. Wbudowany sandbox musi oferować opcję wstępnego filtrowania zawartości, która skanuje pliki, argumenty wiersza poleceń i adresy URL pod kątem podejrzanego zachowania.

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

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

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

66. Telemetria - Możliwość przesyłania nieprzetworzonych danych bezpieczeństwa z punktów końcowych z systemem operacyjnym Windows do SIEM Splunk (wymaga TLS 1.2 lub wyższy).

67. Oprogramowanie pozwala na skanowanie punktów końcowych pod kątem wyszukiwania wskaźników zagrożeń, wskaźniki te obejmują:

Maszyny Wirtualne

1. Możliwość w kliencie instalowanym na stacji roboczej wirtualnej ustawienie informacji do pomocy technicznej, takiej jak: (strona pomocy, adres e-mail, numer telefonu).

2. Możliwość określenia jak długo maja być przechowywane zdarzenia na stacji roboczej.

3. Możliwość zabezpieczenia hasłem klienta przed odinstalowaniem.

4. Wersja kliencka nie pełni roli ochrony antywirusowej, jest tylko agentem dla Security Servera.

5. Dla maszyn z systemem Linux możliwość wskazania katalogów które mogą być chronione w czasie rzeczywistym.

6. Możliwość określenia co jaki czas mają być wysyłane pliki z kwarantanny do producenta.

7. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.

8. Możliwość wskazania do jakiego serwera ochrony mają się łączyć klienci maszyn wirtualnych.

Stacje robocze i serwery Windows

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. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
4. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".
5. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
6. Skanowanie plików spakowanych i skompresowanych.
7. Oprogramowanie zawiera monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego.
8. Oprogramowanie posiada możliwość zablokowania hasłem odinstalowania programu.
9. Produkt oraz sygnatury muszą być aktualizowane nie rzadziej niż raz na godzinę.
10. Oprogramowanie musi posiadać możliwość raportowania zdarzeń informacyjnych.
11. Program musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju.
12. Program musi posiadać możliwość skanowania jedynie nowych niezmienionych plików.
13. Program musi mieć wbudowany skaner wyszukiwania rootkitów
14. Możliwość odblokowania ustawień programu po wpisaniu hasła
15. Możliwość uruchomienia zadania skanowania z niskim priorytetem
16. Możliwość wykorzystania dodatkowej maszyny wirtualnej która przejmie role silnika skanującego.

17. Możliwość określenia jak długo maja być przechowywane zdarzenia na stacji roboczej.

18. Możliwość zabezpieczenia hasłem klienta przed odinstalowaniem

19. Dla maszyn z systemem Linux możliwość wskazania katalogów które mogą być chronione w czasie rzeczywistym.

20. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.

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 przeciągu ostatnich kilku godzin / dni.

3. Zdolność konfigurowania różnych akcji wykonywanych na plikach zainfekowanych, podejrzanych oraz nie możliwych do przeskanowania.

4. Możliwość wykluczenia potencjalnie niechcianych aplikacji (PUA) z filtrowania antymalware.

5. Możliwość skanowania w poszukiwania 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 przekierowania 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. Centralna instalacja i zarządzanie programami służącymi do ochrony stacji roboczych i serwerów plikowych Windows.
2. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, oraz zaporą osobistą (tworzenie reguł obowiązujących dla wszystkich stacji) zainstalowanymi na stacjach roboczych w sieci korporacyjnej z jednego serwera zarządzającego.
3. Możliwość integracji wielu domen Active Directory
4. Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych.
5. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie, Zainstalowanych modułów, ostatniej aktualizacji oraz przypisanej polityki).
6. Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci, analityk bezpieczeństwa lub z ustawieniami niestandardowymi
7. Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, wersji systemu operacyjnego.
8. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu.
9. Możliwość wysłania linku instalacyjnego bezpośrednio z poziomu konsoli administracyjnej.

10. Możliwość zmiany konfiguracji na stacjach i serwerach z poziomu centralnej konsoli zarządzającej lub z poziomu punktu końcowego po włączeniu odpowiedniej opcji w politykach bezpieczeństwa.

11. Możliwość uruchomienia centralnej konsoli jedynie z poziomu przeglądarki internetowej.

12. Możliwość ręcznego (na żądanie) i automatycznego generowanie raportów (według ustalonego harmonogramu) i wyeksportowanie go do formatu: pdf i csv.

13. Raport generowany według harmonogramu z możliwością automatycznego wysłania go do osób zdefiniowanych w tym raporcie również zbiorczo w formie archiwum zip.

14. Możliwość generowania raportu co godzinę.

15. Po instalacji oprogramowania antywirusowego nie jest wymagane ponowne uruchomienie komputera do prawidłowego działania programu.

16. Aktywacja modułu kontroli urządzeń nie wymaga restartu stacji docelowej.

17. Możliwość dodania etykiety do stacji roboczej.

18. Możliwość dezinstalacji oprogramowania antywirusowego innych firm w trakcie instalacji zdalnej.

19. Możliwość przechowywania kwarantanny maksymalnie 180 dni

20. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać.

21. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.

22. W całym okresie trwania subskrypcji użytkownik ma prawo do korzystania z bezpłatnej pomocy technicznej świadczonej za pośrednictwem telefonu i poczty elektronicznej.

23. Wykorzystanie nierelacyjnej bazy danych MongoDB w serwerze administracyjnym.[2]

24. Możliwość aktualizacji serwera administracyjnego bez potrzeby przeinstalowywania.

25. 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.

26. Możliwość automatycznego przypisywania polityk na podstawie reguły lokalizacji, możliwość określenia 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

27. Integracja z serwerem Syslog.

28. Uwierzytelnienie dwuskładnikowe realizowane przy pomocy aplikacji kompatybilnej ze standardem RFC6238

29. Możliwosc ustawienia wymagania zmiany hasła logowania do konsoli co 90 dni.

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

31. Funkcja pojedynczego logowania – Single Sign-on (SSO).

32. Możliwość naprawy instalacji z poziomu konsoli.

33. Raport streszczający - Możliwość podglądu raportu, który streszcza stan środowiska w firmie z rozróżnieniem na takie sekcje jak:

-Zarządzane punkty końcowe

-Aktualny zapas wolnych miejsc w licencji z rozróżnieniem na stacje robocze windows, serwery windows, macOS, linux oraz fizyczne punkty końcowe i maszyny wirtualne

-Pięć najczęściej blokowanych zagrożeń

-Podział zagrożeń na urządzenia takie jak stacje robocze i serwery

-Status incydentów bezpieczeństwa, które wystąpiły

-Stan modułów punktów końcowych

-Ocena ryzyka firmy

-Zablokowane strony WWW w oparciu o wykryte tam szkodliwe oprogramowanie, phishing, oszustwa.

-Zablokowane techniki ataku sieciowego z podziałem na techniki ataku takie jak wczesny dostęp, dostęp do poświadczeń, wykrycie, ruch poprzeczny, crimeware

34. Możliwość integracji z innymi systemami poprzez API takich elementów bądź sekcji jak:
    a) Pakiety
    b) Sieć
    c) Kwarantanna
    d) Licencjonowanie
    e) Integracje
    f) Polityki
    g) Raporty
    h) Konta
    i) Firmy
35. 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 pozwala na określenie godziny, kiedy te maszyny będą usuwane
36. Możliwość określenia własnego serwera NTP.
37. Integracja z vCenter Server.
38. Integracja z Xen Server.
39. Integracja z nutanix Prism Element.
40. Możliwość integracji z Amazon EC2.
41. Intergracja z Azure.

42. Możliwość zarządzania ochroną na serwerach Exchange, tworzenie polityk i konfiguracji zdalnej ochrony.

43. Możliwość przypisywania polityk w zależności od zalogowanego użytkownika domenowego.

44. Możliwość wygenerowania i pobrania logów ze stacji roboczej z poziomu konsoli zarządzającej.

45. Pion firmy - Możliwość określenia profilu przedsiębiorstwa w konsoli webowej, dostępne muszą być opcje takie jak:

    a) Lotnictwo

    b) Rolnictwo

    c) Automotive

    d) Usługi komercyjne

    e) Doradztwo

    f) Energia

    g) Usługi finansowe

    h) Rząd

    i) Opieka zdrowotna

    j) Technologie

    k) Transport

    l) Non-profit

    m) Górnictwo

    n) Media

46. Funkcja kontroli aplikacji, która daje możliwość skanowania punktów końcowych pod kątem wykrywania zainstalowanych na nim aplikacji lub dostępnych procesów.

47. Funkcja kontroli aplikacji może działać w trybie testowym lub produkcyjnym.

48. Funkcja kontroli aplikacji pozwala na zablokowanie wybranych plików lub procesów w oparciu o ścieżkę, hash lub certyfikat.

49. Możliwość wyświetlania adresu MAC dołączonego do nazwy hosta.

50. Możliwość wyświetlenia czy punkt końcowy jest serwerem czy stacją roboczą.

51. Możliwość wyświetlenia informacji czy zainstalowany na punkcie końcowym system operacyjny to Windows, Linux, MacOS.

52. Możliwość wyświetlenia wersji systemu operacyjnego zainstalowanego na punkcie końcowym.

53. Możliwość filtrowania punktów końcowych, które były online w ciągu ostatnich 24 godzin, 7 lub 30 dni.

54. Menu tworzenia paczek instalacyjnych musi określać czy dany moduł jest dostępny dla stacji roboczych Windows, Serwerów Windows, Linux, MacOS.

55. Oprogramowanie umożliwia pobranie oddzielnego pakietu instalacyjnego dla systemów MacOS z Intel x86 oraz oddzielnego dla Apple M1.

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

57. Oprogramowanie umożliwia ochronę kontenerów instalowaną bezpośrednio na hoście kontenera oferuje wgląd w złośliwą aktywność serwera Linux i kontenerów w czasie rzeczywistym.

58. Program testowy – Oprogramowanie musi umożliwiać dobrowolne przystąpienie do darmowych testowych programów wczesnego dostępu. Program wczesnego dostępu powinien umożliwiać testowanie najnowszych funkcji oprogramowania których nie ma jeszcze w wersji końcowej produktu. Uzyskanie dostępu do programu testowego musi być natychmiastowe.

59. Znaczniki punktów końcowych – oprogramowanie musi umożliwiać przypisywanie znaczników (tagów) do punktów końcowych. Oprogramowanie musi umożliwiać przypisywanie znaczników ręcznie lub automatycznie. Oprogramowanie musi umożliwiać filtrowanie punktów końcowych na podstawie wybranych znaczników, musi istnieć możliwość filtrowania punktów końcowych na podstawie kilku wybranych znaczników w jednym czasie.

60. Oprogramowanie musi skanować nośniki USB zanim użytkownik zaloguje się do systemu Windows.

EDR-Endpoint Detection and Response

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

Wspierane systemy operacyjne

A. Systemy desktopowe

- 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

B. Systemy operacyjne dla serwerów:

- 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

C. MacOS:

macOS Sonoma (14.x)

macOS Ventura (13.x)

macOS Monterey (12.x)

macOS Big Sur (11.x)

macOS Catalina (10.15)

macOS Mojave (10.14)

D. Linux

Oparte o RPM

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

RHEL 8.x - 4.18.0 64-bit

RHEL 9x - 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 36 – 38 – 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 6 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

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 – 5.15.0 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

openSUSE Leap 15.2 - 15.4 - 5.3.18 / 5.14.x 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. Czujnik EDR, który gromadzi i przetwarza dane w celu raportowania danych dotyczących punktu końcowego i zachowania aplikacji.
2. Security Analytics, komponent służący do interpretacji metadanych gromadzonych przez czujnik EDR.
3. Możliwość instalacji dodatkowego, lekkiego agenta z czujnikiem EDR dla urządzeń z systemem Windows, aby rozszerzyć już zainstalowaną ochronę. Agent posiada też ochronę urządzenia i ruchu sieciowego oraz filtr stron internetowych.

Wykrywanie podejrzanej aktywności

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

1. Bazowanie na systemach bazujących na wskaźnikach ataku MITRE i własnej inteligencji.
2. Zgłaszanie wszystkich 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 przedziale czasu.

2. Produkt integruje się z bazą wiedzy ATT & CK firmy MITRE i odpowiednio oznacza zdarzenia bezpieczeństwa.

3. Produkt zapewnia zaawansowaną wizualizację zdarzeń bezpieczeństwa z określonymi informacjami lub działaniami z następującymi informacjami:

a) Karta Podsumowanie 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) Działania naprawcze gromadzą informacje o działaniach blokujących automatycznie podejmowanych przez produkt w związku z bieżącym zdarzeniem bezpieczeństwa.

Incydenty

Oprogramowanie pozwala na informowanie o zagrożeniach wykrytych i zablokowanych w formie grafu i linii zdarzeń oraz daje możliwość:

a) Filtrowania zdarzeń

b) Blokowania procesów

c) Dodawanie procesów do czarnej listy

d) Dodawanie procesów do białej listy

e) Izolacja hosta

f) Aktualizacja oprogramowania firm trzecich na hoście (wymagany add-on)

g) Przesłanie pliku do Sandbox

h) Sprawdzenie informacji o pliku w Google

i) Sprawdzenie informacji o pliku w VirusTotal

Filtrowanie zdarzeń odbywa się na podstawie (Tylko konsola on-premise):

a) Ocena zagrożenia od 10 do 100 punktów

b) Data wykrycia

c) Status

d) ID

e) Nazwa punktu końcowego

f) Typ ataku

a) Ransomware

b) Potencjalnie niechciana aplikacja

c) Malware

d) Exploit

e) Fileless

f) Password stealer

g) Downloader

h) Inne

i) Zdefiniowane przez użytkownika

Możliwość szybkiego podglądu otwartych incydentów, najczęstszych powiadomień, urządzeń, które mają najczęściej problem.

Możliwość wyświetlenia 10,20,30,50,100 zdarzeń na jednej stronie.

Możliwość wyświetlenia zablokowanych hashy plików.

Możliwość dodania własnych hashy MD5 oraz SHA256

Możliwość importu hashy z pliku CSV

Możliwość filtrowania dodanych hashy na podstawie:

a) Typu hashu

b) Wartości hash

c) Źródło dodania

d) Informacje o źródle

e) Nazwa pliku

f) Firma, której dotyczy wpis

g) Możliwość wyświetlenia 10,20,30,50,100 wpisów na jednej stronie.

Funkcja dostępna tylko w wersji cloud

Konsola Cloud – serwer administracyjny po stronie producenta

1. Telemetria - Możliwość przesyłania nieprzetworzonych danych bezpieczeństwa z punktów końcowych z systemem operacyjnym Windows do SIEM Splunk (wymaga TLS 1.2 lub wyższy).

2. 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 wykrywać błędne konfiguracje oraz naprawiać je lub ignorować z podziałem na typ błędnej konfiguracji:

-Ochrony przeglądarki internetowej

-Sieć i poświadczenia

-Błędna konfiguracja systemu operacyjnego

System ponadto musi określać nasilenie tych błędnych konfiguracji w oparciu o punkty procentowe.

b) System zarządzania ryzykiem który powinien wykrywać luki w aplikacjach podając przy tym numer CVE tych luk.

c) System, który pozwala na śledzenie i wykrywanie niezwyczajnych działań jakie podejmuje użytkownik na punkcie końcowym wraz z poinformowaniem ilu użytkowników takie działanie dotyczy oraz jakie jest jego nasilenie.

d) System pozwala na skanowanie punktów końcowych pod kątem wykrywania ryzyka na podstawie harmonogramu lub pojedynczo utworzonego zadania.

e) System pozwala na raportowanie na ilu urządzeniach wykryto błędną konfigurację i luki w aplikacjach oraz jaka jest ilość takich podatności i ich nasilenie wyrażone w procentach.

f) System pozwala na raportowanie u ilu użytkowników wykryto podejrzane działania oraz jakie jest ich nasilenie.

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

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

b) Funkcja pojedynczego logowania – Single Sign-on (SSO).

c) Możliwość naprawy instalacji z poziomu konsoli.

d) Raport streszczający - Możliwość podglądu raportu, który streszcza stan środowiska w firmie z rozróżnieniem na takie sekcje jak:

-Zarządzane punkty końcowe

-Aktualny zapas wolnych miejsc w licencji z rozróżnieniem na stacje robocze windows, serwery windows, macOS, linux oraz fizyczne punkty końcowe i maszyny wirtualne

-Pięć najczęściej blokowanych zagrożeń

-Podział zagrożeń na urządzenia takie jak stacje robocze i serwery

-Status incydentów bezpieczeństwa, które wystąpiły

-Stan modułów punktów końcowych

-Ocena ryzyka firmy

-Zablokowane strony WWW w oparciu o wykryte tam szkodliwe oprogramowanie, phishing, oszustwa.

-Zablokowane techniki ataku sieciowego z podziałem na techniki ataku takie jak wczesny dostęp, dostęp do poświadczeń, wykrycie, ruch poprzeczny, crimeware.

4. Pion firmy - Możliwość określenia profilu przedsiębiorstwa w konsoli webowej, dostępne muszą być opcje takie jak:

a) Lotnictwo

b) Rolnictwo

c) Automotive

d) Usługi komercyjne

e) Doradztwo

f) Energia

g) Usługi finansowe

h) Rząd

i) Opieka zdrowotna

j) Technologie

k) Transport

l) Non-profit

m) Górnictwo

n) Media

5. Filtrowanie zdarzeń na podstawie:

a) ID

b) Data utworzenia

c) Ostatnia aktualizacja

d) Status

e) Przydzielający

f) Priorytet

g) Ocena zagrożenia od 10 do 100 punktów

h) Podmioty

i) Zasoby

j) Skorelowane zdarzenia

k) Typ zdarzenia

l) Ostatnia faza killchain

m) Wykonane czynności

6. Wyszukiwanie zdarzeń odbywa się na podstawie:

a) ID

b) Ostatnia aktualizacja

c) Status

d) Osoba przydzielająca

e) Nazwa zdarzenia

f) Typ zdarzenia

g) Wszystkie

h) W organizacji

i) W punkcie końcowym

j) Data utworzenia

k) Priorytet

l) Ostatnia faza killchain

m) Wykonane czynności

7. Możliwość integracji sekcji Firmy z innymi systemami poprzez API.

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

9. Program testowy – 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.

10. 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) Elementy startowe Windows

e) Arp cache

f) Ip forwarding

g) Pobieranie listy wszystkie otwarte pliki dla każdego procesu w systemie docelowym.

h) Lista zamontowanych nośników

i) Filtry ip tables

j) Połączenia TLS które używają certyfikatów self-signed

k) Używane rozszerzenia w przeglądarce Chrome

l) Używane rozszerzenia w przeglądarce Firefox

m) Używane rozszerzenia w przeglądarce Safari

n) Źródła apt w systemach Linux

o) Wyświetlanie zainstalowanych pakietów DEB

p) Wyświetlanie zainstalowanych pakietów RPM

q) Pakiety Python zainstalowane w systemie

r) Lista zainstalowanych użytkowników, którzy łączyli się z publicznych adresów IP

s) Lista użytkowników, którzy zostali utworzeni w ciągu ostatnich 30 dni (Linux)

t) Wykrywanie czy aplikacje zdalnego dostępu są zainstalowane w systemie MacOS

u) Wykrywanie czy Kontrola Kont Użytkowników (UAC) jest wyłączona

v) Wykrywanie czy SecureBoot jest włączony

w) Lista zapamiętanych połączeń bezprzewodowych

x) Wykrywa, czy zmienił się domyślny folder startowy użytkownika

y) Wykrywa, czy zmienił się domyślny folder startowy maszyny

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

a) Możliwość pobierania przez partnera plików z kwarantanny podległych firm

Usługa dostępna tylko w wersji on-premise

Konsola On-premise – lokalny serwer administracyjny

1. Integracja z serwerem Syslog.

2. Powiadomienia z modułu sprawdzającego procesy są wzbogacone o ścieżkę i identyfikator procesu nadrzędnego, a także o wiersz poleceń, który uruchomił proces. Jeśli ma to miejsce te dane są również przesyłane za pośrednictwem Syslog.

3. Wykorzystanie nierelacyjnej bazy danych MongoDB w serwerze administracyjnym.

4. Możliwość określenia własnego serwera NTP.

5. Integracja z vCenter Server.

6. Integracja z Xen Server.

7. Integracja z nutanix Prism Element.

8. Intergracja z Azure.

9. Funkcja kontroli aplikacji, która daje możliwość skanowania punktów końcowych pod kątem wykrywania zainstalowanych na nim aplikacji lub dostępnych procesów. Funkcja kontroli aplikacji może działać w trybie testowym lub produkcyjnym. Funkcja kontroli aplikacji pozwala na zablokowanie wybranych plików lub procesów w oparciu o ścieżkę, hash lub certyfikat.

10. Filtrowanie zdarzeń odbywa się na podstawie:

a) Ocena zagrożenia od 10 do 100 punktów

b) Data wykrycia

c) Status

d) ID

e) Nazwa punktu końcowego

f) Typ ataku

a) Ransomware

b) Potencjalnie niechciana aplikacja

c) Malware

d) Exploit

e) Fileless

f) Password stealer

g) Downloader

h) Inne

i) Zdefiniowane przez użytkownika

Wyszukiwanie zdarzeń może odbywać się na podstawie:

a) Nazwa alertu

b) IP punktu końcowego

c) Hash MD5

d) Hash SHA256

e) Nazwa użytkownika

8. Licencje FortiGate-60F

Zamawiający jest w posiadaniu rozwiązania FortiGate-60F. W ramach postępowania należy dostarczyć licencję do ww. rozwiązania pozwalającą na korzystanie z funkcji bezpieczeństwa urządzenia na poziomie minimum Unified Threat Protection (UTP) od 22 luty 2025 do dnia 30.06.2026 r.

9. AHR do FortiGate-60F

Zamawiający jest w posiadaniu rozwiązania FortiGate-60F. W ramach postępowania należy dostarczyć licencję do ww. rozwiązania pozwalającą na korzystanie rozszerzonego wsparcia gwarancyjnego polegającego na dostarczeniu sprzętu zastępczego na następny dzień od momentu zgłoszenia na okres 22 luty 2025 do dnia 30.06.2026 r.

10. FortiSwitch-148F – serwis do 30.06.2026 r.

Zamawiający jest w posiadaniu rozwiązania – 2 urządzenia FortiSwitch-148F. W ramach postępowania należy dostarczyć licencję do ww. rozwiązania pozwalającą na korzystanie z serwisu producenta na poziomie minimum FortiCare Premium Support do dnia 30.06.2026 r.

11. OneDrive

OneDrive for Business (Plan 2) - Dysk OneDrive: do 5 TB Rozmiar pojedynczego pliku: 100 GB na okres do 30.06.2026r.