OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa pn.: „Wzmocnienie systemu cyberbezpieczeństwa w Gminie Krościenko Wyżne" w ramach zadania „Cyberbezpieczny Samorząd" obejmuje następujące części:

Część 1.
Wdrożenie lub aktualizacja polityk bezpieczeństwa informacji (SZBI)

Część 2.
Podniesienie poziomu wiedzy i kompetencji personelu JST kluczowego z punktu widzenia SZBI wdrożonego w urzędzie

Część 3.
Dostawa i wdrożenie infrastruktury IT oraz oprogramowania w ramach projektu grantowego
pn. "Cyberbezpieczny Samorząd"
Priorytet II: Zaawansowane usługi cyfrowe
Działanie 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa
Fundusze Europejskie na Rozwój Cyfrowy 2021-2027

Opis przedmiotu zamówienia wg Wspólnego Słownika Zamówień (CPV):

48620000-0	Systemy operacyjne
48000000-8	Pakiety oprogramowania i systemy informatyczne
48710000-8	Pakiety oprogramowania do kopii zapasowych i odzyskiwania
48820000-2	Serwery
48821000-9	Serwery sieciowe
48823000-3	Serwery plików
72265000-0	Usługi konfiguracji oprogramowania
32428000-9	Modernizacja sieci
32420000-3	Urządzenia sieciowe
80500000-9	Usługi szkoleniowe

Zawartość:

I. OGÓLNY OPIS PRZEDMIOTU ZAMÓWIENIA I WYMAGAŃ ZAMAWIAJĄCEGO

1. Wprowadzenie

Celem realizowanego projektu jest zwiększenie poziomu bezpieczeństwa informacji jednostek samorządu terytorialnego (JST) poprzez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych. Realizacja projektu poprzez wsparcie grantowe jednostek samorządowych, będzie obejmowała:

CZĘŚĆ 1.

Wdrożenie lub aktualizację polityk bezpieczeństwa informacji (SZBI), a także przeprowadzenie w JST audytów SZBI:

Zakres przedmiotu zamówienia cz. 1

Dział 1

Przygotowanie i wdrożenie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) składającego się z : Polityki Bezpieczeństwa Informacji, Polityki Zarządzania Systemem Teleinformatycznym, Polityki Zarządzania Ciągłością Działania wraz z Planami Ciągłości Działania, Polityki Zarządzania Incydentami Cyberbezpieczeństwa, Polityki Ochrony Danych, Analizy Ryzyka Bezpieczeństwa Informacji w obszarze IT oraz zostaną wprowadzone/dostosowane procedury: procedury korzystania z urządzeń mobilnych, procedury pracy zdalnej, postępowanie z nośnikami, procedury kontroli dostępu, zabezpieczenie pomieszczeń i obiektów, procedury czystego biurka, procedury czystego ekranu, procedury kopii zapasowych, procedury ochrony logów, bezpieczeństwo komunikacji, zarządzanie bezpieczeństwem sieci, przesyłanie informacji, plany ciągłości działania, procedury zarządzania incydentami, prywatność i ochrona danych osobowych, szacowanie ryzyka w obszarze bezpieczeństwa informacji, szkolenia personelu, plan zarządzania podatnościami, plan reagowania na incydenty, plan przywracania, Analiza ryzyka i aktualizacja polityk i procedur w okresie 24 miesięcy od dnia zawarcia Umowy.

Usługa do realizacji w Gminie Krościenko Wyżne w terminie 6 miesięcy od dnia podpisania umowy.

Dział 2

Audyt Bezpieczeństwa Informacji zgodny z przepisami Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t. j. Dz. U. 2024 r., poz. 773) wraz z Ankietą końcową - Ankieta Dojrzałości cyberbezpieczeństwa wg załącznika Nr 6 do regulaminu konkursu grantowego „Cyberbezpieczny Samorząd”.

Usługa do realizacji w Gminie Krościenko Wyżne w terminie 6 miesięcy od dnia podpisania umowy.

-Zleceniobiorca zobowiązuje się do opracowania i dostarczenia Zamawiającemu wytworzonej dokumentacji oraz wyników audytu w wersji papierowej i elektronicznej podczas omówienia wyników.

- Zakończenie prac każdej z części musi zostać potwierdzone protokołem odbioru, podpisanym przez Wykonawcę i Zamawiającego.

- Podpisanie protokołu odbioru upoważnia Wykonawcę do wystawienia faktury (do każdej części).

- Brak rozpoczęcia działań w terminie 30 dni kalendarzowych od terminu złożenia oficjalnego zamówienia, upoważnia Zamawiającego do odstąpienia od zamówienia.

CZĘŚĆ 2.

Podniesienie poziomu wiedzy i kompetencji personelu JST kluczowego z punktu widzenia SZBI wdrożonego w urzędzie

Zakres przedmiotu zamówienia cz. 2

Przeprowadzenie szkoleń z zakresu podstaw cyberbezpieczeństwa (budujących świadomość cyberzagrożeń i sposobów ochrony) dedykowane kadrze pracowniczej (osób niebędących pracownikami IT).

Wymagania co do organizacji szkoleń:
- szkolenia przeprowadzone drogą online;
- czas trwania szkolenia dla każdej grupy: max. 3 godziny;
- ilość Uczestników szkoleń: 20 osób, podzielonych na 2 grupy;
- terminy realizacji: 3 miesiące od dnia podpisania umowy;
- szkolenie zakończone wystawieniem certyfikatów dla każdego Uczestnika;
- minimalny zakres szkolenia: Data Leak, Polityka haseł, Socjotechniki, Phishing / Spoofing, Vhishing / ID Call Hijacking, Metadane, Web Archive, Pliki Cookies, Zagrożenia związane z nieznanym sprzętem, Ataki Bruteforce / Ataki Słownikowe, Spear Phishing.

- Wykonawca przedstawi Zamawiającemu do akceptacji szczegółowy zakres szkoleń najpóźniej 14 dni kalendarzowych przed uzgodnionym terminem realizacji szkolenia.

-Zrealizowanie szkoleń musi zostać potwierdzone protokołem odbioru, podpisanym przez Wykonawcę i Zamawiającego.

- Podpisanie protokołu odbioru upoważnia Wykonawcę do wystawienia faktury.

- Brak rozpoczęcia działań w terminie 30 dni kalendarzowych od terminu złożenia oficjalnego zamówienia, upoważnia Zamawiającego do odstąpienia od zamówienia.

CZĘŚĆ 3.

Wdrożenie technologii i systemów teleinformatycznych podnoszących poziom bezpieczeństwa informacji oraz środków zwiększających odporność - zgodnie z obowiązującymi przepisami prawa (w tym z rozporządzeniem w sprawie Krajowych Ram Interoperacyjności) a także z uwzględnieniem uznanych norm, standardów i rekomendacji w obrocie profesjonalnym

Zakres przedmiotu zamówienia cz. 3

Przedmiotem zamówienia jest dostawa sprzętu oraz oprogramowania IT oraz wdrożenie systemów i rozwiązań teleinformatycznych (instalacja, konfiguracja i integracja) mających na

celu podniesienie poziomu cyberbezpieczeństwa oraz zwiększenie odporności Jednostki w ramach projektu grantowego pn. „Cyberbezpieczny Samorząd" realizowanego w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC). Priorytet II: Zaawansowane usługi cyfrowe.
Działanie 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa.

Zakres zamówienia składa się z następujących zadań:

1. Dostawa, instalacja oraz konfiguracja urządzeń sieci WLAN i LAN:

- Przełącznik sieciowy 48 port – 1 szt.
- Punkt dostępowy 802.11ax zgodny z Wi-Fi 6 – 5 szt.
- Oprogramowanie do centralnego zarzadzania.
- Usługi instalacji, konfiguracji oraz wdrożenia.

2. Dostawa, instalacja oraz konfiguracja urządzenia typu NGFW, implementacja mechanizmów bezpieczeństwa sieciowego:

- Urządzenie NGFW.
- Usługi instalacji, konfiguracji oraz wdrożenia.

3. Zakup platformy serwerowej wraz z odpowiednim środowiskiem systemowym na potrzeby wdrożenia usług katalogowych oraz oprogramowania zwiększającego poziom cyberbezpieczeństwa:

- Serwer wirtualizacji Rack 19" – 1 kpl.
- Oprogramowanie systemowe i wirtualizacyjne – 1 kpl.
- Licencje dla użytkowników serwera – 20 lic.
- Usługi instalacji, konfiguracji oraz wdrożenia.

4. Dostawa, instalacja i konfiguracja systemu archiwizacji danych oraz wykonywania kopii zapasowych:

- Serwer NAS– 1 kpl.
- Oprogramowanie do archiwizacji i backupu danych serwerowych – 1 lic.
- Oprogramowanie do archiwizacji i backupu danych stacji roboczych – 5 lic.
- Usługi instalacji, konfiguracji oraz wdrożenia.

5. Wdrożenie Systemu Centralnej Autoryzacji i zarządzania tożsamością:

- Serwer Centralnej Autoryzacji (AD, MFA, VPN) – 1 lic.
- Licencje dostępowe do Serwera Centralnej Autoryzacji – 100 lic.
- Licencje systemu MFA – 4 lic.
- Usługi instalacji, konfiguracji oraz wdrożenia - 1 kpl.

6. Dostawa i wdrożenie kompleksowego rozwiązania do monitorowania bezpieczeństwa EDR/XDR, szkolenie:

- Oprogramowanie EDR/XDR – 26 lic.
- Usługi instalacji, konfiguracji oraz wdrożenia.

- Organizacja i przeprowadzenie autoryzowanego szkolenia z narzędzia EDR/XDR.

7. Podniesienie poziomu bezpieczeństwa danych poprzez wdrożenie polityki backupu.

8. Dostawa, instalacja oraz uruchomienie UPSów:

- UPS serwerowy RACK – 1 szt.
- UPS stanowiskowy 1000 VA – 3 szt.

3. Ogólne wymagania Zamawiającego

Niniejszy dokument ma na celu umożliwienie dokonania wyboru najkorzystniejszej oferty na dostawę oprogramowania i urządzeń, wdrożenie rozwiązań oraz zapewnienie innych usług teleinformatycznych, których podstawowym celem jest podniesienie poziomu bezpieczeństwa informacji oraz zwiększenie odporności JST, w ramach projektu „Cyberbezpieczny Samorząd".
Dokument zawiera opis wymagań pod kątem kryteriów funkcjonalnych, technicznych i jakościowych, oraz wskazuje technologie, które muszą być wykorzystane tak aby osiągnąć założone cele i zapewnić optymalną relację ceny do jakości rozwiązania.
Opisane w dokumencie wymagania należy traktować jako podstawowe i minimalne.
Tam, gdzie w opisie przedmiotu zamówienia został wskazany znak towarowy (marka), producent, dostawca, patent, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty dostarczone przez konkretnego Dostawcę lub nastąpiło wskazanie norm, europejskich ocen technicznych, wspólnych specyfikacji technicznych lub innych odniesień, o których mowa w art. 101 ust. 1 pkt 2 lub ust. 3 ustawy, Zamawiający zgodnie z art. 99 ust. 5 ustawy dopuszcza złożenie oferty równoważnej lub z godnie z art. 101 ust. 4 ustawy zaoferowanie rozwiązań „równoważnych" w stosunku do wskazanych w opisie przedmiotu zamówienia pod warunkiem, że zapewnią uzyskanie parametrów technicznych nie gorszych od założonych w SWZ.
Ciężar wykazania spełnienia tych wymagań leży po stronie wykonawcy w składanej ofercie lub jeżeli ten przypadek ma miejsce w trakcie realizacji umowy – w chwili zaistnienia konieczności dokonania takiej zmiany.
- W przypadku zastosowania zasad wskazanych powyżej w trakcie realizacji umowy, mogą one wystąpić pod warunkiem, że zmiany te nie będą wpływać na oferowany w ofercie przedmiot zamówienia i efekt zakreślony niniejszym OPZ.
- W przypadku zastosowania materiałów, urządzeń, wyrobów lub rozwiązań równoważnych, Wykonawca zobowiązany jest do ich wskazania w ofercie oraz do złożenia wraz z ofertą kart technicznych lub innych dokumentów potwierdzających, że oferowane rozwiązania równoważne spełniają wymagania Zamawiającego opisane w przedmiocie zamówienia.

Wymagania ogólne dotyczące sprzętu:

1. Wszystkie dostarczone urządzenia muszą być fabrycznie nowe, bez wad i uszkodzeń, nieregenerowane, nieużywane i nie będące przedmiotem wystaw i prezentacji oraz o ile nie wyspecyfikowano inaczej w wymaganiach szczegółowych dla urządzeń, wyprodukowane po dniu 30 czerwca 2023 r.
2. Wszystkie urządzenia będą pochodziły z oficjalnego, europejskiego kanału dystrybucji, nie dopuszcza się urządzeń posiadających wadę prawną w zakresie pochodzenia sprzętu, wsparcia technicznego czy w zakresie gwarancji producenta.
3. Urządzenia zostaną dostarczone przez Wykonawcę własnym transportem i na własny koszt w miejsce wskazane przez Zamawiającego. Wszystkie urządzenia muszą być dostarczone w oryginalnych opakowaniach producenta.
4. Wszystkie urządzenia powinny być zgodne z normami UE i przeznaczone na rynek UE, oraz powinny posiadać certyfikat CE.
5. Dostarczany sprzęt powinien być kompletny i gotowy do uruchomienia, tak aby nie był konieczny zakup dodatkowych elementów czy akcesoriów.
6. Wykonawca dostarczy stosowne potwierdzenie gwarancji sprzętu i oprogramowania zapewniające, że sprzęt objęty jest gwarancją producenta.
7. Serwis sprzętu będzie świadczony przez producenta lub jego autoryzowanego partnera serwisowego posiadającego wdrożoną normę min. PN-EN ISO 9001 lub równoważną.

8. Sprzęt dostarczany w ramach niniejszego zamówienia, powinien być objęty 24 miesięczną gwarancją i wsparciem producenta, chyba że okres i warunki gwarancji zostały dodatkowo określony w opisie szczegółowym specyfikowanego wyposażenia/sprzętu. W okresie gwarancji Wykonawca jest zobowiązany zapewnić Zamawiającemu:
    a. usuwanie wszelkich wad i nieprawidłowości powstałych na wskutek standardowej i zgodnej z przeznaczeniem eksploatacji przedmiotu zamówienia,
    b. przyjmowanie zgłoszeń serwisowych w godzinach 8.00-20.00 (telefonicznie oraz e-mail) z możliwością zgłaszania awarii bezpośrednio u producenta (na wypadek braku reakcji serwisowej ze strony Wykonawcy),
    c. dostęp do bezpośredniego wsparcia technicznego producenta wraz z prawem do aktualizacji oprogramowania systemowego.
9. W ramach gwarancji wymagane jest wsparcie producenta sprzętu, a czas reakcji na zgłoszenia będzie realizowany w trybie następny dzień roboczy w miejscu instalacji i zastrzeżeniem, że uszkodzone nośniki danych pozostają u Zamawiającego. Ponadto wymagane jest, aby dostarczony poziom wsparcia producenta dawał możliwość kategoryzacji zgłoszeń i w przypadku awarii krytycznych gwarantował natychmiastową pomoc telefoniczną, szybką interwencję specjalisty ds. eskalacji zgłoszeń oraz wizytę serwisanta i/lub wysyłkę uszkodzonych części.
10. Udzielona gwarancja producenta nie wyłącza uprawnień Zamawiającego z tytułu rękojmi w stosunku do Wykonawcy.

Wymagania ogólne dotyczące oprogramowania:
Wykonawca zobowiązany jest dostarczyć Zamawiającemu:

1. certyfikaty licencyjne wystawione przez producenta Oprogramowania, o ile nie są dostępne w formie elektronicznej na dedykowanym portalu klienckim;
2. nośniki instalacyjne Oprogramowania, o ile nie są dostępne w formie elektronicznej na dedykowanym portalu klienckim;
3. adresy poczty elektronicznej, numery telefonów oraz inne dane dostępowe umożliwiające Zamawiającemu korzystanie ze Wsparcia technicznego świadczonego przez producenta Oprogramowania w pełnym zakresie, o ile nie są dostępne w formie elektronicznej na ogólnodostępnym lub dedykowanym portalu klienckim;
4. zestawienie dostarczonych Zamawiającemu pozycji w zakresie Oprogramowania, zawierające m.in.: numer partii (SKU), pełna nazwa produktu, wersja i edycja oprogramowania, metryka licencyjna, rodzaj licencji (terminowa/bezterminowa), okres obowiązywania licencji, okres obowiązywania wsparcia technicznego, poziom wsparcia technicznego;
5. standardowe warunki licencyjne producenta Oprogramowania, o ile nie są dostępne w formie elektronicznej na ogólnodostępnym lub dedykowanym portalu klienckim;
6. standardowe warunki Wsparcia technicznego producenta Oprogramowania, o ile nie są dostępne w formie elektronicznej na ogólnodostępnym lub dedykowanym portalu klienckim;
7. oświadczenie producenta Oprogramowania potwierdzające dostawę licencji i objęcie ich wsparciem technicznym na poziomie zgodnym z wymaganiami Zamawiającego, o ile nie potwierdzają jej certyfikaty licencyjne i standardowe warunki Wsparcia technicznego.

Wymagania w zakresie dokumentacji technicznej:
Przed rozpoczęciem prac wdrożeniowych, Wykonawca zobowiązany jest do opracowania dokumentacji technicznej (koncepcji technicznej wdrożenia) na podstawie wcześniej przeprowadzonej analizy przedwdrożeniowej oraz z uwzględnieniem wymagań warunków zamówienia. Zakres dokumentacji technicznej powinien obejmować:
a) Projekt techniczny wdrożenia.

b) Harmonogram Wdrożenia.
c) Dokumentację Powykonawczą (po zakończeniu realizacji prac wdrożeniowych).

Dokumentacja powinna zawierać schematy i architekturę wdrażanych systemów i rozwiązań.

Pozostałe wymagania:

Realizacja powyższego zakresu zamówienia musi być wykonana w oparciu o obowiązujące przepisy, przez Wykonawcę posiadającego stosowne doświadczenie, uprawnienia i potencjał wykonawczy oraz osoby o odpowiednich kwalifikacjach i doświadczeniu zawodowym.

Wykonawca zobowiązany jest do powołania zespołu zajmującego się realizacją przedmiotu zamówienia składającego się co najmniej z:

- Kierownika Projekt ze strony Wykonawcy;
- Zespołu inżynierów odpowiedzialnych za konkretne obszary wdrożenia.

II. SZCZEGÓŁOWE WŁAŚCIWOŚCI I WYMAGANIA FUNKCJONALNO - UŻYTKOWE DLA CZĘŚCI 3

1. Dostawa, instalacja oraz konfiguracja urządzeń sieci WLAN i LAN.

Przed przystąpieniem do prac instalacyjno-wdrożeniowych, należy opracować koncepcję techniczną w zakresie rozbudowy i modernizacji sieci LAN/WiFi.

Koncepcja powinna obejmować:

- część instalacyjno-montażową;
- część aktywną związaną z zaplanowaniem architektury sieci i zakresu konfiguracji urządzeń aktywnych. Należy przygotować koncepcję wdrożenia uwzględniając hierarchiczny model projektowania i budowy sieci tj. wydzielając warstwę dystrybucyjną oraz dostępową.

1.1. Przełącznik sieciowy 48 port – 1 szt.

Przełącznik sieciowy wraz z niezbędnymi modułami SFP+ (do realizacji redundantnych połączeń w modelu hierarchicznym) o minimalnych parametrach:

a) Parametry podstawowe:
- Typ i liczba portów - 48x 10/100/1000 POE+ RJ45, 4x 10Gigabit Ethernet SFP+
- Budżet mocy dla POE – 370W
- Obudowa 1U, rackmount (dostarczone uchwyty montażowe)
- Możliwość stackowania przełączników – do 200 portów w stosie – z wykorzystaniem wbudowanych portów 10G oraz z zachowaniem funkcji cross-stack w tym Link Aggregation i port mirroring

b) Zarządzenie energią:
- Obsługa standardu Energy Efficient Ethernet (IEEE 802.3az)
- Możliwość wyłączenia diod LED w celu oszczędzania energii
- Zasilanie PoE można włączać i wyłączać w oparciu o harmonogram zdefiniowany przez użytkownika w celu oszczędzania energii
- Zapewnia zasilanie PoE podczas restartu urządzenia

c) Parametry wydajnościowe:
- Przełącznik line-rate zapewniający pracę z pełną wydajnością wszystkich interfejsów
- Pamięć DRAM – 1GB
- Pamięć Flash – 512MB
- Wielkość bufora pakietów – 1.5MB
- Obsługa 4000 sieci VLAN
- 16.000 adresów MAC
- Wire-speed IPv4 routing – 990 tras statycznych; 128 interfejsów IP
- Obsługa ramek jumbo – do 9000 bajtów
- 2000 IGMP group
- 8 połączeń zagregowanych typu „port channel”
- Ilość wpisów w listach kontroli dostępu Security ACL – 1000

d) Obsługa protokołu SNTP

e) Obsługa IGMPv1/2/3 i MLDv1/2 Snooping

f) Obsługa routingu dynamicznego z wykorzystaniem protokołu RIPv2

g) Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
- IEEE 802.1w Rapid Spanning Tree

- IEEE 802.1s Multi-Instance Spanning Tree
- Per-VLAN Rapid Spanning Tree (PVRST+)
- Obsługa 126 instancji protokołu STP

h) Obsługa protokołu LLDP i LLDP-MED
i) Obsługa Q-in-Q oraz Selective Q-in-Q
j) Urządzenie wspiera połączenia link aggregation zgodnie z IEEE 802.3ad (LACP)
k) Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
l) Możliwość uruchomienia funkcji serwera DHCP
m) Mechanizmy związane z bezpieczeństwem sieci:
   - Wiele poziomów dostępu administracyjnego poprzez konsolę
   - Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN
   - Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X
   - Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
   - Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X
   - Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard
   - Obsługa funkcji IPv6 RA Guard, ND Inspection, DHCPv6 Guard
   - Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+
   - Obsługa Private VLAN z możliwością definicji portów promiscuous, isolated i community
   - Obsługa list kontroli dostępu (ACL) – możliwość filtracji ruchu w oparciu adresy MAC (source/destination), VLAN ID, adresy IPv4 lub IPv6, TCP/UDP source/destination port, 802.1p priorty, TCP flag. Obsługa czasowych list ACL
   - Obsługa mechanizmów zapewaniających bezpieczną pracę urządzenia w tym ochronę procesów: Executable Space Protection [X-Space], Address Space Layout Randomization [ASLR], Built-In Object Size Checking [BOSC]
   - Bezpieczny proces bootowania urządzenia
   - Suplikant 802.1X - przełącznik można skonfigurować tak, aby działał jako suplikant do innego przełącznika
n) Mechanizmy związane z zapewnieniem jakości usług w sieci:
   - Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi
   - Implementacja algorytmu Weighted Round-Robin (WRR) dla obsługi kolejek
   - Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)
   - Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP
   - Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi
   - Kontrola sztormów dla ruchu broadcast/multicast/unicast
   - Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP
   - Optymalizacja ruchu iSCSI - mechanizm nadawania priorytetu ruchowi iSCSI w stosunku do innych typów ruchu

o) Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN i RSPAN z możliwością konfiguracji do 4 sesji monitorujących
p) Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.)
q) Obsługa protokołu sFlow
r) Zarządzanie:
   - Port konsoli – USB typu C i RJ45
   - Port USB umożliwiający podłączenie zewnętrznego nośnika danych np. w celu uaktualnienia oprogramowania urządzenia
   - Obsługa protokołów SNMPv3, SSHv2, https, syslog, SCP
   - Aplikacja mobilna umożliwiająca łatwe zarządzania urządzeniami
   - Wbudowany graficzny interfejs zarządzania przełącznikiem dostępny z poziomu przeglądarki
   - Tekstowy plik konfiguracyjny – z możliwością edycji z pomocą edytora tekstu
s) Zasilacz AC 230V
t) Praca w szerokim zakresie temperatur: 0°C – 50°C
u) Głębokość urządzenia nie przekracza 35cm

1.2. Punkt dostępowy 802.11ax zgodny z Wi-Fi 6 – 5 szt.

Punkt dostępu bezprzewodowego:

a) obsługa standardów IEEE 802.11a/b/g/n/ac/ax
   - obsługa OFDMA (uplink/downlink), BSS Coloring
   - obsługa MU-MIMO – min. 2x2
   - obsługa kanałów 20, 40 MHz dla 802.11n
   - obsługa kanałów 20, 40, 80 MHz dla 802.11ac/ax
   - obsługa prędkośći PHY do 1,4 Gbps (ax)
   - obsługa agregacji ramek A-MPDU (Tx/Rx), A-MSDU (Tx/Rx)
   - obsługa beamforming 802.11ax
   - obsługa MRC (Maximal Ratio Combining)
b) konfigurowalna moc nadajnika
   - dla zakresu 2.4 GHz: do 20 dBm
   - dla zakresu 5GHz: do 20 dBm
c) praca dwuzakresowa w pasmach: 2,4 GHz oraz 5 GHz
d) segmentacja z użyciem VLAN (minimum 16 vlan)
e) portal captive dla gości
f) zarządzenie HTTPS, SNMP
g) Wsparcie dla protokołów:
   - 802.11r
   - 802.11h
   - 802.1X, RADIUS Authentication, Authorization, and Accounting (AAA)
   - obsługa modyfikacji autoryzacji w wyniku uwierzytelnienia AAA (RADIUS)
   - wsparcie IEEE 802.11i, WPA2, WPA3
h) interfejs GigabitEthernet (10/100/1000)
i) zintegrowane anteny o minimalnym zysku 4 dBi dla pasma 2,4 GHz i 5 dBi dla pasma 5 GHz
j) kompatybilny z PoE (Power over Ethernet), zgodność z IEEE 802.3af/at
k) anteny zintegrowane o zysku min. 4 dBi dla pasma 2,4 GHz oraz 5 dBi dla pasma 5 GHz

l) obudowa przystosowana do pracy w zakresie temperatur 0 – 40°C

1.3. Oprogramowanie do centralnego zarządzania.

Oprogramowanie do centralnego zarzadzania i monitorowania siecią zbudowaną z dostarczonych urządzeń sieciowych (przełączniki oraz punkty dostępowe).

a) narzędzie w formie maszyny wirtualnej posiadające wsparcie dla dostarczonego systemu wirtualizacji,
b) monitorowanie wydajności: System powinien monitorować kluczowe wskaźniki wydajności sieci,
c) alerty i powiadomienia: Konfiguracja alertów w przypadku wystąpienia problemów sieciowych
d) wizualizacja sieci: Graficzne przedstawienie topologii sieci,
e) generowanie raportów: Tworzenie raportów dotyczących wydajności, bezpieczeństwa i dostępności sieci,
f) eksport danych: możliwość eksportowania raportów w popularnych formatach (PDF, CSV),
g) szablony konfiguracji: umożliwienie tworzenia i stosowania szablonów konfiguracji dla urządzeń,
h) kopie zapasowe: automatyczne tworzenie kopii zapasowych konfiguracji urządzeń,
i) system musi być kompatybilny i posiadać wsparcie z dla dostarczonych urządzeń sieciowych,
j) zarządzanie użytkownikami: możliwość tworzenia kont użytkowników z różnymi poziomami uprawnień.

1.4. Usługi instalacji, konfiguracji oraz wdrożenia.

W ramach zamówienia należy dostarczyć, zainstalować oraz skonfigurować urządzenia aktywne sieci tj. przełączniki sieciowe oraz urządzenia sieci bezprzewodowej.
Należy przygotować koncepcję wdrożenia uwzględniając hierarchiczny model projektowania i budowy sieci tj. wydzielić warstwę dystrybucyjną (przełącznik dystrybucyjny oraz serwerowy z redundancją i mechanizmem stack) oraz warstwę dostępową sieci (dostarczone oraz istniejące przełączniki dostępowe).
Ponadto wymagana będzie segmentacja sieci w oparciu o technologię 802.1Q (VLAN) oraz konfiguracja innych mechanizmów sieciowych które przyczynią się do poprawy bezpieczeństwa, wydajności i dostępność oraz sieci wewnętrznej LAN.
Dodatkowo zamówienie obejmuje dostawę oraz instalację sieci bezprzewodowej (kompleksowo: okablowanie, montaż urządzeń i uruchomienie) obejmującej zasięgiem budynek Urzędu Gminy. Sieć WiFi powinna być oparta o kontroler sieci bezprzewodowej i co najmniej 5 urządzen AP (Access Point). Przed instalacją urządzeń należy wykonać pomiary predykcyjne i wyznaczyć optymalną lokalizację dla urządzeń AP aby zapewnić odpowiednie pokrycie zasięgiem sieci oraz wydajność.

Zakres prac instalacyjno-wdrożeniowych powinien obejmować co najmniej:

1. Część pasywna:
    - zakończenie torów kablowych w istniejącej szafie 19'' (w punkcie dystrybucyjnym sieci LAN);
    - montaż urządzeń bezprzewodowych oraz instalacja innych urządzeń aktywnych sieci LAN;
    - wykonanie połączeń między urządzeniami dostarczonymi oraz istniejącymi;
    - wykonanie pomiarów dynamicznych torów kablowych.

2. Część aktywna:
    - aktualizacja oprogramowania urządzeń do najnowszej wersji stabilnej, zalecanej przez producenta;
    - konfiguracja środowiska zarządzania w szczególności: ustawienie wszystkich parametrów związanych z adresacją i routingiem IP, ograniczenie zdalnego dostępu do urządzeń, konfiguracja autentykacji użytkowników, zapewnienie możliwości zarządzania poprzez protokoły SSH i HTTPS, podłączenie do systemu centralnego zarządzania;
    - konfigurację mechanizmów STP;
    - wykonanie segmentacji sieci (serwery, peryferia, stacje robocze, goście itp) w oparciu o technologię 802.1Q;
    - integracja z systemem centralnej autentykacji i zarządzania tożsamością i wdrożenie mechanizmu 802.1x;
    - dodatkowo w celu ograniczenia niepożądanego ruchu w warstwie 2 wskazana jest izolacja poszczególnych komputerów (port isolation).

2. Dostawa, instalacja oraz konfiguracja urządzenia typu NGFW, implementacja mechanizmów bezpieczeństwa sieciowego

2.1. Urządzenie NGFW min. 8x GE RJ45 – 1 kpl.

Parametr lub warunek	Minimalne wymagania
Wymagania Ogólne	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. Uwaga! W przypadku dostawy tzw. produktów podwójnego zastosowania, Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
Interfejsy, Dysk, Zasilanie	1. System realizujący funkcję Firewall musi dysponować minimum: • 10 portami Gigabit Ethernet RJ-45.

	• 2 gniazdami SFP 1 Gbps. 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 1.4 mln. jednoczesnych połączeń oraz 45 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 900 Mbps. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 700 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 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
Kontrola aplikacji	1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
Kontrola WWW	1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.

	3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. 6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. 7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu -składnikowego. 3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. 4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu -składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
Logowanie	1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W 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.
Gwarancja, wsparcie oraz licencje	1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. 2. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: ICSA lub EAL4 dla funkcji Firewall. 3. Wymagane 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 na okres 12 miesięcy.

2.2. Usługi instalacji, konfiguracji oraz wdrożenia.

Przed rozpoczęciem prac instalacyjno-wdrożeniowych należy opracować ogólne założenia polityki bezpieczeństwa oraz koncepcję techniczną, która powinna zostać zatwierdzona przez Zamawiającego.

Zakres prac wdrożeniowych powinien obejmować co najmniej:

1. Przygotowanie polityki bezpieczeństwa komunikacji z Internetem.
2. Aktualizacja oprogramowania urządzeń do najnowszej wersji stabilnej, zalecanej przez producenta.
3. Instalacja urządzeń w szafach dystrybucyjnych, podłączenie okablowania i uruchomienie komunikacji w sieci LAN oraz na styku z Internetem.
4. Konfiguracja środowiska zarządzania w szczególności: ustawienie wszystkich parametrów związanych z adresacją i routingiem IP, ograniczenie zdalnego dostępu do urządzeń, konfiguracja autentykacji użytkowników, zapewnienie możliwości zarządzania poprzez protokoły SSH i HTTPS.
5. Konfiguracja autentykacji użytkowników w zakresie dostępu do poszczególnych usług (aplikacji) w oparciu o usługi katalogowe AD.
6. Konfiguracja inspekcji ruchu pod katem programów złośliwych, wirusów itp.
7. Konfiguracja mechanizmów zabezpieczających przed znanymi atakami w sieci typu DoS, Spoofing, Sniffing itp.
8. Konfiguracja systemu raportowania oraz rejestru zdarzeń.
9. Testy poprawności konfiguracji
10. Przygotowanie instrukcji wykonywania kopii konfiguracji urządzenia i odtwarzania w przypadku awarii.

Ponadto zakres prac wdrożeniowych może obejmować inne usługi i mechanizmy, takie jak:

- Kształtowania ruchu.

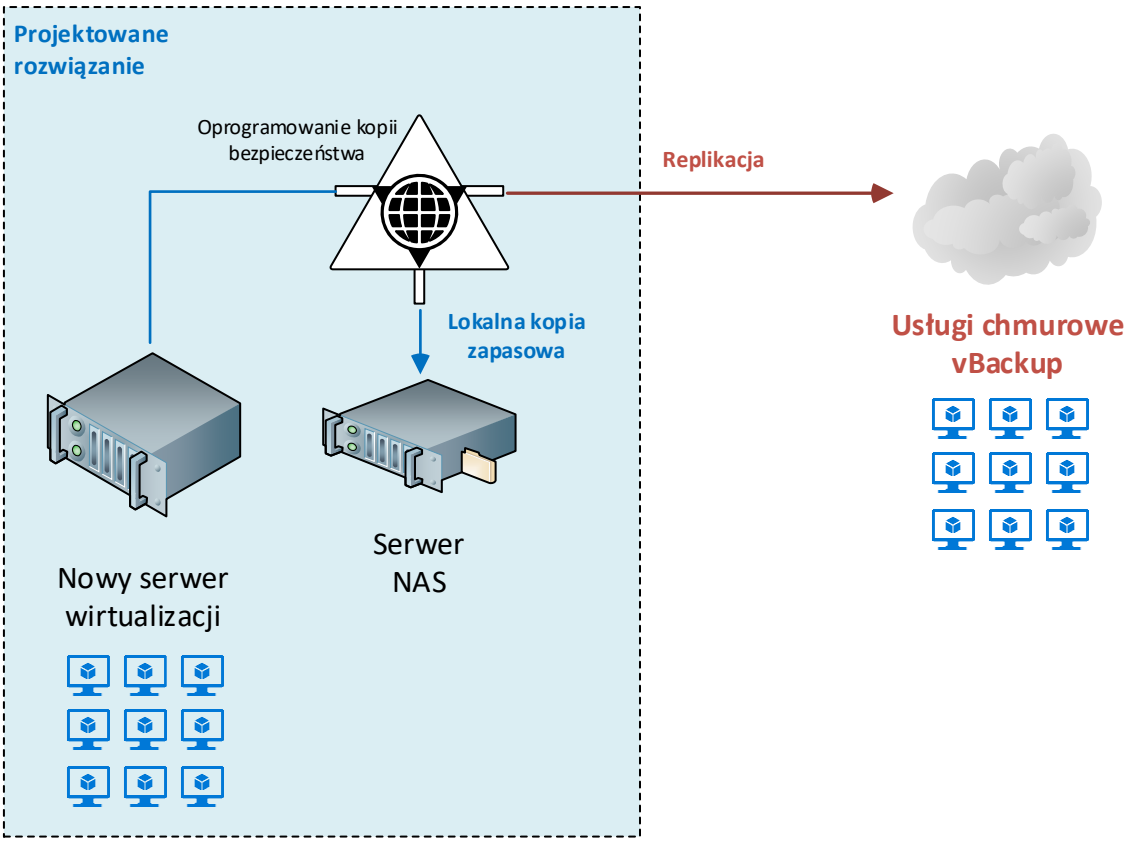
- Konfiguracja systemu: Intrusion Prevention System (IPS).
- Optymalizacja WAN (kilka łącz internetowych)
- Logowanie zdarzeń:
    1. dostępu do internetu,
    2. wystąpień naruszeń bezpieczeństwa,
    3. logowania użytkowników,
    4. wykrycia niepożądanego ruchu.

3. Zakup platformy serwerowej wraz z odpowiednim środowiskiem systemowym na potrzeby wdrożenia usług katalogowych oraz oprogramowania zwiększającego poziom cyberbezpieczeństwa

Serwer wirtualizacji należy skonfigurować i podłączyć do sieci zamawiającego. W ramach jego zasobów należy wdrożyć usługi:

- Podstawowy oraz zapasowy kontroler domeny, usługi katalogowe LDAP.
- Dodatkowe usługi domenowe DHCP, WSUS, PrintServer, Serwer Plików, Centrum certyfikatów.
- Centralny system Autoryzacji i zarzadzania tożsamością.
- Wirtualna przystawka do zarządzania infrastrukturą backup'ową.
- Systemy do zarządzania monitoringu stanu infrastruktury IT i infrastruktury serwerowej.

Kopie serwera powinny być wykonywane w ramach nowo dostarczonego systemu NAS i oprogramowania
Poniżej przedstawiono ogólny schemat docelowego rozwiązania, obejmujący dostarczane w ramach postępowania serwer NAS wraz z zasobami dyskowymi oraz projektowany do wdrożenia system serwerowy, który poza kopią lokalną będzie miał możliwość backupowania do udziałów chmurowych:



Projektowane rozwiązanie obejmuje następujące elementy infrastruktury serwerowej:

- serwer wirtualizacji,
- system NAS,
- oprogramowanie systemowe oraz oprogramowanie do wykonywania kopii bezpieczeństwa z uwzględnieniem dodatkowej lokalizacji (opcja repliki danych do chmury).

Dostawa oraz wdrożenie wszystkich wskazanych wyżej elementów infrastruktury odpowiada na zdiagnozowane potrzeby w ramach przeprowadzonej inwentaryzacji i wypełnia sugestie i zalecenia programowe w zakresie zwiększenia odporności i możliwości reagowania na zagrożenia.
Projektowane rozwiązanie powinno również spełnić wymagania określone w rozdziale IV rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, obowiązujących norm oraz standardów rynkowych.
Zgodnie bowiem z zapisami §20 ust. 2 (KRI) system powinien spełniać wymagania w zakresie:
- minimalizacji ryzyka utraty informacji w wyniku awarii,
- zapewnienia bezpieczeństwa przechowywanych plików systemowych oraz innych,
- zapewnienia możliwości regularnej aktualizacji oprogramowania (nowy system będzie posiadał wsparcie techniczne producenta w okresie eksploatacji).

Szczegółowe wymagania w zakresie parametrów technicznych i funkcjonalnych poszczególnych elementów infrastruktury zostały określone w dalszej części dokumentu.

3.1. Serwer wirtualizacji Rack 19” – 1 kpl.

Parametr lub warunek	**Minimalne wymagania techniczne i funkcjonalne**
Obudowa	Typu RACK, wysokość 2U. Szyny umożliwiające wysunięcie serwera z szafy stelażowej z możliwością instalacji ramienia do zarządzania kablami. Możliwość zainstalowania min. 12 dysków twardych hot plug 3,5”, Wszystkie dyski muszą być obsługiwane przez pojedynczy zainstalowany kontroler RAID.
Płyta główna	Dwuprocesorowa. Wyprodukowana i zaprojektowana przez producenta serwera. Możliwość instalacji procesorów 64-rdzeniowych. Min. 3 złącza PCI Express generacji 4 w tym: 1 fizyczne złącze o prędkości x16. Min. 1 złącze OCP 3.0 na potrzeby instalacji karty sieciowej. Min. 32 gniazda pamięci RAM. Wsparcie dla technologii: SDDC, ADDDC, ECC, Memory Mirroring. Wbudowany wewnętrzny slot na kartę Micro SD.
Procesor	Procesor 16-rdzeniowy, taktowanie bazowe 2GHz, architektura x86_64, maksymalny TDP 150W. Osiągający w teście SPEC CPU 2017 Floating Point wynik min. 383 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie http://spec.org/cpu2017/results/cpu2017.html dla oferowanego serwera.
Ilość procesorów	2
Pamięć	512 GB RAM DDR5 Registered 5600MHz. Pamięci obsadzone w sposób gwarantujący najwyższa możliwość wydajność. Możliwość rozbudowy do 8TB RAM.
Dyski twarde	4 szt. dysków SATA Hot-Plug 1,92TB SSD Mixed Use. 4 szt. dysków SATA 4TB HDD Hot-Plug 7200 RPM.

	Możliwość instalacji na płycie głównej 2 dysków M.2 zabezpieczonych sprzętowym Raid (dyski nie mogą zajmować złączy PCI Express, ani klatek dla dyski hot plug).
Kontrolery I/O	Kontroler SAS RAID 12Gb dla dysków wewnętrznych posiadający 4GB pamięci cache, obsługujący poziomy RAID: 0,1,10,5,50,6,60 z podtrzymaniem pamięci cache w przypadku utraty zasilania.
Kontrolery LAN	4x 1Gbit Base-T RJ45, Karta nie może zajmować żadnego ze slotów PCIe Dodatkowo 2x 10Gbit Base-T RJ45.
Porty	Z przodu obudowy: 1x USB 3.2, 1x USB 2.0 (z możliwością zarządzania serwerem), możliwość instalacji portu VGA. Wewnątrz obudowy: 1x USB 3.2, slot na kartę Micro SD. Z tyłu obudowy: 3x USB 3.2, 1x VGA, 1x RJ-45 do zarządzania serwerem, możliwość instalacji portu DB9. Wszystkie tylne porty USB, port RJ-45 służący do zarządzania, tylny port VGA, wewnętrzny port USB, wewnętrzny port na kartę Micro SD powinny być umieszczone na osobnej dedykowanej płytce I/O, którą łączy się bezpośrednio z płytą główną serwera. Możliwość instalacji dodatkowego redundantnego portu RJ45 służącego do zarządzania, w slocie OCP zamiast karty sieciowej.
Diagnostyka	Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID. Możliwość użycia aplikacji mobilnej na telefonie, do przeglądania awarii, konfiguracji i włączenia/wyłączenia serwera.
Zarządzanie	Wymagany wbudowany sprzętowy kontroler zdalnego zarządzania posiadający swój własny min. 2 rdzeniowy procesor o taktowaniu min. 1.2GHz. Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna Pozyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres ip karty zarządzającej, utylizacja cpu, utylizacja pamięci oraz komponentów I/O, lokalizacja Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów. Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń. Wysyłanie określonych zdarzeń poprzez SMTP oraz SNMPv3. Update systemowego firmware. Monitoring i możliwość ograniczenia poboru prądu. Zdalne włączanie/wyłączanie/restart. Zapis video zdalnych sesji. Podmontowanie lokalnych mediów z wykorzystaniem Java client. Przekierowanie konsoli szeregowej przez IPMI. Zrzut ekranu w momencie zawieszenia systemu. Możliwość przejęcia zdalnego ekranu. Możliwość zdalnej instalacji systemu operacyjnego. Alerty Syslog. Przekierowanie konsoli szeregowej przez SSH. Wyświetlanie danych aktualnych I historycznych dla użycia energii oraz temperatury serwera.

	Możliwość mapowania obrazów ISO z lokalnego dysku operatora. Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS. Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API. Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego. Kontroler zarządzania musi posiadać 4Gb wewnętrznej pamięci (dopuszcza się zastosowanie karty Micro SD w celu uzyskania tej pojemności). Pamięć kontrolera zarządzania musi pełnić funkcję RDOC (Remote Disc on Card) oraz musi umożliwiać przechowywanie plików firmware. Monitorowanie zmian sprzętowych w celu wykrycia nieoczekiwanych zmian. Po wykryciu zmiany zapis w logu serwera lub uniemożliwienie boot'u. Możliwość synchronizacji konfiguracji i poziomów firmware pomiędzy serwerami. Możliwość monitorowania i zarządzania grupą serwerwów z poziomu kontrolera zarządzania pojedynczego serwera. Ilość serwerów możliwych do zarządzania – minimum 200. Wraz z serwerem powinno zostać dostarczone dodatkowe oprogramowanie zarządzające umożliwiające: - zarzadzanie infrastruktura serwerów i storage bez udziału dedykowanego agenta, - przedstawianie graficznej reprezentacji zarządzanych urządzeń, - możliwość skalowania do minimum 1000 urządzeń, - obsługę szyfrowanej komunikacji z zarządzanymi urządzeniami, wsparcie dla NIST 800-131A oraz FIPS 140-2, - wsparcie dla certyfikatów SSL tzw self-signed oraz zewnętrznych, - udostępnianie szybkiego podgląd stanu środowiska, - udostępnianie podsumowania stanu dla każdego urządzenia, - tworzenie alertów przy zmianie stanu urządzenia, - monitorowanie oraz tracking zużycia energii przez monitorowane urządzenie, możliwość ustalania granicy zużycia energii, - konsola zarzadzania oparta o HTML 5, - dostępność konsoli monitorującej na urządzeniach przenośnych ze wsparciem dla systemu Android oraz iOS, aplikacja musi umożliwiać włączenie wyłączenie oraz restart urządzenia, musi również mieć możliwość aktywowania diody lokacyjnej na urządzeniu, - automatyczne wykrywanie dołączanych systemów oraz szczegółowa inwentaryzacja, - możliwość podnoszenia wersji oprogramowania dla komponentów zarządzanych serwerów w oparciu o repozytorium lokalne jak i zdalne dostepne na stronie producenta oferowanego rozwiązania, - definiowanie polityk zgodności wersji firmware komponentów zarządzanych urządzań, - definiowanie roli użytkowników oprogramowania, - obsługa REST API oraz Windows PowerShell, - obsługa SNMP, SYSLOG, Email Forwarding,

	- autentykacja użytkowników: centralna (możliwość definiowania wymaganego poziomu skomplikowania danych autentykacyjnych) oraz integracja z MS AD oraz obsługa single sign on oraz SAML, - obsługa tzw Forward Secrecy w komunikacji z zarządzanymi urządzeniami, - przedstawianie historycznych aktywności użytkowników, -blokowanie możliwości podłączenia innego systemu zarzadzania do urządzeń zarządzanych, - tworzenie dziennika zdarzeń ukończonych sukcesem lub bledem, oraz zdarzeń bedacych w trakcie. Możliwość definiowania filtrów wyświetlanych zdarzeń z dziennika. Możliwość eksportu dziennika zdarzeń do pliku csv, - Obsluga NTP, - przesyłanie alertów do konsoli firm trzecich, - tworzenie wzorców konfiguracji zarządzanych urządzeń (definiowanie przez konsole albo kopiowanie konfiguracji z już zaimplementowanych urządzeń), - instalowanie systemów operacyjnych oraz wirtalizatorów Vmware i Hyper-V. Wymagana jest integracja konsoli zarządzania z konsolą wirtualizatora tak, aby zarządzanie środowiskiem sprzętowym mogło odbywać się z konsoli wirtualizatora. Wymaga się możliwości instalacji systemu na przynajmniej 20 nodach jednocześnie - możliwość automatycznego tworzenia zgłoszeń w centrum serwisowym producenta dla określonych zdarzeń wraz z przesyłem plików diagnostycznych. Producent serwera ponadto powinien zapewniać narzędzia integrujące zarządzanie infrastrukturą z następującymi produktami: VMware vCenter, Microsoft AdminCenter, Microsoft SystemCenter, RedHat CloudForms, Splunk.
Bezpieczeństwo	Zainstalowany moduł TPM 2.0.
Wspierane OS	Wspierane systemy operacyjne: Microsoft Windows Server 2019, 2022; Red Hat Enterprise Linux 8.6, 8.7, 9.0, 9.1, SUSE Linux Enterprise Server 15 SP4 oraz 15 Xen SP4; VMware vSphere (ESXi) 7.0 U3, ESXI 8.0; Ubuntu 22.04 LTS.
Zasilanie, chłodzenie	Redundantne zasilacze hot plug o mocy min. 1100W z certyfikatem min. Titanium; Redundantne wentylatory hot plug, zainstalowane nadmiarowo min. N+1.
Gwarancja	3 lata gwarancji producenta serwera w trybie on-site z gwarantowanym czasem reakcji do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. Dyski twarde nie podlegają zwrotowi organizacji serwisowej. Możliwość wykupienia dodatkowego serwisu zapewniającego gwarantowany czas naprawy serwera w ciągu 6 godzin. W przypadku braku funkcjonalności przewidywania awarii dla wszystkich komponentów wymienionych w punkcie. Diagnostyka wymagane jest dostarczenie serwera nadmiarowego, mogącego zastąpić funkcjonalnie jak i wydajnościowo wymagania powyżej maszyny.
Dokumentacja, inne	Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymagane oświadczenie wykonawcy lub producenta. Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta.

	Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila, na który można zgłaszać usterki. W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji. Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera.

3.2. Oprogramowanie systemowe i wirtualizacyjne – 1 kpl.

Wymagana jest dostawa najnowszej wersji wieczystej licencji uprawniającej zgodnie z zasadami licencjonowania określonymi przez producenta do zainstalowania i użytkowania na oferowanym serwerze w środowisku fizycznym, lub min. czterech wirtualnych uruchomień serwerowego systemu operacyjnego posiadającego następujące, wbudowane cechy:

1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
2. Możliwość wykorzystywania 16 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. Możliwość uruchomienia czterech maszyn wirtualnych.
32. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

3.3. Licencje dla użytkowników serwera – 20 lic.

Wymagana jest dostawa najnowszej wersji wieczystej licencji uprawniającej zgodnie z zasadami licencjonowania producenta serwerowego systemu operacyjnego określonego w pkt. 3.2 do legalnego korzystania z zasobów serwerów przez min. 20 użytkowników.

3.4. Usługi instalacji, konfiguracji oraz wdrożenia.

W ramach zamówienia należy dostarczyć, zainstalować oraz skonfigurować środowisko wirtualizacji
Następnie wykonać wdrożenie usług, o których mowa w punkcie 4.4 oraz 5.4.

4. Dostawa, instalacja i konfiguracja systemu archiwizacji danych oraz wykonywania kopii zapasowych

Macierz dyskowa stanowi jeden z ważniejszych elementów infrastruktury IT ponieważ odpowiada za bezpieczeństwo przechowywania, przetwarzania oraz transmisji danych, w związku z tym rozwiązanie powinno spełniać wymagania określone w rozdziale IV rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, obowiązujących norm oraz standardów rynkowych.

Użytkowa przestrzeń dyskowa macierzy będzie wykorzystana na potrzeby:

- Zapisu danych z systemów dziedzinowych i ich archiwizacja.
- Przechowywania plików dziennika systemowego.
- Udostępnienia przestrzeni na udziały współdzielone.

Należy dostarczyć serwer pamięci masowej (NAS) wraz z dyskami dużej pojemności oraz wysokiej dostępności klasy Enterprise.
Macierz dyskowa zapewnia bezpieczeństwo danych poprzez zastosowanie redundantnych komponentów takich jak dyski i zasilacze (typu hot plug). Przestrzeń dyskowa zostanie skonfigurowana w macierz RAID 6 (awarii może ulec dwa dyski, a dane nie zostaną uszkodzone).
Dodatkowo do autoryzacji dostępu do danych na serwerze będzie wykorzystana infrastruktura AD, gdyż serwer NAS posiada możliwość podłączenia do domeny. Wszystkie zdarzenia logowania na urządzenie, zapisu bądź odczytu danych są logowane i archiwizowane na urządzeniu. Dodatkowo, wszystkie siłowe próby autoryzacji zostaną zablokowane (blacklist'a) a informacja o zdarzeniu przekazana drogą mailową do administratora.
Urządzenie obsługuje także dwuetapową autoryzację (MFA), która znacząco podnosi poziom bezpieczeństwa danych.

4.1. Serwer NAS – 1 kpl.

Parametr lub warunek	**Minimalne wymagania techniczne i funkcjonalne**
Obudowa	Typu RACK, wysokość 2U. Szyny umożliwiające wysunięcie serwera z szafy stelażowej z możliwością instalacji ramienia do zarządzania kablami. Możliwość zainstalowania 12 dysków twardych hot plug 2.5" / 3,5", oraz 2 dysków M.2 2280 PCIe Gen 5. Możliwość podłączenia modułu rozszerzającego o min. 16 dysków.
Płyta główna	Min. 3 złącza PCI Express generacji 4 w tym: • 2 fizyczne złącza o prędkości x4, • 1 fizyczne złącza o prędkości x8. 4 gniazda pamięci RAM DDR5.
Procesor	Procesor 8-rdzeniowy, taktowanie bazowe 3,8GHz, architektura x86_64 osiągający w teście CPU Mark wynik Multithread Rating 25500 pkt. Wynik musi być opublikowany na stronie www.cpubenchmark.net.
Pamięć	32 GB pamięci RAM z możliwością rozbudowy do 192GB. 5GB pamięci Flash do ochrony systemu operacyjnego przed podwójnym rozruchem.
Dyski twarde	4 szt. dysków 8TB SATA 6Gb/s 256GB Cache Hot-Plug, technologia NASware, praca 24x7.

	2 szt. dysków 2TB SSD SATA 6Gb/s Hot-Plug, technologia NAND, praca 24x7. Obsługa dysków o pojemności do 18 TB.
Kontrolery I/O	RAID 0,1,5,50,6,60,10, Triple Parity, Triple Mirror. • konfiguracja priorytetu odbudowy grup RAID, • RAID HotSpare i Global HotSpare, • SSD Trim, • HDD S.M.A.R.T. • skanowanie uszkodzonych bloków, wykrywanie uszkodzenia i naprawa danych, • Cache odczytu i dziennik zapisu z wykorzystaniem dysków SSD.
Kontrolery LAN	2x 10GBase-T RJ45 (10G/5G/2,5G/1G).
Porty	2x USB 3.2 Gen2 10Gb/s Typu A. Ilość dostępnych portów nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozdzielaczy czy dodatkowych kart rozszerzeń.
Zarządzanie	Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera Obsługiwane systemy plików: • dyski wewnętrzne: ZFS, • dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+. Szyfrowanie dysków zewnętrznych i udziałów, min AES 256 Obsługa minimum 2048 kopii migawkowych. Możliwość migracji danych ze zmianą poziomu RAID. Obsługa woluminów logicznych o maksymalnej pojemności min. 250 TB. Obsługa do 4096 użytkowników lokalnych. Wbudowana obsługa iSCSI: • obsługa wielu jednostek LUN na Target, • obsługa mapowania i maskowania LUN, • obsługa SPC-3 Persistent Reservation, • obsługa MPIO & MC/S, • wykonywanie migawek oraz kopii zapasowej LUN. Wbudowana obsługa Fibre Channel: • wsparcie opcjonalnych kart FC, • mapowanie LUN, Obsługa protokołów CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web. Funkcje: LDAP serwer i klient, VPN serwer i klient, obsługa PPTP, OpenVPN Wsparcie dla wirtualizacji: • możliwość uruchomienia maszyn wirtualnych z systemem Windows, Linux, Unix i Android, • import, klonowanie i kopie migawkowe maszyn wirtualnych, • GPU pass-through dla dodatkowych kart graficznych. Administracja systemu: • ochrona dostępu do sieci z automatycznym blokowaniem połączeń, • obsługa HTTP/HTTPS, FTP z SSL/TLS (Explicit), SFTP, • powiadamianie przez e-mail i SMS (z wykorzystaniem zewnętrznych usług), • DDNS oraz zdalny dostęp w chmurze producenta,

	• SNMP v2, v3, • monitorowanie zasobów systemu w czasie rzeczywistym, rejestr zdarzeń.
Zasilanie, chłodzenie	Redundantne zasilacze o mocy min. 550W. Min. 3szt wentylatorów.
Gwarancja	5 lat gwarancji producents w trybie on-site.

4.2. Oprogramowanie do archiwizacji i backupu danych serwerowych – 1 lic.

W ramach licencji wieczystej lub subskrypcji oprogramowania na okres nie krótszy niż 24 miesiące oprogramowanie musi spełniać następujące wymagania poprzez wbudowane mechanizmy:

Wsparcie dla Host-a	VMware ESX/ESX(i) 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0. Hyper-V. Citrix XenServer 4.1.5, 5.5, 5.6, 6.0, 6.1, 6.2, 6.5, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6. Red Hat Virtualization 4.0, 4.1. Linux KVM. Oracle VM Server 3.0, 3.3, 3.4. Scale Computing Hypercore 8.8, 8.9, 9.0, 9.1, 9.2, 9.3
Wsparcie dla maszyn wirtualnych	Windows XP (SP3) i nowsze. Windows Server 2003 i nowsze. Windows SBS 2011/2008, 2003/2003R2. Windows Storage Server 2012/2012R2, 2008R2/2008/2003. Windows MultiPoint Server 2012/2011/2010. Linux OS. macOS.
Zarządzanie systemem kopii zapasowych	• Interfejs zarządzania oparty na przeglądarce www. Zgodność interfejsu z większością popularnych przeglądarek www. • Interfejs musi być zgodny z platformami mobilnymi (możliwość zarządzania systemem z poziomu urządzenia mobilnego). • Interfejs musi oferować możliwość prezentacji najważniejszych danych dotyczących stanu systemu i zadań przez niego realizowanych w przejrzystej formie graficznej z możliwością dostosowania zawartości, treści i formy prezentacji poszczególnych danych. • Moduł raportujący z możliwością zdefiniowania zawartości, formy i częstotliwości generowania raportów oraz metody ich dostarczania (wysyłanie na podany adres email lub zapisywanie do wskazanego folderu). Definiowanie uprawnień dla administratorów system kopi zapasowych na poziomie dostępu do poszczególnych obiektów (maszyn, hostów, lokalizacji, modułów, itp.). • Integracja z MS Active Directory na poziomie zarządzania dostępem i administratorami.

	• Wsparcie dla Single Sign On dla logowania do systemu.
	• Zarządzanie procesem tworzenia kopi zapasowych dla wielu różnych podsieci, również w przypadku stosowania NAT. • Definiowanie planów wykonywania kopii zapasowych, ich replikacji i zarządzaniem ich retencją (kasowaniem). • Tworzenie zcentralizowanych (obejmujących swym zasięgiem wiele maszyn lub ich grupy) planów wykonywania kopi zapasowych. • Możliwość zdalnej instalacji agentów kopi zapasowych z poziomu konsoli cyberochrony na maszynach z systemem operacyjnym Windows. Zdalne uaktualniania agentów kopi zapasowych. • Zdalne zarządzanie procesem wykonywania kopii zapasowej i odzyskiwania danych. • Możliwość zdefiniowania dedykowanej maszyny, której agent kopi zapasowej wykonywał będzie czynności zarządzania i replikacji kopii zapasowych z wielu innych maszyn (zadania kopiowania, przenoszenia, konsolidacji plików kopi zapasowej). • Możliwość zastosowania zcentralizowanych modułów do zarządzania przechowywaniem plików kopii zapasowych. • Centralny katalog wszystkich danych zapisanych w kopiach zapasowych Wbudowany serwer PXE umożliwiający bootowanie maszyn przez sieć LAN z przygotowanego nośnika startowego.
Kopia zapasowa	• Kopie zapasowe całych dysków i partycji. • Kopie zapasowe wybranych plików i folderów. • Kopia zapasowa udziałów sieciowych. • Technologia bezagentowego wykonywania kopii zapasowej dla maszyn wirtualnych (dotyczy Hyper-V i VMWare ESXi). • Kopie zapasowe aplikacji (Exchange, SQL, SharePoint, Active Directory) Kopie zapasowe baz danych Oracle. • Kopie zapasowe hostów Hyper-V i VMWare ESXi. • Zapis kopi zapasowych (plikowych i dyskowych) w magazynie chmurowym dostarczanym przez producenta systemu kopi zapasowych. • Zapis kopi zapasowych na udziały sieciowe. Zapis kopi zapasowych na serwer SFTP. • Zapis kopi zapasowych na dedykowaną ukrytą partycję na maszynie, której kopia zapasowa jest wykonywana. • Zapis kopi zapasowych na urządzenia taśmowe (pojedyncze napędy, biblioteki taśmowe, autoloadery). • Możliwość wyszukiwania plików w kopiach zapasowych. Szyfrowanie plików kopii zapasowych. • Wsparcie dla technologii VSS.

	• Deduplikacja kopi zapasowych na poziomie bloków danych. Deduplikacja wykonywana na źródle w celu ograniczenia ilości danych przesyłanych przez sieć. • Kompresja plików kopii zapasowych. • Replikacja kopi zapasowych na kolejne nośniki (dyski, napędy taśmowe, magazyn chmurowy). • Możliwość zaplanowania zadań związanych weryfikacją, replikacją i retencją plików kopi zapasowych.
Odtwarzanie kopii zapasowych w oparciu o co najmniej:	• Odtworzenie całej maszyny (Windows, Linux, Mac) – tzw. Bare Metal Restore. • Odtworzenie całej maszyny (Windows, Linux, Mac) na innej platformie sprzętowej niż ta, z której wykonano kopię zapasową. • Odtworzenie całego hosta (Hyper-V i VMWare ESXi) na takiej samej lub innej platformie sprzętowej. • Odtworzenie poszczególnych plików i folderów. • Automatyzacja procesu odtwarzania całych maszyn – np.: po zabootowaniu maszyny z przygotowanego wcześniej nośnika, powinna zostać odtworzona ostatnia wykonany kopia zapasowa automatycznie, bez konieczności jej wyszukiwania i wskazywania). • Granularne odtwarzanie baz danych Microsoft Exchange. • Granularne odtwarzanie skrzynek pocztowych i poszczególnych wiadomości email z Microsoft Exchange. • Wyszukiwanie i podgląd odtwarzanych wiadomości email. Granularne odtwarzanie baz danych Microsoft SQL. Granularne odtwarzanie witryn i plików Microsoft SharePoint. Odtwarzanie kontrolerów domeny Microsoft Active Directory. Granularne odtwarzanie baz danych Oracle. • Przywracanie przyrostu względem danych, które już się znajdują na dysku, na który przywracana jest kopia zapasowa. • Dla hostów VMware ESXi i Hyper-V – uruchomienie maszyny wirtualnej bezpośrednio z pliku kopii zapasowej bez konieczności odtwarzania całej maszyny na hoście. Możliwość docelowego odtworzenia uruchomionej maszyny z pliku kopii zapasowej na wybranym hoście bez przerywania jej pracy.
Dodatkowe (obowiązkowe) wymagania związane ochroną	• Ochrona systemów operacyjnych Windows przed złośliwym oprogramowaniem typu ransomware w oparciu o heurystyczne algorytmy identyfikacji i eliminacji zagrożeń. • Skanowanie oprogramowania celem poszukiwania podatności. • Podatności wypisane muszą być z minimum informacjami takimi jak nazwa produktu, który zawiera podatność, maszyny na których znaleziono takie oprogramowanie, stopień ważności w skali CVSS.

Model Licencjonowania	• Możliwość zakupu licencji subskrypcyjnych w okresie 1/3/5 lat . • Model licencjonowania oparty na maszynach fizycznych i hostach – brak limitów na chronioną ilość danych, maszyn wirtualnych i aplikacji).

4.3. Oprogramowanie do archiwizacji i backupu danych stacji roboczych – 5 lic.

W ramach licencji wieczystej lub subskrypcji oprogramowania na okres nie krótszy niż 24 miesiące oprogramowanie musi spełniać następujące wymagania poprzez wbudowane mechanizmy:

Funkcje i ocena podatności na zagrożenia	• Identyfikowanie luki w zabezpieczeniach zanim znajdą je napastnicy. • Określenie potencjału zagrożeń dla Twoich systemów. • Zmniejszanie potencjalnych zagrożeń. • Zoptymalizowanie swoich inwestycji w bezpieczeństwo. • Automatyczne wykrywanie maszyn i zdalna instalacja agentów. • Wykrywanie maszyn za pomocą sieci. • Wykrywanie maszyn w oparciu o Active Directory. • Importuj listę maszyn z pliku. • Automatyczne przypisywanie planów ochrony. • Wsadowa instalacja zdalnego agenta za pomocą. specjalnego kreatora (Discovery Wizard).
Tworzenie kopii zapasowych i odzyskiwanie danych	• Szybkie i niezawodne odzyskiwanie aplikacji, systemów i danych - na dowolnym urządzeniu i po każdym incydencie. • Kopie zapasowe całych dysków i partycji. • Kopie zapasowe wybranych plików i folderów. • Kopia zapasowa udziałów sieciowych. • Zapis kopi zapasowych (plikowych i dyskowych) w magazynie chmurowym dostarczanym przez producenta systemu kopi zapasowych. • Zapis kopi zapasowych na udziały sieciowe. Zapis kopi zapasowych na serwer SFTP. • Zapis kopi zapasowych na dedykowaną ukrytą partycję na maszynie, której kopia zapasowa jest wykonywana. • Zapis kopi zapasowych na urządzenia taśmowe (pojedyncze napędy, biblioteki taśmowe, autoloadery). • Możliwość wyszukiwania plików w kopiach zapasowych. • Możliwość szyfrowania plików kopi zapasowych. Wsparcia dla technologii VSS. • Deduplikacja kopi zapasowych na poziomie bloków danych. Deduplikacja wykonywana na

	źródle w celu ograniczenia ilości danych przesyłanych przez sieć. • Kompresja plików kopi zapasowych. • Możliwość replikacji kopi zapasowych na kolejne nośniki (dyski, magazyn chmurowy). • Możliwość replikacji kopi zapasowych na nośniki taśmowe. • Możliwość zaplanowania zadań związanych weryfikacją, replikacją i retencją plików kopi zapasowych.
Ochrona Antimalware	Kompleksowa ochrona, oparta na sztucznej inteligencji ochrona przed złośliwym oprogramowaniem nowej generacji - w tym filtrowanie adresów URL i automatyczne skanowanie kopii zapasowych w poszukiwaniu złośliwego oprogramowania.
Cyberbezpieczeństwo i zarządzanie punktami końcowymi	Zarządzanie ochroną punktów końcowych: ocena podatności i zarządzanie poprawkami, funkcje zdalnego pulpitu i monitorowanie integralności dysków.
Ochrona danych	Tworzenie kopii zapasowej z dowolnego źródła danych na ponad 20 platformach - wirtualnych, fizycznych, w chmurze lub mobilnych, niezależnie od rozmiaru i lokalizacji danych. A nawet jeśli ilość danych rośnie lub infrastruktura ewoluuje, elastyczna, skalowalna pamięć masowa i łatwe zarządzanie kopiami zapasowymi sprawiają, że tworzenie kopii zapasowych danych przedsiębiorstwa jest bardzo proste. Kopia zapasowa obrazu dysku dzięki oprogramowaniu do tworzenia kopii zapasowych na komputerze PC, które tworzy kopie zapasowe całego komputera, a także wybranych plików lub danych, i zabezpieczaj kopie zapasowe w różnych miejscach pamięci masowej. Będziesz mógł łatwo odzyskać cały obraz lub odzyskać pojedyncze pliki, foldery, elementy i aplikacje.
Aktywna ochrona	Ochrona swoich pracowników przed atakami ransomware za pomocą oprogramowania do tworzenia kopii zapasowych na komputery PC, które aktywnie wykrywa, blokuje i odwraca podejrzane zmiany w danych, plikach kopii zapasowych i agentach kopii zapasowych. Wbudowana technologia wykorzystuje sztuczną inteligencję i uczenie maszynowe, aby zapewnić bezpieczeństwo danych. Uniwersalne przywracanie Dzięki któremu możesz odzyskać dane na innym sprzęcie, bez problemów z niezgodnością. Uzyskaj większą elastyczność dzięki oprogramowaniu do tworzenia kopii zapasowych na komputerze z systemem Windows, które może przywracać dane

	na tym samym komputerze lub dowolnym innym sprzęcie, w tym w środowiskach fizycznych lub wirtualnych typu bare-metal.
Funkcje dodatkowe oprogramowania	• Opatentowana technologia tworzenia obrazów dysków. • Magazyny danych – dyski, NAS, SAN. • Kopie zapasowe danych użytkowników. • Przyjazna dla ekranów dotykowych centralna i zdalna konsola zarządzająca dostępna z poziomu przeglądarki internetowej. • Modyfikowalne panele informacyjne. • Oracle Database. • Exchange i SQL w klastrach. • Centralny magazyn danych i deduplikacja. • Obsługa autoloaderów, bibliotek i napędów taśmowych. • Zarządzanie grupą oparte na zasadach. • Role administracyjne i przekazywanie zadań. • Zaawansowane raporty. • Operacje zarządzania kopiami zapasowymi off-host.
Przestrzeń chmurowa	Dostarczona wraz z oprogramowaniem. W przypadku uzyskania uzasadnionej pewności, że doszło do naruszenia bezpieczeństwa, producent oprogramowania bez zbędnej zwłoki dostarczy informacje o takowym naruszeniu na adres e-mail podany podczas rejestracji konta. W przypadku wyżej wymienionego naruszenia, producent podejmie kroki, aby udokumentować, naprawić i zminimalizować skutki naruszenia bezpieczeństwa w odniesieniu do danych osobowych oraz aby zapobiec jego powtórzeniu. Kopie zapasowe wykonywane do dostarczonej przestrzeni chmurowej oraz ich repliki muszą być przechowywane na terenie Polski. Producent przechowuje dane osobowe klienta (dane osobowe oraz kopie zapasowe) przy użyciu technik szyfrowania, minimum AES-256. Producent nie wykorzystuje danych osobowych klienta bez anonimizacji w środowiskach programistycznych lub testowych. Producent oprogramowania przeprowadza okresowe oceny ryzyka i przeglądy co najmniej raz w roku. Infrastruktura (chmurowy magazyn kopii zapasowych) jest zaprojektowana zgodnie z podejściem N+1 (to, co niezbędne +1). Producent oprogramowania jest zgodny z standardem bezpieczeństwa ISO 27001 lub SOC 2, a magazyn kopii zapasowych musi być zgodny z certyfikatami ISO 9001,

	ISO 27001 oraz certyfikację DCOS na minimum 4 poziomie. Przestrzeń chmurowa dostarczana wraz z oprogramowaniem to minimum 50GB w ramach jednej licencji, na cały okres jej trwania.

4.4. Usługi instalacji, konfiguracji oraz wdrożenia - 1 kpl.

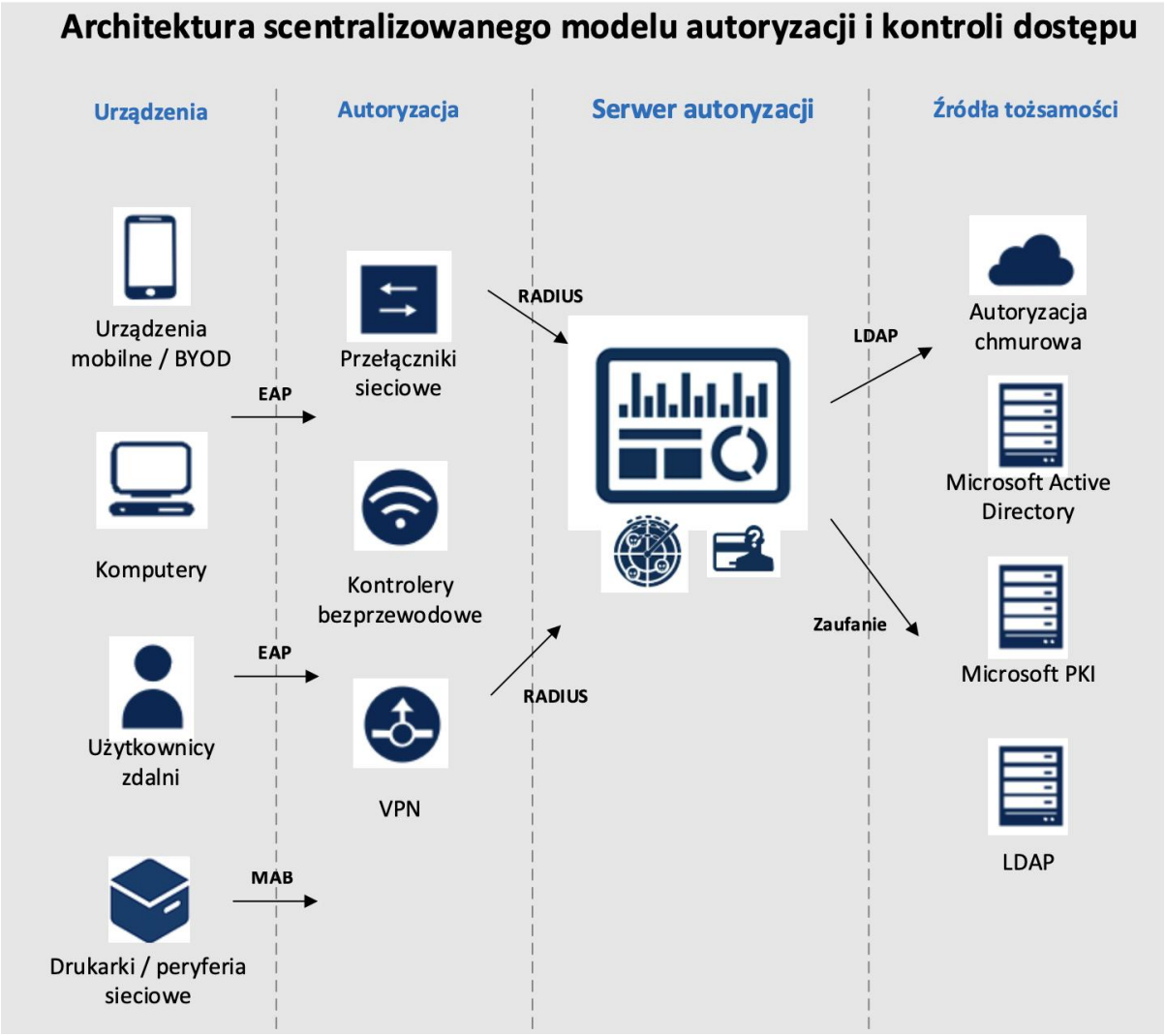
Wykonawca odpowiedzialny jest za opracowanie polityki tworzenia kopii zapasowej, w której opisane zostaną wszystkie zasady, według których będą tworzone kopie zapasowe z wyszczególnieniem kto je wykonuje, kiedy, gdzie przenoszone będą nośniki danych oraz kto będzie odpowiedzialny za poszczególne etapy wykonywania czynności, kto będzie odpowiedzialny za monitoring i weryfikację tworzonych kopii zapasowych.
Zakres wdrożenia:

1) Dostawa serwera oraz niezbędnych licencji oprogramowania do tworzenia kopii zapasowych z wsparciem technicznym oraz dostępem do aktualizacji.
2) Montaż dostarczonych urządzeń oraz ich konfiguracja do pracy w infrastrukturze Zamawiającego, uruchomienie; aktualizacja firmware.
3) Konfiguracja maszyny wirtualnej dla systemu backupu; instalacja serwera/konsoli zarządzającej kopiami zapasowymi:
    a) Opracowanie Harmonogramu tworzenia kopii zapasowych z podziałem na maszyny fizyczne/wirtualne; określeniem: częstotliwości tworzenia kopii pełnych, częstotliwości tworzenia kopii przyrostowych, częstotliwości tworzenia kopii na nośnikach wymiennych, częstotliwości weryfikacji poprawności tworzonych kopii zapasowych, częstotliwości i zakresu przeprowadzania testów odtworzeniowych. Na podstawie Harmonogramu Wykonawca skonfiguruje zadania backupowe na dostarczonym oprogramowaniu. Uruchomi tworzenie kopii zapasowych na serwerze backupowym oraz serwerze NAS, a także w zasobach chmurowych.
    b) Począwszy od dnia uruchomienia tworzenia kopii zapasowych, Wykonawca będzie zobowiązany do monitorowania pracy systemu backupowego przez min. 7 dni. Nadzór będzie miał na celu potwierdzenie prawidłowości wykonywanych kopii na serwerze oraz nośnikach wymiennych; potwierdzenie tworzenia kopii zgodnie z Harmonogramem.
    c) Po zakończeniu pełnego cyklu tygodniowego tworzenia kopii zapasowych zgodnie z Harmonogramem, przeprowadzi testy odtworzenia maszyn wirtualnych. Testy odtworzeniowe będą przeprowadzone przy udziale administratora Zamawiającego.
    d) Po okresie monitorowania, na podstawie potwierdzenia przez Zamawiającego zgodności wykonywanych kopii zgodnie z Harmonogramem oraz na podstawie zakończonych sukcesem testów odtworzeniowych, Wykonawca przeprowadzi instruktaż z zakresu:
    1) bieżącej obsługi systemu, podstaw administracji,
    2) modyfikacji Harmonogramu i zadań backupowych,
    3) czynności sprawdzania prawidłowości wykonywanych kopii zapasowych na serwerze oraz nośnikach wymiennych,
    4) procedury i czynności przeprowadzania testów odtworzeniowych.

5. Wdrożenie Systemu Centralnej Autoryzacji i zarządzania tożsamością

Budowa Centralnego Systemu Autoryzacji obejmuje instalację oraz integrację kilku systemów (AD, MFA, VPN), które powinny tworzyć jednolitą architekturę bezpiecznego uwierzytelniania użytkowników i urządzeń w sieci jednostki. Rozwiązanie powinno zapewnić:

a) Centralną Autentykację i autoryzację z integracją ze środowiskiem Active Directory.
b) Możliwość zastosowania uwierzytelniania dwuskładnikowego MFA (np. SMS, tokeny, aplikacje mobilne) w dostępie zdalnym lub do lokalnych zasobów (usługi, urządzenia).
c) Możliwość zapewnienia profiling'u dla użytkowników przy współpracy z Active Directory.
d) Możliwość tworzenia reguł dostępu opartych na tożsamości użytkowników z AD, ich lokalizacji, ról oraz innych atrybutów (np. dział, grupa, urządzenie).
e) Możliwość zastosowania uwierzytelniania dwuskładnikowego MFA (np. SMS, tokeny, aplikacje mobilne) w dostępie zdalnym lub do lokalnych zasobów (usługi, urządzenia).
f) Możliwość identyfikacji typu urządzeń łączących się z siecią (laptopy, smartfony, drukarki itp.), co pozwoli na stosowanie różnych polityk bezpieczeństwa.
g) Wdrożenie dla wszystkich użytkowników mechanizmu Active Directory na ich komputerach.
h) Narzędzia do prostego zarządzania mechanizmami autoryzacji użytkowników oraz możliwość monitorowania ich aktywności w środowisku informatycznym.



Koncepcyjny schemat systemu przedstawia powyższy rysunek. Podstawą jego funkcjonowania jest źródło tożsamości, stąd konieczność wdrożenia usług Active Directory. Kompleksowe wdrożenie zapewni bezpieczny i kontrolowany dostęp do urządzeń WLAN, LAN, WAN, komputerom, serwerom oraz innym urządzeniom podłączonym do infrastruktury.
Komputery klienckie w sieci powinny muszą zostać podłączone do domeny, najlepiej z zachowaniem ustawień użytkowników.

W ramach zamówienia mają zostać wykonane następujące zadania:

- Wdrożenie Systemu Centralnej Autoryzacji.
- Analiza aktualnego stanu i konfiguracji domeny obejmującej Urzad Gminy.
- Wdrożenie dobrych praktyk w zakresie usług katalogowych wraz z migracją użytkowników i stacji niepodłączonych do domeny.
- Wdrożenie Centrum certyfikacji typu Enterprise.
- Wdrożenie protokołu 802.1x dla przełączników sieciowych oraz urządzeń sieci WLAN.
- Wdrożenie autoryzacji dwuskładnikowej (MFA).

W ramach wdrożenia usług Active Directory (AD), które stanowi podstawę bezpiecznego zarządzania tożsamością oraz kontrolowanego dostępu do urządzeń sieciowych, serwerów oraz stacji roboczych, kluczowym elementem jest zapewnienie, że wszystkie komputery klienckie w infrastrukturze spełniają minimalne wymagania w zakresie wsparcia technicznego i zgodności z systemem Windows Server 2022 lub nowszym.

Koncepcja techniczna systemu.

Budowa systemu obejmuje instalację oraz integrację: AD, MFA, VPN - które powinny tworzyć jednolitą architekturę bezpiecznego uwierzytelniania użytkowników i urządzeń w sieci jednostki. Rozwiązanie powinno zapewnić:

- Autentykację i autoryzację przy integracji ze środowiskiem Active Directory oraz innych mechanizmów jak RADIUS.
- Możliwość zastosowania uwierzytelniania dwuskładnikowego MFA.

Kompleksowe wdrożenie Active Directory zapewni bezpieczny i kontrolowany dostęp do urządzeń WLAN, LAN, WAN, komputerom, serwerom oraz innym urządzeniom podłączonym do infrastruktury.
Komputery klienckie w sieci powinny zostać podłączone do domeny z zachowaniem ustawień użytkowników.

5.1. Serwer Centralnej Autoryzacji - 1 lic.

System powinien zapewniać pełne zarządzanie cyklem życiowym dostępu do zasobów sieciowych, niezależnie od miejsca uzyskiwanego dostępu. System realizuje wsparcie dla dostępu gościnnego w sieci, identyfikację stacji, rejestrację urządzeń. System może obejmować kontrolą dostęp wszystkich urządzeń podłączonych do sieci IP w tym terminali, komputerów PC, smartfonów i tabletów, telefonii IP, terminali video i innych podłączonych urządzeń.
System pracujący w modelu HA zainstalowany w ramach dostarczonej platformy wirtualizacyjnej.

a) System musi posiadać funkcjonalność aktywnego zapobiegania dostępu do sieci nieautoryzowanych użytkowników i urządzeń końcowych.
b) System musi współpracować z urządzeniami wielu producentów (tzw. multi vendor)

c) System musi być w pełni zarządzany z poziomu interfejsu graficznego dostępnego przez przeglądarkę internetową z jednej konsoli, interfejs WEB w wersji HTML5 niewymagających obsługi dodatkowych wtyczek.
d) System musi wspierać funkcjonalność instalacji rozproszonej na wielu maszynach (serwerach) fizycznych lub wirtualnych w ramach jednej licencji.
e) System musi wspierać mechanizm DISASTER RECOVERY – tworzenia kopii lustrzanej całego systemu w celu zachowania ciągłości działania w ramach jednej licencji.
f) System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych stacji końcowych.
g) System musi umożliwiać obsługę co najmniej 200 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do przynajmniej 1 000 jednoczesnych unikatowych autoryzacji do sieci poprzez rozbudowę oferowanego rozwiązania.
h) Licencja ma być zwalniana po rozłączeniu urządzenia końcowego.
i) System musi umożliwiać obsługę jednocześnie podłączonych agentów oraz BYOD (Bring Your Own Device) co najmniej tyle samo co licencja na jednoczesne unikatowe autoryzacje do sieci w ciągu dnia.
j) System musi umożliwiać instalację na maszynie wirtualnej (VM), PaaS lub maszynie fizycznej, w tym:
    - VM – min. VMWare ESXi, Hyper-V, Proxmox, KVM
    - Maszyny fizyczne - serwery wspierane przez producenta.
k) System musi posiadać funkcjonalność serwerów:
    - serwera RADIUS dla infrastruktury sieciowej,
    - serwera OTP dla infrastruktury VPN, Captive Portal, Tacacs+,
    - serwera SYSLOG,
    - serwera TACACS+,
    - serwera Monitoringu,
    - serwera DHCP,
    - serwera polityk uwierzytelniania i kontroli dostępu 802.1X,
    - serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego.
l) System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, poprzez zapewnienie redundancji dla modułów realizujących dostępu do sieci i DHCP.
m) System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC.
n) System musi umożliwiać uwierzytelnianie tożsamości i urządzeń końcowych za pomocą wewnętrznej bazy i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, Google G Suite, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC.
o) System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z zewnętrznych systemów (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc, Microsoft Active Directory, Radius, OpenLDAP, relacyjnych baz danych (jak MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC), CheckPoint, Service Now.
p) Podczas synchronizacji musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenia lokalnych haseł, certyfikatów, wysłania konfiguracji dostępowych poprzez email.
q) System musi wspierać funkcjonalność API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci.

r) System musi mieć możliwość autoryzacji protokołem NTLM z wieloma serwerami Microsoft Active Directory, także nie połączonych relacjami zaufania.
s) System musi mieć możliwość obsługę wielu PKI dla różnych grup użytkowników.
t) System musi posiadać funkcjonalność tworzenia kont administracyjnych z konfigurowalnym dostępem do dowolnych spośród wszystkich funkcjonalności systemu oraz do dowolnych obiektów utworzonych i/lub zarządzanych w systemie.
u) System musi mieć możliwość zmiany parametrów kont Microsoft Active Directory (min. Login, Hasło, Imię, Nazwisko, Email, Status).
v) System musi posiadać funkcjonalność konfiguracji praw kontroli dostępu do poszczególnych elementów menu interfejsu oraz obiektów na poziomie ich dodawania, edycji, kasowania.
w) Interfejs graficzny systemu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim i polskim).
x) System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP lub podsieci.
y) System musi posiadać możliwość raportowania podłączonych tożsamości, urządzeń końcowych podłączonych do sieci, min. Tożsamość, mac adres, urządzenie końcowe, port, SSID, urządzenie sieciowe, informacja o autoryzacji oraz przydzielony Vlan z przydzielonym adresem IP.
z) System musi zapewniać scentralizowane monitorowanie urządzeń sieciowych. W systemie musi być dostępny dedykowany interfejs graficzny, na którym dostępny jest podgląd wszystkich portów i modułów zarządzanego urządzenia.
aa) System musi umożliwiać monitoring urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP.
bb) System musi umożliwiać zbieranie danych inwentaryzacyjnych, ich zmian oraz sprawdzanie kondycji urządzeń sieciowych oraz końcowych za pomocą min. protokołu SNMP.
cc) Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu konfiguracji zmian, konfiguracji ustawień portu z zakresu min. VLANów, Autoryzacji, Statusu, Opisu.
dd) System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej.
ee) System musi posiadać możliwość konfiguracji serwera DHCP dla stworzonych podsieci IP.
ff) System musi umożliwiać konfigurację własnych szablonów przesyłanych wiadomości e-mail oraz wydruku poświadczeń dostępu do sieci.
gg) System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsieciach minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3.
hh) System musi posiadać funkcjonalność wysyłania zdarzeń np. do systemów SIEM minimum protokołem Syslog informacji z serwerów autoryzacji, DHCP, VPN, OTP, Tacacs+.
ii) System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa lokalnie lub na udziałach zewnętrznych.
jj) System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD).
kk) System musi posiadać możliwość logowania w oparciu o portale społecznościowe, minimum: Facebook i Google, LinkedIn.
ll) System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez email, bramkę SMS oraz zapasową bramkę SMS.
mm) System musi posiadać funkcję personalizacji strony gościnnej.

nn) Captive Portal musi się automatycznie dostosować formatem do podłączonego urządzenia końcowego min: komputer, tablet, telefon.
oo) Captive Portal musi umożliwiać rejestracje gości potwierdzanych przez konta typu sponsor.
pp) Captive Portal musi mieć możliwość włączenia dwuskładnikowego uwierzytelniania konta (OTP) minimum za pomocą tokenu wygenerowanego na Google Authenticatorze lub wysłanego przez bramkę SMS oraz zapasową bramkę SMS.
qq) Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory.
rr) Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory.
ss) Captive Portal musi umożliwiać logowanie typu HotSpot za pomocą kodu dostępu.
tt) Captive Portal musi umożliwiać tworzenie dynamicznych pól formularza rejestracyjnego, np.: pole tekstowe, lista wyboru.
uu) Interfejs graficzny Captive Portalu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim, polskim, niemieckim, hiszpańskim, francuskim i ukraińskim).
vv) Captive Portal musi posiadać możliwość pobrania konfiguracji dla OTP.
ww) Captive Portal powinien wspierać automatyczne kasowanie wygasłych kont gościnnych: na żądanie, okresowo wg zadanej liczbie dni.
xx) Captive Portal powinien umożliwiać konfiguracje maksymalnej ilości nieudanych logowań.
yy) System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP.
zz) System powinien posiadać mechanizm integracji z systemami zewnętrznymi za pomocą protokołu, min. Syslog, SNMP Trap, Rest API, w celu wykrywania anomalii, blokowania dostępu do sieci, rozłączania tożsamości/urządzenia końcowego.
aaa) System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny.
bbb) System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z RFC 5176.
ccc) System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych.
ddd) System musi obsługiwać różne metody profilowania do wykrywania typu urządzeniu, systemu operacyjnego, przez co najmniej DHCP Fingerprinting, DHCP SPAN, SNMP, Vendor OUI, TCP, Active Directory, CDP/LLDP, HTTP/S, DNS, Radius, WMI, MDM, WinRM, ONVIF.
eee) System musi umożliwiać integracje z zewnętrznymi rozwiązaniami typu MDM
fff) System musi posiadać funkcjonalność dwuskładnikowego uwierzytelniania konta (OTP) realizowaną poprzez tworzenie tokenu w Google Authenticator i SMS,.
ggg) System musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa co najmniej:

- Czy system jest aktualny z możliwością automatycznego naprawienia niezgodności
- Czy włączony jest firewall
- Czy jest uruchomiony system antywirusowy i aktualna baza sygnatur
- Czy jest włączone szyfrowanie dysku systemowego
- Czy urządzenie końcowe jest podłączone do domeny Microsoft Active Directory
- Czy na dysku znajdują się pliki lub katalogi wskazane przez administratora
- Czy w systemie są uruchomione procesy wskazane przez administratora

- Czy w systemie są uruchomione usługi wskazane przez administratora z możliwością automatycznego naprawienia niezgodności
- Czy w systemie są wpisy w rejestrze wskazane przez administratora wg klucza, a także pod kątem:
  – Wartości klucza rejestru
  – Typu wartości: Number, String, Version

hhh) System musi posiadać możliwość wysyłania komunikatów do użytkowników min za pomocą agenta i Captive Portal.

iii) System musi współpracować z serwerem tokenów.

jjj) System musi posiadać mechanizm autokonfiguracji sieci (autokonfiguratory sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania pracowników działo IT dla systemów co najmniej:

- Microsoft Windows
- Mac OS
- iOS
- Android

kkk) System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfiguratory sieci).

lll) System musi wspierać protokół IPv6 min dla konsoli SSH, komunikacji RADIUS, NTP, SNMP, komunikację z Microsoft Active Directory.

Mechanizmy uwierzytelniania

a) System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS.

b) System musi obsługiwać uwierzytelnianie w oparciu o następujące protokoły:

- MAC,
- PAP/ASCII,
- CHAP,
- SNMP,
- 802.1X.

c) wraz z możliwością wyboru szczegółowego sposobu uwierzytelniania np. IEEE 802.1x (PEAP), IEEE 802.1x (EAP-TLS), IEEE 802.1x (EAP-TTLS), MAC (PAP), MAC (CHAP), MAC (MD5), TEAP, itp.

d) System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości.

e) System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych.

f) System musi wspierać implementację protokołu 802.1X z różnymi suplikantami (min. Windows XP, Windows Vista, Windows 7, Windows 8 i 8.1, Windows 10, Windows 11, Apple Mac OS X Supplicant, Apple iOS Supplicant, Google Android Supplicant, Ubuntu Supplicant).

g) System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły:

- Tożsamość/Urządzenie końcowe,
- Grupa tożsamości/urządzeń końcowych,
- Parametry urządzeń końcowych, min: system operacyjny, wersja,
- Atrybuty Active Directory,
- Jednostka organizacyjna tożsamości/urządzeń końcowych,
- Urządzenia sieciowe sieci przewodowej, bezprzewodowej,
- Grupy urządzeń sieciowych,
- Porty urządzeń sieciowych,
- Grupy portów urządzeń sieciowych,
- Jednostka organizacyjna portów,
- Punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID),
- Data, czas ważności polityki,

- Wewnętrzny Captive Portal,
- Metoda autoryzacji.

h) System musi umożliwiać przypisywanie sieci VLAN i/lub atrybutów RADIUS zwrotnych VSA podczas etapu autoryzacji, np.: ACL, Quality of Service, co najmniej następujących producentów: Cisco Networks, Aruba Networks, Extreme Networks, Hewlett Packard Enterprise, Juniper Networks, Ruckus Networks, MicroTik, Ubiquiti Networks.
i) System musi wspierać funkcjonalność *IP-to-ID Mapping*, polegającą na łączeniu tożsamości, adresu IP, adresu MAC.
j) System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu tożsamości, urządzenia końcowego, adresu MAC podczas etapu autoryzacji, minimum za pomocą mechanizmów SNMP, DHCP, NMAP, WMI.
k) System musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej konsoli.
l) System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV.
m) System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o pojedynczy obiekt i/lub w postaci zbiorczego pliku w formacie CSV.
n) System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach.
o) System musi umożliwiać tworzenie hasła dnia, dla tożsamości zarejestrowanych przez wewnętrzny Captive portal.
p) System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o urządzenie końcowe i/lub w postaci zbiorczego pliku w formacie CSV. Lokalna baza urządzeń końcowych musi być tworzona per urządzenie końcowe na podstawie unikalnego adresu MAC.
q) System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów MAC.
r) System musi wspierać funkcjonalność różnych typów autoryzacji na pojedynczym porcie urządzenia sieciowego: min. autoryzację pojedynczą, autoryzację wielokrotną, uwierzytelnianie urządzeń typu Voice VLAN, równoczesną obsługę różnych typów autoryzacji skonfigurowanych na porcie i/lub autoryzację poprzez portal www.
s) System musi umożliwiać integrację z EDUROAM w zakresie autoryzacji użytkowników.
t) System musi umożliwiać przesyłanie zwrotnych parametrów do systemów zewnętrznych i/lub urządzeń sieciowych za pomocą protokołu min. HTTP zawierających min. informacje o identyfikatorze tożsamości, adresie MAC oraz IP.

Obsługa serwerów certyfikatów CA

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

Obsługa serwerów DHCP

1) System musi posiadać funkcję zintegrowanego serwera DHCP.

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

Obsługa serwerów TACACS+

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

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

Raportowanie i monitoring

System musi umożliwiać generowanie raportów oraz monitoring przynajmniej następujących parametrów:

1) Monitoring autoryzacji.
2) Monitoring dla zdarzeń systemowych.
3) Monitoring dla zdarzeń DHCP.
4) Monitoring dla tożsamości.
5) Monitoring dla urządzeń końcowych.
6) Monitoring dla urządzeń sieciowych.
7) Raport stanu systemu (min. szczegółowy dane z nodów systemu, wykorzystanie polityk dostępu, ostatnie krytyczne błędy, niski status komponentów drukarek, ostanie aktywności serwerów autoryzacji, DHCP, urządzeń sieciowych uwzględniający ostatnią aktywność autoryzacji, obciążenie procesora, pamięci, zmiany konfiguracji, obciążenie serwera DHCP, autoryzacji, obciążenia portów – przepustowość, liczby autoryzacji) dostępny min. z poziomu konsoli CLI, interfejsu WWW oraz raportu email.
8) Raport ze zdarzeń logowania z informacją o nadam adresie IP.
9) Raport stanu systemu z poziomu konsoli CLI min. obciążenie procesora, pamięci, przestrzeni dyskowej, działania usług.
10) Raport z logów DHCP z informacją o polityce dostępu logowania do sieci.

11) System musi posiadać mechanizm graficznego podglądu stanu przełącznika i portów w czasie rzeczywistym.
12) System musi wspierać mechanizm graficznego podglądu urządzeń sieciowych działających w stosie.
13) System musi wspierać mechanizm graficznego podglądu wykrytych niezgodności vlanów w urządzeniach sieciowych działających w środowisku.
14) System musi wpierać funkcjonalność graficznego monitoringu zasobów zarządzanych drukarek sieciowych.
15) System musi posiadać mechanizm graficznego podglądu stanu tożsamości oraz urządzeń końcowych w tym podstawowe dane, ostatnia autoryzacja do sieci, wykorzystanie urządzeń końcowych wg tożsamości na dzień, parametry urządzeń końcowych, min: system operacyjny, wersja.
16) System musi umożliwiać podgląd tożsamości, urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych, kontrolerów wifi.
17) Raport z logów OTP z informacją o poprawnej i błędnej autoryzacji, wysłanego tokenu przez bramkę SMS.
18) Raport zdarzeń Microsoft Active Directory, minimum:
    - Logowania, wylogowania z system w tym błędne logowania
    - Logowania do sieci 802.1X

Alarmy

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

Licencja wsparcia technicznego producenta oprogramowania:

Wykonawca dostarczy wraz dożywotnią licencją systemu NAC – 24 miesięczną licencje na wsparcie
producenta oprogramowania. Licencja ta powinna obejmować minimum:

- Kontakt mailowy z działem wsparcia technicznego w celu rozwiązania problemów związanych z wdrożeniem lub obsługą systemu NAC
- Rozwiązywanie powtarzalnych i rozwiązywalnych problemów związanych z oprogramowaniem a także wsparcie przy identyfikacji problemów trudnych do powtórzenia.

- Wsparcie przy rozwiązywaniu problemów oraz pomoc w określaniu parametrów dla konfiguracji oprogramowania oraz wstępne obejścia dla wykrytych problemów.
- Dostęp do dokumentacji i instrukcji na stronie internetowej.
- Dostęp do aktualizacji i poprawek, które powinny być dostępne z poziomu interfejsu oprogramowania.

5.2. Licencje dostępowe do Serwera Centralnej Autoryzacji – 100 lic.

Wymagana jest dostawa licencji uprawniającej zgodnie z zasadami licencjonowania producenta systemu centralnej autoryzacji w pkt. 5.2 do legalnego korzystania z zasobów serwerów przez min. 100 urzadzeń jednocześnie.

5.3. Licencje systemu MFA – 4 lic.

W ramach licencji wieczystej lub subskrypcji oprogramowania na okres nie krótszy niż 24 miesiące, oprogramowanie musi być kompatybilne z oprogramowaniem EDR/XDR.

Minimalne wymagania licencji (4 szt.):

Ochrona poprzez dwuskładnikowe uwierzytelnianie

- Wsparcie dla systemów z rodziny Microsoft Windows Server: 2008 / 2008 R2 / 2012 / 2012 R2 / SBS 2008 / SBS 2011 / 2012 Essentials / 2012 R2 Essentials / Windows Server 2016 / Windows Server 2016 Essentials / Windows Server 2019 / Windows Server 2019 Essentials.
- Rozwiązanie musi wspierać integrację z Microsoft Dynamics CRM 2011 / 2013 / 2015 / 2016.
- Rozwiązanie musi wspierać integrację z Microsoft Sharepoint 2010 / 2013 / 2016 /2019.
- Rozwiązanie musi wspierać integrację z Microsoft Remote Desktop Web Access.
- Rozwiązanie musi wspierać integrację z Microsoft Terminal Services Web Access.
- Rozwiązanie musi integrację z Microsoft Remote Web Access.
- Rozwiązanie musi posiadać wbudowany serwer RADIUS umożliwiający uwierzytelnianie użytkowników dla rozwiązań VPN, które wspierają technologię RADIUS.

Aplikacja mobilna

- Aplikacja mobilna musi wspierać telefony działające pod kontrolą systemów mobilnych: Android (w wersji 4.1 lub wyższej), iOS (9 lub wyższej), Windows Phone 8.1, Windows Mobile 10.
- Aplikacja mobilna do generowania OTP (jednorazowego hasła) musi być dostarczona przez producenta rozwiązania w ramach zakupionej licencji.
- Użytkownik musi mieć możliwość dodatkowego zabezpieczenia aplikacji w postaci kodu PIN.
- Aplikacja do działania nie może wymagać od użytkownika aktywnego połączenia z Internetem – generowanie OTP (jednorazowego hasła) musi odbywać się w trybie offline.
- Dwuskładnikowe uwierzytelnienie musi być możliwe również przy użyciu jednorazowych haseł SMS.
- Aplikacja zainstalowana na urządzeniach mobilnych musi umożliwiać generowanie OTP dla więcej niż jednego serwera uwierzytelniającego.
- Wsparcie techniczne do programu świadczone w języku polskim, przez polskiego dystrybutora autoryzowanego przez producenta program.u

5.4. Usługi instalacji, konfiguracji oraz wdrożenia.

W ramach zamówienia mają zostać wykonane następujące zadania:

- Wdrożenie usług katalogowych wraz z migracją użytkowników sieci do domeny.
- Wdrożenie Centrum certyfikacji typu Enterprise.
- Wdrożenie Systemu Centralnej Autoryzacji (integracja z domeną).
- Wdrożenie zasad GPO i dystrybucja podstawowego oprogramowania.
- Integracja dostarczanych i istniejących urządzeń sieciowych (switche, AP itp.) z Systemem NAC, w ramach funkcjonalności dostępnych na urządzeniach.
- Wdrożenie protokołu 802.1x dla przełączników sieciowych oraz urządzeń sieci WLAN.
- Wdrożenie autoryzacji dwuskładnikowej (MFA) w zakresie dostępu VPN.

6. Dostawa i wdrożenie kompleksowego rozwiązania do monitorowania bezpieczeństwa EDR/XDR, szkolenie.

6.1. Oprogramowanie EDR/XDR – 26 lic.

W ramach licencji wieczystej lub subskrypcji oprogramowania na okres nie krótszy niż 24 miesiące oprogramowanie musi spełniać następujące wymagania:

Administracja zdalna w chmurze:

1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania Antywirusowego.
2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.
4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawieunikatowego identyfikatora sprzętowego stacji.
5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

Ochrona stacji roboczych:

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
2. Rozwiązanie musi wspierać architekturę ARM64.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
10. Rozwiązanie musi integrować się z Intel Threat Detection Technology.
11. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
13. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
14. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
15. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    - tryb automatyczny z regułami, gdzie program automatycznie tworzy i
    - wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych
    - przez użytkownika,
    - tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w
    - przypadku wykrycia aktywności w systemie,
    - tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone
    - przez użytkownika,
    - tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i
    - użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez
    - użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie
    - przełączyć się w tryb pracy oparty na regułach,
    - tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o
    - szczególnie podejrzanych zdarzeniach.
17. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych

aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.

18. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
19. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
23. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:
    - tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
    - tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
    - tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i
    - wychodzący, zezwalając tylko na połączenia skonfigurowane przez
    - administratora,
    - tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
24. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
25. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
26. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
27. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
28. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
29. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
30. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

Ochrona serwera

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

Dodatkowe wymagania dla ochrony serwerów Windows:

9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
13. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
14. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

Dodatkowe wymagania dla ochrony serwerów Linux:

18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
20. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
21. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów.
22. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

Szyfrowanie

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10 i Microsoft Windows 11.
2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

Ochrona urządzeń mobilnych opartych o system Android

1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.
5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
   - usunięcie zawartości urządzenia,
   - przywrócenie urządzenie do ustawień fabrycznych,
   - zablokowania urządzenia,
   - uruchomienie sygnału dźwiękowego,
   - lokalizację GPS.
6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
   - nazwę aplikacji,
   - nazwę pakietu,
   - kategorię sklepu Google Play,
   - uprawnienia aplikacji,
   - pochodzenie aplikacji z nieznanego źródła.

Ochrona serwera pocztowego MS Exchange

1. Rozwiązanie musi wspierać instalację na systemach Microsoft Windows Server 2012 i nowszych.
2. Rozwiązanie musi zapewniać wsparcie dla systemów poczty Microsoft Exchange 2010/2013/2016/2019.
3. Rozwiązanie musi zapewniać wsparcie dla ról Mailbox, Edge, Hub.
4. Rozwiązanie musi skanować pocztę przychodzącą i wychodzącą na serwerze MS Exchange.
5. Rozwiązanie musi zapewnić skanowanie bezpośrednio w bazach danych Exchange przy pomocy VSAPI.
6. Rozwiązanie musi mieć możliwość tworzenia różnych reguł blokowania wiadomości w tym co najmniej po zdefiniowanym nadawcy, odbiorcy, temacie wiadomości, typie załącznika, rozmiarze załącznika, rozmiarze wiadomości, nagłówku wiadomości, na podstawie uzyskanego wyniku skanowania antyspamowego i antywirusowego, godzinie odbioru, obecności załącznika chronionego hasłem lub uszkodzonego archiwum.
7. Rozwiązanie musi posiadać wbudowany w oprogramowanie filtr antyspamowy odpowiedzialny za filtrowanie niechcianej poczty.
8. System antyspamowy ma być wyposażony przynajmniej w możliwość sprawdzania list RBL, DNSBL oraz mechanizm reputacji poczty.
9. Administrator musi mieć możliwość dodania własnych adresów list RBL oraz DSBL, z których będzie korzystać aplikacja.
10. Rozwiązanie ma posiadać mechanizm greylisting (szara lista).
11. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.

Sandbox w chmurze

1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.

2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.
3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
7. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów.
8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo.
12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:
    - Czysty,
    - Podejrzany,
    - Bardzo podejrzany,
    - Szkodliwy.
13. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

Ochrona usługi Microsoft 365

1. Rozwiązanie musi obejmować ochroną usługi Microsoft, takie jak Exchange Online, Onedrive, Sharepoint oraz aplikację Teams.
2. Rozwiązanie musi posiadać możliwość dodania kilku tenantów usługi Micosoft 365.
3. Administrator musi mieć możliwość wskazania, które konto użytkownika będzie objęte ochroną.
4. Rozwiązanie musi być zarządzane za pomocą dowolnej przeglądarki internetowej z dowolnego miejsca w sieci.
5. Rozwiązanie musi być dostępny w języku polskim.
6. Konsola rozwiązania musi posiadać możliwość raportowania co najmniej:
    - użytkowników, otrzymujących najwięcej spamu,
    - użytkowników, otrzymujących najwięcej wiadomości typu „phishing”,
    - użytkowników, otrzymujących największą ilość szkodliwego oprogramowania,
    - kont użytkowników, które mogę być podejrzane.
7. Konsola rozwiązania musi posiadać funkcjonalność logowania zdarzeń z podziałem na dzienniki dla Exchange Online i Onedrive.

8. Dzienniki Exchange Online muszą posiadać funkcjonalność informowania co najmniej:
    - jaka ilość wiadomości została przeskanowania,
    - wynik skanowania poszczególnej wiadomości,
    - czynność podjęta przez rozwiązanie.
9. Dzienniki Onedrive muszą posiadać funkcjonalność informowania co najmniej o:
    - zagrożeniach, które zostały wykryte,
    - na jakim koncie zostały wykryte,
    - jakie zagrożenie zostało wykryte,
    - podjętą czynność.
10. Rozwiązanie musi posiadać funkcjonalność kwarantanny, do której będą przenoszone zainfekowane obiekty z usługi Exchange Online oraz Onedrive.
11. Musi istnieć możliwość pobrania plików z kwarantanny w formie oryginalnego pliku i pliku zabezpieczonego hasłem.
12. Administrator musi posiadać możliwość przypisania konfiguracji, do dodanych do rozwiązania tenantów lub do poszczególnych grup i użytkowników.
13. Administrator musi posiadać możliwość konfiguracji rozwiązania w oparciu o co najmniej:
    - wykorzystania do analizy mechanizmów chmurowych, tego samego producenta,
    - wprowadzenia białych i czarnych list adresów ochrony Exchange'a Online,
    - dodania znacznika do tematu wiadomości zakwalifikowanej jako SPAM i phishing.
14. Rozwiązanie musi zapewniać funkcję ochrony przed zagrożeniami 0-day.
15. Funkcja ochrony przed zagrożeniami 0-day musi wykorzystywać do działania chmurę producenta.
16. Funkcja ochrony przed zagrożeniami 0-day musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
17. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
18. Rozwiązanie musi posiadać możliwość przesyłania powiadomień e-mail z funkcją wyboru preferowanego języka.

Moduł XDR

1. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
2. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
3. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
4. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
5. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica".
6. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.
7. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
8. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.
9. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.

10. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.
11. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.
12. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia.
13. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
14. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
15. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.
16. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.
17. Konsola administracyjna musi mieć możliwość tagowania obiektów.
18. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.

Moduł zarządzania podatnościami i aktualizacjami

1. Rozwiązanie musi mieć możliwości wykrywania podatności w systemach operacyjnych (co najmniej Windows 10, Windows 11) oraz aplikacjach zainstalowanych na zarządzanych stacjach.
2. Baza wykrywanych podatności musi zawierać minimum 35000 CVE.
3. Rozwiązanie nie może wymagać instalacji dodatkowej konsoli, ani innych dodatkowych komponentów na stacjach końcowych.
4. Automatyczne wykrywanie podatności musi wykonywać się zgodnie z harmonogramem, nie częściej niż raz dziennie.
5. Moduł wykrywania podatności musi umożliwiać wyświetlanie szczegółów danej podatności zawierające minimum:
    - nazwę aplikacji lub systemu operacyjnego,
    - punktację CVS, S
    - opis wykrytej podatności,
    - wartość ryzyka oceniona przez wewnętrzne mechanizmy producenta.
6. Moduł wykrywania podatności musi wykrywać podatności w minimum 700 aplikacjach.
7. Moduł zarządzania aktualizacjami musi umożliwiać wykonanie automatycznej aktualizacji dla minimum 150 popularnych aplikacji.
8. Moduł zarządzania aktualizacjami musi umożliwiać stworzenie białej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje będą aplikowane

tylko i wyłącznie dla wskazanych aplikacji w białej liście. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.

9. Moduł zarządzania aktualizacjami musi umożliwiać stworzenie czarnej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje oprogramowania będą realizowane dla wszystkich - ponad 150 aplikacji, oprócz aplikacji wskazanych na czarnej liście. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.
10. Zarządzanie aktualizacjami aplikacji musi umożliwiać ręczne wdrażanie poprawek na wybranych stacjach.
11. Moduł zarządzania aktualizacjami oraz wykrywania podatności musi być zintegrowany bezpośrednio z programem antywirusowym tego samego producenta zainstalowanym na zarządzanym komputerze.
12. Stacja robocza posiadająca włączony moduł wykrywania podatności oraz zarządzania aktualizacjami musi być w odpowiedni sposób oznaczona w konsoli centralnego zarządzania.
13. Administrator konsoli musi mieć możliwość włączenia modułu wykrywania podatności i zarządzania aktualizacjami przy pomocy menu kontekstowego dostępnego w konsoli centralnego zarządzania.
14. Moduł wykrywania podatności ma umożliwiać wyłączenie powiadomień dla wybranej podatności.

Ochrona poprzez dwuskładnikowe uwierzytelnianie

1. Rozwiązanie musi wspierać systemy operacyjne Microsoft Windows Server: 2008 / 2008 R2 / 2012 / 2012 R2 / SBS 2008 / SBS 2011 / 2012 Essentials / 2012 R2 Essentials / Windows Server 2016 / Windows Server 2016 Essentials / Windows Server 2019 / Windows Server 2019 Essentials / Windows Server 2022.
2. Rozwiązanie musi wspierać system operacyjne Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / Windows 11.
3. Rozwiązanie musi wspierać architekturę 32 i 64-bitową systemu Windows.
4. Oprogramowanie musi wspierać integrację z Microsoft Exchange 2007 / 2010 / 2013 / 2016 / 2019.
5. Oprogramowanie musi wspierać integrację z Microsoft Dynamics CRM 2011 / 2013 / 2015 / 2016.
6. Oprogramowanie musi wspierać integrację z Microsoft Sharepoint 2010 / 2013 / 2016 / 2019.
7. Oprogramowanie musi wspierać integrację z Microsoft Remote Desktop Web Access.
8. Oprogramowanie musi wspierać integrację z Microsoft Terminal Services Web Access.
9. Oprogramowanie musi wspierać integrację z Microsoft Remote Web Access.
10. Rozwiązanie musi posiadać wbudowany serwer RADIUS umożliwiający uwierzytelnianie użytkowników dla rozwiązań VPN, które wspierają protokół RADIUS.
11. Aplikacja mobilna musi wspierać telefony działające pod kontrolą systemów mobilnych: Android (w wersji 4.4 lub wyższej), iOS (12 lub wyższej).
12. Aplikacja mobilna do generowania OTP (jednorazowego hasła) musi być dostarczona przez producenta rozwiązania w ramach zakupionej licencji.
13. Użytkownik musi mieć możliwość dodatkowego zabezpieczenia aplikacji w postaci kodu PIN.
14. Aplikacja do działania nie może wymagać od użytkownika aktywnego połączenia z Internetem – generowanie OTP (jednorazowego hasła) musi odbywać się w trybie offline.
15. Dwuskładnikowe uwierzytelnienie musi być możliwe również przy użyciu jednorazowych haseł SMS.

16. Aplikacja zainstalowana na urządzeniach mobilnych musi umożliwiać generowanie OTP dla więcej niż jednego serwera uwierzytelniającego
17. Wsparcie techniczne do programu świadczone w języku polskim, przez polskiego dystrybutora autoryzowanego przez producenta programu.

6.2. Usługi instalacji, konfiguracji oraz wdrożenia.

W ramach postępowania należy przeprowadzić kompleksowe wdrożenie systemu XDR obejmujące stacje robocze Zamawiającego w zakresie:

- analiza potrzeb Zamawiającego w zakresie ochrony i wykrywania zagrożeń oraz opracowanie planu wdrożenia,
- przygotowanie założeń architektury środowiska centralnego zarządzania (w chmurze),
- instalacja oprogramowania na stacjach końcowych (testy oraz wdrożenie docelowe,)
- ustawienie polityk bezpieczeństwa, grup zarządzania i integracji z innymi systemami w infrastrukturze,
- wdrożenie zaawansowanych modułów analityki i wykrywania zagrożeń,
- przeprowadzenie testów funkcjonalnych i wydajnościowych, w tym symulacja ataków, oraz optymalizacja konfiguracji na podstawie wyników.

6.3. Organizacja i przeprowadzenie autoryzowanego szkolenia z narzędzia EDR/XDR.

Przedmiotem zamówienia jest organizacja i przeprowadzenie szkolenia z narzędzia Extended Detection & Response (XDR) dla pracowników Zamawiającego. Szkolenia muszą być prowadzone w formie zdalnej, w dni robocze. Czas trwania min.1 dzień. Zamawiający dopuszcza również dostarczenie voucherów na szkolenia dla min. 1 osoby.
Szkolenie ma na celu zwiększenie kompetencji uczestników w zakresie wykrywania i reagowania na zagrożenia w sieci oraz skutecznej ochrony przed cyberatakami:

1. Szkolenie musi zostać przeprowadzone przez autoryzowane centrum szkoleniowe producenta rozwiązania.
2. Wykonawca powinien dostarczyć dokument potwierdzający autoryzację producenta przed rozpoczęciem szkolenia.
3. Wykonawca powinien mieć doświadczenie w prowadzeniu szkoleń z zakresu cyberbezpieczeństwa i narzędzi XDR.

Zakres szkolenia powinien obejmować poniższe tematy:

- Diagnostyka nietypowych zachowań i naruszeń w sieci firmowej.
- Reagowanie na wykryte incydenty oraz ocena ich ryzyka.
- Podejmowanie działań zaradczych w przypadku naruszeń bezpieczeństwa.
- Wykrywanie zagrożeń APT.
- Identyfikacja unikatowych plików w sieci.
- Monitorowanie aktywności aplikacji.
- Przeprowadzanie analizy powłamaniowej.
- Ochrona przed atakami ransomware.
- Blokowanie uruchamiania niepożądanych plików w sieci.

7. Podniesienie poziomu bezpieczeństwa danych poprzez wdrożenie polityki backupu

Wykonawca odpowiedzialny jest za opracowanie oraz implementację polityki tworzenia kopii zapasowej, w której opisane zostaną wszystkie zasady, według których będą tworzone kopie zapasowe z wyszczególnieniem kto je wykonuje, kiedy, gdzie przenoszone będą nośniki danych oraz kto będzie odpowiedzialny za poszczególne etapy wykonywania czynności, kto będzie odpowiedzialny za monitoring i weryfikację tworzonych kopii zapasowych.
Zakres wdrożenia:

a) Dostawa serwera wirtualizacji oraz niezbędnych licencji oprogramowania do tworzenia kopii zapasowych z wsparciem technicznym oraz dostępem do aktualizacji.
b) Montaż serwera, konfiguracja serwera do pracy w infrastrukturze Zamawiającego, uruchomienie; aktualizacja firmware serwerów; konfiguracja maszyny wirtualnej dla systemu backupu; instalacja serwera/konsoli zarządzającej kopiami zapasowymi.
c) Opracowanie Harmonogramu tworzenia kopii zapasowych z podziałem na maszyny fizyczne/wirtualne; określeniem: częstotliwości tworzenia kopii pełnych, częstotliwości tworzenia kopii przyrostowych, częstotliwości tworzenia kopii na nośnikach wymiennych, częstotliwości weryfikacji poprawności tworzonych kopii zapasowych, częstotliwości i zakresu przeprowadzania testów odtworzeniowych. Na podstawie Harmonogramu Wykonawca skonfiguruje zadania backupowe na dostarczonym oprogramowaniu. Uruchomi tworzenie kopii zapasowych na serwerze backupowym oraz serwerze NAS, a także w zasobach chmurowych.
d) Począwszy od dnia uruchomienia tworzenia kopii zapasowych, Wykonawca będzie zobowiązany do monitorowania pracy systemu backupowego przez min. 7 dni. Nadzór będzie miał na celu potwierdzenie prawidłowości wykonywanych kopii na serwerze oraz nośnikach wymiennych; potwierdzenie tworzenia kopii zgodnie z Harmonogramem.
e) Po zakończeniu pełnego cyklu tygodniowego tworzenia kopii zapasowych zgodnie z Harmonogramem, przeprowadzi testy odtworzenia maszyn wirtualnych. Testy odtworzeniowe będą przeprowadzone przy udziale administratora Zamawiającego.
f) Po okresie monitorowania, na podstawie potwierdzenia przez Zamawiającego zgodności wykonywanych kopii zgodnie z Harmonogramem oraz na podstawie zakończonych sukcesem testów odtworzeniowych, Wykonawca przeprowadzi instruktaż z zakresu:
    - bieżącej obsługi systemu, podstaw administracji,
    - modyfikacji Harmonogramu i zadań backupowych,
    - czynności sprawdzania prawidłowości wykonywanych kopii zapasowych na serwerze oraz nośnikach wymiennych,
    - procedury i czynności przeprowadzania testów odtworzeniowych.

8. Dostawa, instalacja oraz uruchomienie UPSów

Zamówienie obejmuje dostawę, instalację i uruchomienie ups-a sewerowego oraz zasilaczy awaryjnych dla wskazanych przez Zamawiającego stanowisk komputerowych.

8.1. UPS serwerowy RACK– 1 szt.

UPS do szafy Rack 3kVA/3kW 1f/1f 2U + moduł bateryjny 19” 2U.

Moc	3kW
Napięcie zasilające	L+N+PE 230V AC
Tolerancja napięcia	110 – 300V AC
Częstotliwość	50 / 60 Hz (autowykrywanie)

Tolerancja częstotliwości	40 – 70
Wejściowy współczynnik mocy	>0,99
THDi	< 5%
Power factor	1
THDu	< 1%
Przeciążalność	<= 150% (30s)
Gniazda wyjściowe	8xIEC C13, 1xIEC C19
Start z baterii	Tak
Ilość baterii w obudowie	6 szt.
Max prąd ładowania	1,5 – 8A
Poziom hałasu	<50dB
Głębokość	<=600mm
Wysokość	Max 2U
Zewnętrzny moduł bateryjny 2U	1
Czas autonomii	20 min (3kW)
Szyny montażowe rack	W zestawie
Karta SNMP	tak

8.2. UPS stanowiskowy 1000 VA – 3 szt.

Moc pozorna	1000 VA
Moc czynna	550 W
Architektura UPS-a	line-interactive
Kształt napięcia wyjściowego	Modyfikowana sinusoida
Liczba faz na wejściu	1 (230V)
Czas transferu (maks.)	4 ms
Czas ładowania	8 h
Typ obudowy	Tower
Zabezpieczenia / filtry	• Przeciwprzeciążeniowe • Przeciwprzepięciowe • Przeciwzakłóceniowe
Porty zasilania we.	IEC-C14
Porty zasilania wy.	4 x typ C/E
Gniazda we/wy	• 1 x USB (Type B) • 1 x RS-232 (COM) • 2 x RJ-11/RJ-45
Wymagania środowiskowe	• Temperatura robocza: 0 ~ 40 (°C) • Względna wilgotność robocza (bez kondensacji): 0 ~ 90 (%) • Wysokość robocza: 0-10 000 stóp (0-3000 metrów) (stopy/metry) • Temperatura przechowywania: -4 ~ 122 (°F) • Temperatura przechowywania: -20 ~ 50 (°C) • Względna wilgotność przechowywania (bez kondensacji): 0 ~ 90 (%) • Wysokość przechowywaniau: 0-10 000 stóp (0-3000 metrów) (stopy/metry) • Rozproszenie ciepła online: 23,9 (BTU/hr)

	• Słyszalny hałas od 1,0 M z powierzchni urządzenia: 40 (dBA)
Akcesoria w zestawie	• VP1000ELCD-FR UPS • Przewód USB • Instrukcja obsługi • Karta rejestracji produktu
Kolor	Czarny
Wymiary	100 x 227 x 260 mm
Moc pozorna	1000 VA
Moc czynna	550 W

III. WARUNKI URUCHOMIENIA I ODBIORU WDROŻONYCH ROZWIĄZAŃ ORAZ PRZEKAZANIA DO EKSPLOATACJI

Pozostałe wymagania od Wykonawcy.

1. Poza dostawami i usługami odstawowymi, wykonawca jest zobowiązany do skalkulowania wszelkich usług pomocniczych, jakie uzna za niezbędne do prawidłowego wykonania przedmiotu zamówienia dla przyjętej technologii uwzględniając warunki ich wykonania.
2. Wykonawca powinien ponadto uwzględnić w cenie w ramach kosztów dodatkowych:
   - koszty dostawy sprzętu na miejsce instalacji,
   - koszty zabezpieczenia istniejących elementów obiektu oraz wyposażenia (urządzeń) Użytkownika przed ich zniszczeniem w trakcie wykonywania prac,
   - koszty związane z zorganizowaniem pracy w sposób minimalizujący zakłócenie prowadzenia bieżącej działalności Zamawiającego,
   - koszty zapewnienia bezpieczeństwa bhp i ppoż. w trakcie realizacji prac,
   - koszty testów, prób, badań, odbiorów technicznych – jeśli będą wymagane,
   - koszty opracowania dokumentacji powykonawczej,
   - koszty uporządkowania oraz przywrócenia obiektu po wykonanych robotach do stanu pierwotnego wraz z naprawą ewentualnych szkód użytkownikowi lub osobom trzecim.
3. Wykonawca zobowiązany jest do:
   - dokonywania z Zamawiającym wszelkich koniecznych ustaleń mogących wpływać na zakres i sposób realizacji Przedmiotu Zamówienia oraz ciągła współpraca z Zamawiającym na każdym etapie realizacji.
   - Stosowanie się do wytycznych i polityk bezpieczeństwa informacji obowiązujących u Zamawiającego.
   - Udzielania na każde żądanie Zamawiającego pełnej informacji na temat stanu realizacji Przedmiotu Zamówienia.

Uwaga!

1) Dostarczone rozwiązania teleinformatyczne, ze szczególnym uwzględnieniem dostarczanego i wdrażanego Oprogramowania, muszą być zgodne z powszechnie obowiązującymi przepisami prawa polskiego i europejskiego. Rozwiązania muszą pozwalać na gromadzenie, przetwarzanie i analizowanie danych i informacji w obszarach objętych wdrożeniem.

- Podmioty realizujące zadania publiczne zobowiązane są do stosowania rozwiązań z zakresu interoperacyjności mi. na poziomie technologicznym. Interoperacyjność osiąga się poprzez stosowania minimalnych wymagań dla systemów teleinformatycznych. Zgodnie z §20 ust. 2 pkt. 12 Rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności (KRI) zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych polega mi. na:
  - zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa,
  - redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
  - zapewnienia bezpieczeństwa plików,
  - dbałość o aktualizację oprogramowania.

Dodatkowym ważnym elementem systemu jest możliwość rejestrowania i przechowywania zapisów w dziennikach systemowych (logowanie zdarzeń).

Konieczność zapewnienia tej funkcjonalności wynika z:

§21 ust. 1 KRI (zapewnienie rozliczalności w systemach teleinformatycznych w postaci elektronicznej),

Art. 22 i 23 Ustawy z dnia 5 lipca 2018 o Krajowym Systemie Cyberbezpieczeństwa.

Wdrożone rozwiązania powinny spełniając wymagania przywołanych aktów prawnych oraz standardów rynkowych.

Przeszkolenie dla przedstawicieli Zamawiającego.

Niezależnie od szkoleń specjalistycznych Wykonawca jest zobowiązany do przeszkolenia przedstawicieli Zamawiającego z wdrożonych w ramach projektu systemów i rozwiązań. Szkolenie powinno być przeprowadzone w formie prezentacji z możliwością zalogowania się na konsole urządzeń w trybie do odczytu z możliwością analizy dokonanej konfiguracji i włączenia mechanizmów monitorowania. Przeszkolenie powinno być ukierunkowane na wskazanie roli i funkcji danego elementu systemu w kontekście podniesienia odporności i możliwości zapobiegania incydentom (funkcji podniesienia poziomu cyberbezpieczeństwa). Powinno również obejmować ogólne zasady zarządzania i monitorowania urządzeń.

- Przeszkolenie dla przedstawicieli zamawiającego (maksymalnie 3 osoby).
- Forma: zdalne lub stacjonarne (do ustalenia z Zamawiającym).
- Czas trwania: min. 6 godzin szkoleniowych.
- Materiały szkoleniowe – nie będą wymagane.

Odbiór końcowy

Odbiór końcowy Przedmiotu Zamówienia ma na celu potwierdzenie wykonania wszystkich zadań wynikających z Umowy oraz dostarczenia wymaganej zamówieniem Dokumentacji. Odbiory będą odbywać się zgodnie z zapisami w Umowie na realizację zamówienia. Przed przystąpieniem do odbioru końcowego Wykonawca przygotuje następujące dokumenty:

- Protokoły z pomiarów i testów – jeśli dotyczy.
- Odpowiednie atesty i certyfikaty - jeśli są wymagane.
- Instrukcje obsługi, dokumentacje i inne dokumenty dostarczane wraz ze sprzętem, przez producenta.
- Protokoły odbiorów częściowych.