Szacowanie wartości zamówienia

SIWZ - Specyfikacja Istotnych Warunków Zamówienia / OPZ – Opisz przedmiotu zamówienia

1. Gmina Istebna, Istebna 1000, 43-470 Istebna, NIP: 5482676134, zaprasza do składania ofert cenowych w ramach **szacowanie wartości zamówienia** na: **Dostawa sprzętu i innych rozwiązań cyberbezpieczeństwa dla Gminy Istebna w ramach projektu pn. „Wzmocnienie poziomu cyberbezpieczeństwa w gminie Istebna” w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd” o numerze FERC.02.02-CS.01-001/23”.**

   Postępowanie prowadzone jest w celu oszacowania wartości zamówienia.

Wstęp

W ramach zadania Wykonawca dostarczy sprzęty i oprogramowanie wyszczególnione w niniejszym dokumencie oraz dokona wdrożenia.

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

- Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów z obszaru Unii Europejskiej,

- Niedopuszczalne są produkty prototypowe, nie dopuszcza się urządzeń długotrwale magazynowanych oraz pochodzących z programów wyprzedażowych producenta. Urządzenia nie mogą się znajdować się na liście „end-of-sale” oraz „end-of-support” producenta.

- Zamawiający wymaga, by dostarczone urządzenia były nowe (tzn. wyprodukowane nie dawniej, niż na 6 miesięcy przed ich dostarczeniem) oraz by nie były używane (przy czym Zamawiający dopuszcza, by urządzenia były rozpakowane i uruchomione przed ich dostarczeniem wyłącznie przez Wykonawcę i wyłącznie w celu weryfikacji działania urządzenia, przy czym jest zobowiązany do poinformowania Zamawiającego o zamiarze rozpakowania sprzętu, a Zamawiający ma prawo inspekcji sprzętu przed jego rozpakowaniem);

- Zamawiający wymaga, by dostarczone licencje na oprogramowanie i systemy operacyjne były nowe i nie były nigdy wcześniej aktywowane czy używane na innych urządzeniach;

- Musi posiadać stosowny pakiet usług gwarancyjnych świadczonych przez producenta sprzętu (lub autoryzowany serwis) kierowanych do użytkowników z obszaru Rzeczpospolitej Polskiej;

- Całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne producentów sprzętu.

- Wymagane jest utrzymanie świadczeń gwarancyjnych (przez producenta urządzeń lub jego autoryzowaną placówkę serwisową) także w przypadku bankructwa Wykonawcy niemożliwości ich wypełnienia przez Wykonawcę (np. w przypadku jego bankructwa);

- Wykonawca zapewnia i zobowiązuje się, że korzystanie przez Zamawiającego z dostarczonych produktów nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich;

- Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach:

230 V ±10%, 50Hz;

- W cenę musi być wliczony koszt dostawy – transportu oraz w przypadku sprzętu montażu w szafie krosowej lub innym wskazanym miejscu;

- Wykonawca zapewni dostawę do wskazanej lokalizacji w siedzibie Zamawiającego w dni powszednie w godzinach 8-15;

- Zamawiający opisując przedmiot zamówienia przy pomocy określonych norm, aprobat czy specyfikacji technicznych i systemów odniesienia dopuszcza rozwiązania równoważne opisywanym. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów uwiarygodniających te rozwiązania;

- Rozwiązanie równoważne musi pozwalać na zrealizowanie zakładanego przez Zamawiającego celu poprzez parametry wydajnościowe i funkcjonalne.

Zamawiający dopuszcza realizację poszczególnych grup funkcjonalnych przez zespoły urządzeń pod następującymi warunkami:

a) połączenie urządzeń będzie zrealizowane w sposób nie ograniczający wydajności (sumaryczna przepustowość połączeń pomiędzy dowolnymi urządzeniami wchodzącymi w skład zestawu, jak również wydajność poszczególnych urządzeń nie może być niższa niż wymagana wydajność urządzenia),

b) łączna wielkość zestawu nie będzie przekraczać wymaganej wielkości urządzenia,

c) zapewnione i dostarczone będą wszystkie elementy konieczne do połączenia zespołu urządzeń,

d) wszystkie elementy zestawu będą spełniały wymagania związane z zarządzaniem.

2. Przedmiotem niniejszego **szacowanie wartości zamówienia** jest:

W szczególności wymagany zakres sprzętu obejmuje:

2.1. Centralny system logowania zdarzeń sieciowych UTM – 1 sztuka

Producent..... Model.....

Opis Przedmiotu Zamówienia

Z uwagi na posiadanie przez Zamawiającego oprogramowania i urządzeń sieciowych rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: Microsoft Hyper-V wersje: 2019, 2022;.

Poniżej zamawiający określa minimalne wymagania dla systemu.

1.1. **Interfejsy, Dysk**

1. System musi obsługiwać:
   a) co najmniej 4 interfejsy sieciowe
   b) wspierać powierzchnię dyskową o pojemności minimum 3 TB.

1.2. **Parametry wydajnościowe**

1. System musi być w stanie przyjmować minimum 5 GB logów na dzień.
2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.

W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:

1.3. **Logowanie**

1. System musi zapewniać podgląd logowanych zdarzeń w czasie rzeczywistym.
2. System musi zapewniać możliwość przeglądania logów historycznych z funkcją filtrowania.
3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa.

Muszą one obejmować co najmniej:

a) Listę najczęściej wykrywanych ataków;

b) Listę najbardziej aktywnych użytkowników;
c) Listę najczęściej wykorzystywanych aplikacji;
d) Listę najczęściej odwiedzanych stron www;
e) Listę krajów, do których nawiązywane są połączenia;
f) Listę najczęściej wykorzystywanych polityk Firewall;
g) Informacje o realizowanych połączeniach IPSec.

4. System musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Dodatkowo system musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
5. System musi zapewniać komunikację systemów bezpieczeństwa z systemami, z których przesyłane są logi do systemu centralnego logowania z wykorzystaniem co najmniej z protokołów UDP/514 oraz TCP/514.
6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długoterminowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy Zamawiającego.

1.4. **Raportowanie**

W zakresie raportowania system musi zapewniać:

1. Generowanie raportów co najmniej w formatach: PDF, CSV.
2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
3. Funkcję definiowania własnych raportów.
4. Możliwość spolszczenia raportów.
5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

1.5. **Korelacja logów**

W zakresie korelacji zdarzeń system musi zapewniać:

1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System musi korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:

- Malware
- Aplikacje sieciowe
- Email
- IPS
- Traffic
- Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.

1.6. **Zarządzanie**

1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowaną konsolę zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.
2. Proces uwierzytelniania administratorów musi być realizowany w oparciu o lokalną bazę, Radius, LDAP, PKI.
3. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

2.1. Serwisy i licencje

1. System musi być dostarczony w modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.
2. System musi być objęty serwisem producenta do 18 czerwca 2026, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

2.2. Rozszerzone wsparcie

Do zamawianego produktu Wykonawca zapewni usługi wsparcia technicznego świadczona w języku polskim w zakresie co najmniej:

a) Wdrożenia produktu na miejscu u Zamawiającego zgodnie z wytycznymi zamawiającego oraz podłączenie wskazanych urządzeń UTM (podłączenie, instalacja, konfiguracja) – minimum 6 godzin u zamawiającego;
b) pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu;
c) zdalna konfiguracja produktu (połączenia szyfrowane) zgodnie z wymaganiami użytkownika 5 godzina;
d) wsparcie telefoniczne i doradztwo w zakresie późniejszych zmian konfiguracji produktu 10 godziny.
e) Wdrożenie i wsparcie musi być wykonane przez certyfikowane inżyniera producenta.

2.2. FortiToken do UTM Forti w paczkach po 5 sztuk (dwa urządzenia do rejestracji) – licencja bezterminowa

Producent..... Model.....

Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów programowych.

1. W ramach postępowania powinny zostać dostarczone co najmniej 10 tokenów programowe współpracujące z posiadanym przez Zamawiającego urządzeniem FortiGate, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów oraz w ramach połączeń VPN typu client-to-site. Tokony w paczkach po 5 sztuk – niezależna możliwość rejestracji na 2 urządzeniach UTM po 5 sztuk tokenów.
2. Wsparcie dla tokenów programowych (software token) dla takich systemów operacyjnych jak iOS, Android, Windows Phone (8 i 8.1) oraz Windows 10 Mobile.
3. Dla tokenów na system iOS i Android wymaga się:
   a) aktywacji z systemu firewall FortiGate
   b) generowania kodu (cyfr) co 30 lub 60 sekund,
   c) możliwości dezaktywacji tokenu oraz jego reinstalacji (przeniesienia na inne urządzenie mobilne),
   d) ochrony dostępu poprzez konfigurowalny kod PIN,

Rejestracja na wskazanych przez zamawiającego urządzeniach UTM.

2.3. Urządzenie UTM 1 sztuka

W ramach dostawy należy dokonać dostawy urządzeń FortiGate 100F oraz **4 wkładki SR SFP+ 10 Gbps. (dwa do nowego urządzenia i dwa do posiadanego w ramach klastra)** oraz skonfigurować go w klaster z posiadanym . FortiGate 100F przez Zamawiającego. **Wykonawca dostarcza niezbędne kable sieciowe do połączenia i konfiguracji.**

W przypadku oferowania urządzenia równoważnego dostarczony system musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe a także powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe (dla oferowanego urządzenia równoważnego), które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. W ramach dostawy muszą zostać skonfigurowane działanie urządzenia z posiadanym przez Zamawiającego FortiGate 100F jako klaster HA. Dopuszcza się aby elementy wchodzące w skład systemu ochrony były zrealizowane w postaci zamkniętej platformy sprzętowej lub w postaci komercyjnej aplikacji instalowanej na platformie ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. Dla elementów równoważnego systemu bezpieczeństwa wykonawca zapewni wszystkie poniższe funkcjonalności:

Lp.	Charakterystyka (wymagania minimalne)	Charakterystyka (parametry oferowane)
1.	W ofercie wymagane jest podanie modelu, symbolu oraz producenta	…… */wpisać: model, symbol, producent urządzenia/*

Lp.	Charakterystyka (wymagania minimalne)	Charakterystyka (parametry oferowane)
	Wymagania Ogólne	
2.	System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.	TAK/ NIE*
3.	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 3 administratorów do poszczególnych instancji systemu.	TAK/ NIE*
4.	System musi wspierać IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.	TAK/ NIE*
	Redundancja, monitoring i wykrywanie awarii	
5.	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.	TAK/ NIE*
6.	Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.	TAK/ NIE*

Lp.	Charakterystyka (wymagania minimalne)	Charakterystyka (parametry oferowane)
7.	Monitoring stanu realizowanych połączeń VPN.	TAK/ NIE*
8.	System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.	TAK/ NIE*
Interfejsy, Dysk, Zasilanie		
9.	System realizujący funkcję Firewall musi dysponować minimum: a) 16 portami Ethernet 10/100/1000 Base-TX. b) 8 gniazdami SFP 1 Gbps. c) 2 gniazdami SFP+ 10 Gbps. z zainstalowanymi wkładkami	TAK/ NIE* a) …… b) …… c) …… */wskazać ilość oferowanych portów/*
10.	System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.	TAK/ NIE*
11.	W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q	TAK/ NIE* …… */wskazać ilość możliwych do zdefiniowania interfejsów wirtualnych/*
12.	System musi być wyposażony w zasilanie AC.	TAK/ NIE*
Parametry wydajnościowe		
13.	W zakresie Firewall'a obsługa nie mniej niż 1.5 mln. jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę.	TAK/ NIE* …… */wskazać ilość obsługiwanych jednoczesnych połączeń/*

Lp.	Charakterystyka (wymagania minimalne)	Charakterystyka (parametry oferowane)
		…… */wskazać ilość obsługiwanych nowych połączeń na sekundę/*
14.	Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.	TAK/ NIE* …… */wskazać przepustowość oferowanego urządzenia/*
15.	Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps.	TAK/ NIE* …… */wskazać przepustowość oferowanego urządzenia/*
16.	Wydajność szyfrowania IPSec VPN nie mniej niż 10 Gbps.	TAK/ NIE* …… */wskazać oferowaną wydajność szyfrowania/*
17.	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 2.5 Gbps.	TAK/ NIE* …… */wskazać oferowaną wydajność skanowania/*
18.	Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.	TAK/ NIE* …… */wskazać oferowaną wydajność skanowania/*
19.	Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.	TAK/ NIE* …… */wskazać oferowaną wydajność systemu/*

Lp.	Charakterystyka (wymagania minimalne)	Charakterystyka (parametry oferowane)
	Funkcje Systemu Bezpieczeństwa	
20.	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcji. Mogą one być realizowane w postaci osobnych platform sprzętowych lub programowych: a) Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. b) Kontrola Aplikacji. c) Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. d) Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. e) Ochrona przed atakami - Intrusion Prevention System. f) Kontrola stron WWW. g) Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. h) Zarządzanie pasmem (QoS, Traffic shaping). i) Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). j) Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. k) Analiza ruchu szyfrowanego protokołem SSL. l) Analiza ruchu szyfrowanego protokołem SSH.	TAK/ NIE*
	Polityki, Firewall	
21.	Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.	TAK/ NIE*

Lp.	Charakterystyka (wymagania minimalne)	Charakterystyka (parametry oferowane)
22.	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.	TAK/ NIE*
23.	W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.	TAK/ NIE*
24.	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 • Cisco ACI. • Google Cloud Platform (GCP). • OpenStack. • VMware vCenter (ESXi).	TAK/ NIE*
Połączenia VPN		
25.	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.	TAK/ NIE*

Lp.	Charakterystyka (wymagania minimalne)	Charakterystyka (parametry oferowane)
	• 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.	
26.	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.	TAK/ NIE*
Routing i obsługa łączy WAN		
27.	W zakresie routingu rozwiązanie zapewnia obsługę: • Routingu statycznego. • Policy Based Routingu. • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.	TAK/ NIE*
Zarządzanie pasmem		
28.	System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.	TAK/ NIE*
29.	Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.	TAK/ NIE*
30.	System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.	TAK/ NIE*
Ochrona przed malware		

Lp.	Charakterystyka (wymagania minimalne)	Charakterystyka (parametry oferowane)
31.	Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).	TAK/ NIE*
32.	System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.	TAK/ NIE*
33.	System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).	TAK/ NIE*
34.	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.	TAK/ NIE*
35.	System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.	TAK/ NIE*
Ochrona przed atakami		
36.	Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.	TAK/ NIE*
37.	System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.	TAK/ NIE*
38.	Baza sygnatur ataków zawiera minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.	TAK/ NIE*
39.	Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.	TAK/ NIE*
40.	System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.	TAK/ NIE*
41.	Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany,	TAK/ NIE*

Lp.	Charakterystyka (wymagania minimalne)	Charakterystyka (parametry oferowane)
	Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.	
42.	Wykrywanie i blokowanie komunikacji C&C do sieci botnet.	TAK/ NIE*
Kontrola aplikacji		
43.	Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.	TAK/ NIE*
44.	Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.	TAK/ NIE*
45.	Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.	TAK/ NIE*
46.	Baza zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.	TAK/ NIE*
47.	Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.	TAK/ NIE*
Kontrola WWW		
48.	Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.	TAK/ NIE*
49.	W ramach filtra www dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.	TAK/ NIE*
50.	Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.	TAK/ NIE*
51.	Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.	TAK/ NIE*

Lp.	Charakterystyka (wymagania minimalne)	Charakterystyka (parametry oferowane)
52.	Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.	TAK/ NIE*
53.	Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.	TAK/ NIE*
54.	W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych ulr - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.	TAK/ NIE*
Uwierzytelnianie użytkowników w ramach sesji		
55.	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.	TAK/ NIE*
56.	Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.	TAK/ NIE*
57.	Rozwiązanie umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.	TAK/ NIE*
Zarządzanie		
58.	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. System musi umożliwiać integrację i wspólne zarządzanie przełącznikami dostarczanymi w punkcie 3.1 oraz 3.2.	TAK/ NIE*

Lp.	Charakterystyka (wymagania minimalne)	Charakterystyka (parametry oferowane)
59.	Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.	TAK/ NIE*
60.	Możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.	TAK/ NIE*
61.	System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.	TAK/ NIE*
62.	System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.	TAK/ NIE*
63.	Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.	TAK/ NIE*
64.	Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.	TAK/ NIE*
Logowanie		
65.	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.	TAK/ NIE*
66.	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.	TAK/ NIE*
67.	Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.	TAK/ NIE*

Lp.	Charakterystyka (wymagania minimalne)	Charakterystyka (parametry oferowane)
68.	Musi istnieć możliwość logowania do serwera SYSLOG.	TAK/ NIE*

Wymogi nietechniczne:

Gwarancje, serwisy i licencje		
1.	Gwarancja od montażu do 18 czerwca 2026 a) System musi być objęty serwisem gwarancyjnym producenta realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku gdy producent nie posiada na terenie Rzeczpospolitej Polskiej własnego centrum serwisowego, oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7;	TAK/ NIE*
2.	W ramach postępowania powinny zostać dostarczone subskrypcje na okres do 18 czerwca 2026. Powyższa subskrypcja ma upoważniać Zamawiającego 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.	.....

		*/podać typ (nazwę) okres oferowanej subskrypcji/***
Dokumenty i certyfikaty		
3.	Oświadczenie Wykonawcy, że poszczególne elementy oferowanego systemu bezpieczeństwa posiadają następujące certyfikacje: ICSA lub EAL4 dla funkcji Firewall.	
4.	W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien posiadać po zakończeniu wdrożenia: 1. 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 (t.j. Dz.U. z 2020 r. poz. 509). 2. dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.	

2.4. **Dostawę przełączników sieci LAN – 1 sztuka – o parametrach nie gorszych niż:**

Producent..... Model..... Rok produkcji.....		
Nazwa parametru, elementu lub cechy	**Wymagane parametry techniczne**	**Parametry techniczne oferowanego urządzenia**
Parametry fizyczne	- Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. - Zasilanie AC 230V. - Budżet mocy dla portów PoE min.: 370 W. - Maksymalny pobór mocy bez budżetu dla PoE: 110 W.	TAK/ NIE*
Interfejsy sieciowe	- 48 porty GE RJ-45.W tym porty PoE w ilości co najmniej: 24, zgodne ze standardem: 802.3af oraz 802.3at. **4 gniazdami SFP+ 10 Gbps. z zainstalowanymi wkładkami SR + 4 przewody do podłączenia o długości 3mb**	TAK/ NIE*

Zarządzanie	- Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS), oraz z poziomu UTM FortiGate posiadanego przez zamawiającego. - Wsparcie dla SNMP w wersjach 1-3 - Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. - Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. - Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. - Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). - Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. - Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. - Automatycznie wykonywane rewizje konfiguracji.	TAK/ NIE*
Parametry wydajnościowe	- Przepustowość urządzenia - min. 175 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 250 Mpps. - Tablica adresów MAC o pojemności co najmniej 32k wpisów. - Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.	TAK/ NIE*
Wymagane funkcje	- Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. - Obsługa Jumbo Frames.	TAK/ NIE*

	- Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). - Agregacja portów zgodna ze standardem 802.3ad. - Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q. - Obsługa routingu statycznego. - Port-mirroring. - Uwierzytelnianie 802.1x na poziomie portu. - Uwierzytelnianie 802.1x w oparciu o adres MAC. - W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN). - W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. - W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN. - Obsługa protokołu sFlow.	
Gwarancja	- System musi być objęty serwisem gwarancyjnym producenta do 18 czerwca 2026 roku, 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.	TAK/ NIE*
Rozszerzone wsparcie serwisowe	- System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w następnym dniu roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora do 18 czerwca 2026 roku.	TAK/ NIE*

Dostawa i montaż:

Dostawa wraz z instalacją w szafie krosowej u Zamawiającego oraz wstępna konfiguracją ustalona z Zamawiającym – max. 3 godzin zegarowych na miejscu u Zamawiającego.

2.5. Serwer dla usług cyberbezpieczeństwa

Miejsce instalacji sprzętu i oprogramowania/systemu.

Dostarczony sprzęt i oprogramowanie powinny zostać zamontowane, zainstalowane i skonfigurowane zgodnie z wymaganiami opisanymi w dalszej części, w budynku urzędu w miejscu wskazanym przez Zamawiającego.

Zakres dostawy - server

Lp.	Nazwa parametru, elementu lub cechy	Wymagane parametry techniczne	Parametry techniczne oferowanego urządzenia
	1	2	3
TYP		W ofercie wymagane jest podanie modelu, symbolu oraz producenta	…… …… /wpisać: model, symbol, producent urządzenia/

1.	**Obudowa**	Obudowa Rack o wysokości max. 2U umożliwiającą instalację min. 8 dysków 2,5” z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.	TAK/ NIE*
2.	**Płyta główna**	Płyta główna z możliwością zainstalowania dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.	TAK/ NIE*
3.	**Chipset**	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.	TAK/ NIE*
4.	**Procesor**	Zainstalowane dwa procesory 8-rdzeniowe, taktowanie bazowe 3,2 GHz, architektura x86_64; osiągające w teście SPEC CPU2017 Integer Rate Result wynik SPECrate2017_int_base min. 173 pkt. (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie http://spec.org/cpu2017/results/cpu2017.html [spec.org]	TAK/ NIE* …… …….. */podać procesor - wynik w teście – rodzaj testu i link do testu/*
5.	**RAM**	Min. 256GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać min. 1TB pamięci RAM. (min. 8 slotów musi zostać wolnych)	TAK/ NIE*
6.	**Zabezpieczenia pamięci RAM**	Memory Health Check, Memory Page Retire	TAK/ NIE*
7.	**Gniazda PCI**	- minimum dwa sloty PCIe x16 generacji 4	TAK/ NIE*

			…… …… */podać ilość i rodzaj slotów PCIe/*
8.	**Interfejsy sieciowe**	Interfejs sieciowy 4 x min. 10 Gb Ethernet w SFP +/ SFP28 **obsadzony dwoma wkładkami 10Gb SR —(dwa wolne)** Interfejs sieciowy 2 x 1Gb Ethernet	TAK/ NIE*
9.	**Dyski twarde**	Zainstalowane 5 x min. 960GB SATA SSD skonfigurowane w RAID 5. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażonego w nośniki typu flash o pojemności min. 64GB, z możliwoscią konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmiejszenia ilości wnęk na dyski twarde. Możliwość instalacji hot-swap M.2 SATA o pojemności min. 480GB.	TAK/ NIE*
10.	**Kontroler RAID**	Sprzętowy kontroler dyskowy z pojemnością cache min. 4GB, możliwe konfiguracje poziomów RAID: 0,1,5,6,10,50,60.	TAK/ NIE*
11.	**Wbudowane porty**	min. port USB 2.0 oraz port USB 3.0, port VGA.	TAK/ NIE*
12.	**Video**	Zintegrowana karta graficzna.	TAK/ NIE*
13.	**Wentylatory**	Redundantne	TAK/ NIE*

14.	**Zasilacze**	Min. dwa zasilacze Hot-Plug min. 800W	TAK/ NIE*
15.	**Bezpieczeństwo**	Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła . Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. Moduł TPM 2.0 V3. Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem.	TAK/ NIE*
16.	**Karta Zarządzania**	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika • możliwość podmontowania zdalnych wirtualnych napędów • wirtualną konsolę z dostępem do myszy, klawiatury • wsparcie dla IPv6 • wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz. • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer • integracja z Active Directory	TAK/ NIE*

		• możliwość obsługi przez ośmiu administratorów jednocześnie • Wsparcie dla automatycznej rejestracji DNS • wsparcie dla LLDP • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej • możliwość podłączenia lokalnego poprzez złącze RS-232. • możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy. • Monitorowanie zużycia dysków SSD • możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi, • Automatyczne zgłaszanie alertów do centrum serwisowego producenta • Automatyczne update firmware dla wszystkich komponentów serwera • Możliwość przywrócenia poprzednich wersji firmware • Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON • Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych • Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram. • Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera	
17.	**Certyfikaty**	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001. Serwer musi posiadać deklaracja CE. Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 lub oświadczenie producenta o stosowaniu w fabrykach polityki zarządzania energią, która jest zgodna z obowiązującymi przepisami na terenie Unii Europejskiej. Oferowany serwer musi znajdować się na liście Windows Server Catalog i	TAK/ NIE*

		posiadać status „Certified for Windows” dla systemów Microsoft Windows 2019, Microsoft Windows 2022.	
18.	**Normy Środowiskowe**	Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Bronze według normy wprowadzonej w 2019 roku - ***Wykonawca złoży do oferty dokument potwierdzający spełnianie*** **wymogu.**	TAK/ NIE*
19.	**Warunki gwarancji**	48 miesiące - gwarancja producenta z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta. – **w ofercie należy podać koszt serwera z gwarancją do 18 czerwca 2026 oraz koszt gwarancji na pozostały okres jako odrębną pozycję kosztową** **Dokumenty niezbędne do przedstawienia Zmawiającemu przed podpisaniem protokołu odbioru :** Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.	TAK/ NIE*

		Oświadczenie producenta serwera, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji systemu.	
20.	**Dokumentacja użytkownika**	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego lub przez www sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.	TAK/ NIE*

Dostawa i montaż:

- Dostawa wraz z instalacją u Zamawiającego w szafie krosowej, konfiguracją systemu operacyjnego – max. 6 godzin zegarowych na miejscu u Zamawiającego.

2.6. Licencja dla serwera

Serwerowe systemy operacyjne dla serwerów			
Lp.	**Nazwa parametru, elementu lub cechy**	**Wymagane minimalne parametry techniczne**	**Parametr oferowany**
	1	**2**	**3**

1.	**Oprogramowanie**	Licencje MS Windows Server 2022 Standard lub równoważne (opis równoważności w pkt. 2). Dostarczone licencje muszą upoważniać do użytkowania dostarczonego oprogramowania na czas nieokreślony. Dostarczone licencje muszą umożliwiać uruchomienie min. 3 maszyn wirtualnych z systemem Windows Server 2022 (w ramach dostarczonej licencji) na serwerze po zainstalowania środowiska graficznego na podstawie.	…… /wypełnić/ TAK/ NIE*
	Zamawiający wymaga spełnienia przez oprogramowanie równoważne minimalnych wymagań w zakresie funkcjonalności określonych poniżej:		
2.	**Funkcjonalności i kryteria**	Oprogramowanie równoważne musi spełnić poniższe kryteria: Zakres Przedmiotu Zamówienia obejmuje dostarczenie Oprogramowania Systemowego zwanego dalej SSO. SSO musi posiadać następujące, wbudowane cechy: a) możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym, b) możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny, c) możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych, d) 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,	TAK/ NIE*

		e) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy, f) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy, g) automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading), i) wbudowane wsparcie instalacji i pracy na wolumenach, które: I. pozwalają na zmianę rozmiaru w czasie pracy systemu, II. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, III. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, IV. umożliwiają zdefiniowanie list kontroli dostępu (ACL), j) wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość, k) wbudowane szyfrowanie dysków l) możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET, m) możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów, n) wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla	

		ochrony połączeń internetowych i intranetowych, o) graficzny interfejs użytkownika, p) zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, r) wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play), s) możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu, t) dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa, u) możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: I. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, II. 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: 1) podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, 2) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, 3) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,	

		III. zdalna dystrybucja oprogramowania na stacje robocze, IV. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, V. centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: 1) dystrybucję certyfikatów poprzez http, 2) konsolidację CA dla wielu lasów domeny, 3) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, VI. szyfrowanie plików i folderów, VII. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), VIII.możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów, IX. serwis udostępniania stron WWW, X. wsparcie dla protokołu IP w wersji 6 (IPv6), XI. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 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: 1) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, 2) obsługi ramek typu jumbo frames dla maszyn wirtualnych,	

		3) obsługi 4-KB sektorów dysków, 4) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, 5) możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, 6) możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model), v) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet, w) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath), x) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego, y) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, z) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.	

2.7. **Network Attached Storage (NAS) - 1 sztuka.**

Network Attached Storage (NAS)	**Parametry minimalne**	**……**

		Typ / model / producent
Procesor	wymagany	……. Model / typ
Architektura procesora	64 bit	TAK / NIE
Procesor liczba rdzeni	Nie mniej niż 8 o taktowaniu nie niższym niż 3,6 GHz	TAK / NIE
Pamięć RAM	Nie mniej niż 32GB DDR4	TAK / NIE
Pamieć RAM liczba slotów	Minimum 4 sloty	TAK / NIE
Pamięć RAM - możliwość rozszerzenia	Nie mniej niż do 128 GB	TAK / NIE
Pamięć Flash	Nie mniej niż 5GB	TAK / NIE
Liczba zatok na dyski twarde	Minimum 16	TAK / NIE
Obsugiwane dyski twarde	3.5" SATA oraz 2.5" SATA / SSD SATA	TAK / NIE
Pojemność dysków twardych jakie można stosować	do 24 TB	TAK / NIE
Możliwość podłączenia modułu rozszerzającego	Tak, maksymalnie do 16	TAK / NIE
Porty LAN	Minimum 2 x 1 Gb/s Ethernet, 2 x 10 Gb/s SFP+	TAK / NIE
Diody LED	HDD 1–16, stan urządzenia, LAN	TAK / NIE
Porty USB	min. 1 gniazdo USB 3.2 Gen2 10 Gb/s	TAK / NIE
Przyciski	Reset, Zasilanie	TAK / NIE
Typ obudowy	RACK, 3U	TAK / NIE
Zasilanie	Redundatne min. 500 W(x2), 100–240 V	TAK / NIE
Agregacja łączy	Wymagane	TAK / NIE

Obsługiwane systemy plików	Dyski wewnętrzne: ZFS Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+	TAK / NIE
Możliwość podłączenia karty WLAN na USB	Wymagane	TAK / NIE
Łączenie usług z interfejsem	Wymagane	TAK / NIE
Szyfrowanie udziałów	Wymagane, min AES 256	TAK / NIE
Szyfrowanie dysków zewnętrznych	Wymagane	TAK / NIE
Zarządzanie dyskami	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 z wykorzystaniem dysków SSD Cache odczytu i dziennik zapisu z wykorzystaniem dysków SSD Funkcjonalność migawek udziałów oraz LUN, wraz z możliwością ich replikacji na drugie urządzenie	TAK / NIE

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	TAK / NIE
Obsługa Fiber Channel (FC SAN)	Wsparcie opcjonalnych kart FC Mapowanie LUN	TAK / NIE
Zarządzanie prawami dostępu	Przypisanie pojemności dla użytkowników Importowanie listy użytkowników Zarządzanie kontami użytkowników Zarządzanie grupą użytkowników Zarządzanie uprawnieniami dla użytkowników i grup Obsługa zaawansowanych uprawnień dla podfolderów	TAK / NIE
Obsługa Windows AD	Logowanie użytkowników domenowych poprzez protokoły CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera i klienta LDAP	TAK / NIE
Funkcje backup	Oprogramowanie do tworzenia kopii bezpieczeństwa plików, opracowane przez producenta urządzenia dla systemów Windows. Backup na zewnętrzne dyski twarde.	TAK / NIE

Współpraca z zewnętrznymi dostawcami usług chmury	Przynajmniej: Amazon S3, Amazon Glacier, Microsoft Azure, Google Cloud Storage, Dropbox, OneDrive for Business, Google Drive	TAK / NIE
Darmowe aplikacje na urządzenia mobilne	Monitoring i zarządzanie urządzeniem / Współdzielenie plików / Obsługa kamer Dostępne na systemy iOS oraz Android	TAK / NIE
Minimum obsługiwane aplikacje	Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer pobierania (Bittorrent/HTTP/HTTPS/FTP)	TAK / NIE
VPN	VPN client / VPN server Minimum obsługa PPTP, OpenVPN	TAK / NIE

Administracja systemu	Połączenia HTTP/HTTPS Powiadamianie przez e-mail Powiadamianie przez SMS (z wykorzystaniem zewnętrznych usług) DDNS oraz zdalny dostęp w chmurze producenta SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP oraz lokalnych przez USB Monitorowanie zasobów urządzenia Monitorowanie zasobów systemu w czasie rzeczywistym Rejestr zdarzeń Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania Możliwość aktualizacji oprogramowania z powiadomieniem z serwerów producenta Ustawienia systemowe: kopia zapasowa, przywracanie, resetowanie systemu	TAK / NIE
Wirtualizacja	Możliwość uruchomienia maszyn wirtualnych z systemem Windows, Linux, Unix i Android Import maszyn wirtualnych Klonowanie maszyn wirtualnych	TAK / NIE

	Migawki maszyn wirtualnych GPU pass-through dla dodatkowych kart graficznych	
Zabezpieczenia	Filtracja IP Ochrona dostępu do sieci z automatycznym blokowaniem połączeń Obsługa HTTPS FTP z SSL/TLS (Explicit) Obsługa SFTP (tylko admin) Szyfrowanie AES 256-bit Import certyfikatu SSL	TAK / NIE
Możliwość instalacji dodatkowego oprogramowania	Tak, sklep z aplikacjami producenta i aplikacjami firm zewnętrznych Możliwość instalacji z gotowych paczek oraz wbudowane narzędzia wirtualizacji umożliwiającee zarówno obsługę kontenerów Docker/LXC jak i pełnych maszyn wirtualnych	TAK / NIE
Gwarancja	do 18 czerwca 2026 roku	TAK / NIE

Wykonawca dostarcza NAS do zamawiającego instaluje w szafir RACK oraz podłącza do przełączników przez złącza 2 x 1 Gb/s Ethernet, 2 x 10 Gb/s SFP+ należy zapewnić odpowiednie przewody i wkładki do połączenia. Konfiguracja i podział przestrzeni dyskowej zostanie zrealizowany przez wykonawcę zgodnie ze wskazaniem Zamawiającego.

2.8. Dyski twarde do macierzy dyskowej NAS - 16 sztuk.

Dyski twarde do macierzy dyskowej	Minimalne wymagania	…… Typ / model / producent
Dysk twardy 8TB	**przeznaczony dla systemów NAS pracującym w systemie ciągłym – wykazane przez w/w producenta NAS jako zalecany / kompatybilny.**	TAK / NIE
Pojemność	min. 8000 GB	TAK / NIE
Typ	HDD (magnetyczny)	TAK / NIE
Format	Format 3,5 cala	TAK / NIE
Interfejs	SATA III (6 Gb/s)	TAK / NIE
Pamięć cache	min. 256 MB	TAK / NIE
Prędkość obrotowa	7200 obr./ min.	TAK / NIE
MTBF	**1000000 h**	TAK / NIE

Gwarancja - Uszkodzony dysk pozostaje u zmawiającego do 18 czerwca 2026	**Wymagane**	TAK / NIE
Dysk znajduje się na liście kompatybilności do urządzenia oferowanego w 2.7. Network Attached Storage (NAS) - 1 sztuka.	**Wymagane**	TAK / NIE

2.9. Backup - rozwiązanie, które zapewnia technologie odzyskiwania po awarii, w tym mechanizmy automatycznej odbudowy

Backup - rozwiązanie, które zapewnia technologie odzyskiwania po awarii, w tym mechanizmy automatycznej odbudowy Sprzęt musi być fabrycznie nowy, rok produkcji nie starszy niż 2024r **System musi być dostarczony w ramach sprzętowego appliance z zainstalowanymi i skonfigurowanymi wszystkim usługami, niezbędnymi do pracy systemu.**	**Minimalne wymagania**	**……** **Typ / model / producent**
Zarządzanie i magazyny		
Obudowa rack rozmiar:	1U	TAK / NIE
Procesor:	min. 6 rdzeni, min. 12 wątków. Minimalna częstotliwość bazowa procesora 2,9 GHz	
Pamięć RAM	16GB DDR4	TAK / NIE
Przestrzeń dostępna na przechowywanie danych:	min. 24TB po RAID 5	TAK / NIE

	Osobne dyski SSD M.2 nVME działające w RAID1 w celu instalacji warstwy oprogramowania i systemu operacyjnego,	TAK / NIE
Zasilacz	Redundantne zasilanie	TAK / NIE
Interfejsy sieciowe:	min. 2szt. Ethernet 1Gb	TAK / NIE
Istotne - Zarządzanie i magazyny	1. Produkt dostępny w polskiej wersji językowej.	TAK / NIE
	2. Konsola zarządzająca dostępna z poziomu przeglądarki internetowej	TAK / NIE
	3. System musi umożliwiać tworzenie kopii zapasowych na poziomie dysków	TAK / NIE
	4. System musi umożliwiać tworzenie kopii zapasowych na poziomie plików i folderów	TAK / NIE
	5. System musi umożliwiać replikację kopii zapasowych do wielu lokalizacji docelowych	TAK / NIE
	6. System musi umożliwiać tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT	TAK / NIE
	7. System musi umożliwiać współpracę z usługą kopiowania woluminów w tle (VSS) firmy Microsoft	TAK / NIE
	8. Możliwość zdefiniowania limitu przepustowości sieciowej z jakiej ma korzystać oprogramowanie backupowe	TAK / NIE

9. System zarządzania nie może być oparty o relacyjne bazy danych.	TAK / NIE
10. Rozwiązanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju w procesie tworzenia kopii zapasowej).	TAK / NIE
11. Rozwiązanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera (urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera (urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów).	TAK / NIE
12. Aplikacje klienckie powinny wysyłać dane z kopii zapasowej bezpośrednio na wskazany magazyn – serwer backupu/usługa zarządzania, ani żaden inny element Systemu, nie powinien brać udziału w przesyłaniu danych.	TAK / NIE
13. Rozwiązanie musi być systemem multi-storage-owym i umożliwia tworzenie wielu repozytoriów danych jednocześnie również na innych środowiskach jako przestrzeń do replikacji danych.	TAK / NIE
14. System musi oferować mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.	TAK / NIE
15. Rozwiązanie w warstwie sprzętowej powinno bazować na standardowych komponentach architektury x86, bez	TAK / NIE

powiązania i poleganiu na komponentach wyłącznie jednego dostawy (tzw. "no propietary vendor lock").	
16. System pozwala administratorowi na ustawienie dowolnego harmonogramu replikacji danych pomiędzy dowolnymi wspieranymi magazynami.	TAK / NIE
17. System musi umożliwiać wykonywanie kopii obrazu dysku, kopii plików i katalogów oraz kopii maszyn wirtualnych bez ich zatrzymywania z zachowaniem stuprocentowej integralności i spójności danych wewnątrz wykonanej kopii zapasowej.	TAK / NIE
18. Rozwiązanie musi realizować funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie.	TAK / NIE
19. Rozwiązanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia.	TAK / NIE
20. System musi umożliwiać automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku wystąpienia błędu.	TAK / NIE
21. Rozwiązanie powinno umożliwiać klonowanie planów kopii zapasowych, planów replikacji oraz planów testowego odtwarzania maszyn wirtualnych	TAK / NIE
22. Rozwiązanie powinno umożliwiać uruchamianie przy zadaniach backupu dowolnych skryptów PRE/POST oraz po wykonaniu migawki VSS.	TAK / NIE

23. System powinien umożliwiać definiowanie tzw. okna backupowego dla każdego z zadań w celu umożliwienia zarządzania obciążeniem sieci i uwzględnienia okien serwisowych występujących u Zamawiającego.	TAK / NIE
24. System musi automatycznie dodawać do polityki i harmonogramu tworzenia backupów nowe źródła / maszyny wirtualnych, dodane do bieżącego środowiska (automatyzacja oparta na polityce tworzenia kopii).	TAK / NIE
25. Rozwiązanie musi udostępniać możliwość podglądu postępu działania dowolnego zadania, w tym zadania wykonywania kopii zapasowych, odtwarzania danych, testowego odtwarzania danych, usuwania danych oraz zadania odświeżania zajętości magazynu na dane.	TAK / NIE
26. Rozwiązanie musi posiadać system powiadamiania poprzez e-mail oraz Slack o zdarzeniach w następujących przypadkach: zadanie zostało zakończone pomyślnie, zadanie zostało zakończone z ostrzeżeniami, zadanie zostało zakończone z błędem, zadanie zostało anulowane, zadanie nie zostało uruchomione.	TAK / NIE
27. System powinien umożliwiać wysyłanie powiadomień o statusie wykonanych zadań na dowolne adresy webhook, podawane przez użytkownika,	TAK / NIE

28. Oferowane rozwiązanie musi być dobrane pod względem wydajności w oparciu o najlepsze praktyki producenta.	TAK / NIE
29. Rozwiązanie musi być wyskalowane, dobrane pod względem wymaganej funkcjonalności i wydajności stosownie do ilości zabezpieczanych danych i obiektów z uwzględnieniem przyrostu danych (serwery, maszyny wirtualne, bazy danych itp.) zgodnie z opisem w zapytaniu ofertowym.	TAK / NIE
30. Wydajność oferowanej konfiguracji musi być taka, aby wszystkie funkcje systemu były dostępne w chwili wdrożenia (np. deduplikacja, kompresja, instancja workerów i browserów, replikacja, testowe odtwarzanie maszyn wirtualnych).	TAK / NIE
31. System pozwala na zmniejszenie rozmiaru przechowywanych i przesyłanych danych poprzez usuwanie zduplikowanych bloków danych ze źródła kopii pomiędzy wszystkimi źródłami w obrębie wszystkich kopii na magazynie danych.	TAK / NIE
32. Proces deduplikacji musi być możliwy dla każdego z typów obsługiwanych magazynów.	TAK / NIE
33. Proces deduplikacji nie może wymagać instalacji żadnych dodatkowych komponentów, które będą pośredniczyły w zapisie danych z deduplikowanych	TAK / NIE
34. Proces deduplikacji nie może posiadać pojedynczego punktu awarii	TAK / NIE

35. Proces deduplikacji realizowany jest blokiem o stałej wielkości.	TAK / NIE
36. Proces szyfrowania kopii zapasowych nie może ograniczać procesu deduplikacji w ramach tego samego klucza szyfrującego.	TAK / NIE
37. Kompresja kopii zapasowych musi obsługiwać jeden z wymienionych algorytmów: LZ4, ZStandard. Dodatkowo, musi umożliwiać określenie szczegółowego poziomu kompresji, w tym: niski, średni, wysoki.	TAK / NIE
38. Instalacja, modyfikacja ustawień, polityki tworzenia kopii zapasowej systemu nie może wymagać przerwania pracy lub restartu systemu.	TAK / NIE
39. System musi pozwalać na automatyczne aktualizacje oprogramowania.	TAK / NIE
40. System musi być w stanie kompresować i szyfrować zabezpieczone dane w systemach NAS.	TAK / NIE
41. System musi pozwalać na uruchomienie kontenerów Docker w dowolnych urządzeniach NAS w celu ich zabezpieczenia.	TAK / NIE
42. System tworzenia kopii zapasowej musi przechowywać dane w sposób zapewniający ich niezmienność (tzw. "resilience"), dzięki czemu kopie zapasowe nie będą mogły zostać nadpisane lub zmodyfikowane przez	TAK / NIE

cały okres ich przechowywania, retencji.	
43. System zarówno będzie przechowywać dane w kopii zapasowej w postaci zaszyfrowanej jak też ruch wewnątrz systemu również musi być szyfrowany.	TAK / NIE
44. Archiwum długoterminowych kopii zapasowych musi być szyfrowane, a odzyskiwanie z archiwum obsługiwane z tego samego interfejsu użytkownika, co inne przywracanie dane.	TAK / NIE
45. System musi mieć mechanizmy chroniące przejęcie konta administratora oraz umożliwiać definiowanie dodatkowych uprawnień dla każdej z predefiniowanych ról użytkowników.	TAK / NIE
46. System musi pozwalać na gradację uprawnień administratorów - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.: system operator, backup operator, restore operator, viewer. Dla każdej z tych ról system musi umożliwiać przypisywanie dodatkowych uprawnień, w tym możliwość zablokowania usuwania danych.	TAK / NIE
47. Rozwiązanie musi posiadać możliwość nieodwracalnego usuwania danych z magazynu na dane w momencie spełnienia dodatkowych wymogów.	TAK / NIE

48. W sytuacji, gdyby podstawowe urządzenie tworzenia kopii zapasowej było niedostępne, system musi posiadać możliwość przywrócenia z archiwum za pomocą innej instancji systemu dostarczonej przez tego samego producenta. tzn. archiwum musi zawierać wszystkie informacje konieczne do odzyskania.	TAK / NIE
49. Rozwiązanie musi umożliwiać uruchomienie konsoli w chmurze producenta zlokalizowanej na terenie Polski, w celu umożliwienia dostępu do środowiska zarządzania kopiami zapasowymi w przypadku czasowej niedostępności środowiska lokalnego.	TAK / NIE
50. System kopii zapasowej musi umożliwiać dostęp do konsoli administracyjnej z wielu stacji roboczych.	TAK / NIE
51. System kopii zapasowej musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.	TAK / NIE
52. System powinien posiadać predefiniowane schemat tworzenia kopii zapasowych: G-F-S, Forever incremental,	TAK / NIE
53. Rozwiązanie musi obsługiwać kontrolę dostępu opartą na rolach (RBAC).	TAK / NIE
54. Możliwość składowania utworzonych kopii zapasowych na magazynach chmurowych Amazon AWS, Azure,	TAK / NIE

Wasabi, Google Cloud Storage, Backblaze B2, magazyny zgodne z S3.	
55. Możliwość składowania utworzonych kopii zapasowych na udziałach sieciowych po protokole smb, nfs, iscsi, katalog lokalny	TAK / NIE
56. Zarządzanie i odzyskiwanie danych z kopii musi odbywać się z tego samego interfejsu użytkownika (konsoli), niezależnie od tego, gdzie znajduje się kopia zapasowa (w chmurze AWS, Azure, GCP, w Data Center czy w usłudze typu SaaS).	TAK / NIE
57. Czas przechowywania kopii zapasowej (retention time) systemu backupu nie może być zmieniony np. poprzez manipulowanie wskazaniami zegara serwera NTP w celu szybszego ich wyeksponowania - tzn. czasy przechowywania kopii zapasowych nie będą zależne od wskazań zegara czasu serwera NTP, ale będą wykorzystywać technologię, która mierzy upływ czasu.	TAK / NIE
58. Możliwość generowania raportów dobowych w oparciu o harmonogram	TAK / NIE
59. Produkt musi posiadać możliwość zapisu kopii zapasowych do magazynu chmurowego dostarczanego bezpośrednio przez producenta oprogramowania (datacenter musi być zlokalizowane na terenie Polski)	TAK / NIE

	60. Produkt musi posiadać możliwość zdefiniowania maksymalnej liczby równocześnie backupowanych urządzeń w ramach jednego planu backupowego, niezależnie od typu urządzenia (np. stacja robocza, serwer, maszyna wirtualna)	TAK / NIE
	61. Możliwość wyświetlenia szczegółowych informacji o chronionym urządzeniu takich jak: CPU, RAM, System operacyjny, Adres IP.	TAK / NIE
	62. Produkt musi posiadać możliwość zdefiniowania poziomu obciążenia magazynu, po osiągnięciu którego zostanie wysłane powiadomienia e-mail. (poziom definiowany indywidualnie dla każdego magazynu)	TAK / NIE
Środowiska fizyczne i bazy danych		
Środowiska fizyczne i bazy danych	1. Rozwiązanie powinno umożliwiać tworzenie grup urządzeń w celu automatyzacji procesów podczas pracy z urządzeniami.	TAK / NIE
	2. Produkt musi posiadać możliwość tworzenia zadań dla grupy urządzeń oraz dla wybranych urządzeń.	TAK / NIE
	3. Rozwiązanie musi pozwalać na automatyczne wyłączenie stacji roboczej po wykonaniu kopii zapasowej.	TAK / NIE
	4. Rozwiązanie backupowe musi pozwalać na zabezpieczanie zaszyfrowanych partycji min. BitLocker, Veracrypt, TrueCrypt, Eset Endpoint Encryption.	TAK / NIE

5. System jest niezależny od wersji Microsoft SQL i musi umożliwiać przywracanie danych SQL dla tej samej lub nowszej wersji.	TAK / NIE
6. System musi obsługiwać również narzędzia RMAN firmy Oracle do tworzenia kopii zapasowych i odzyskiwania. Dodatkowo system musi obsługiwać funkcję przyrostowego scalania danych.	TAK / NIE
7. System kopii zapasowej musi wspierać odtwarzanie pojedynczych plików z systemów Windows oraz Linux.	TAK / NIE
8. Odtwarzanie Bare Metal Restore w Systemie może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika.	TAK / NIE
9. Rozwiązanie powinno umożliwiać uruchamianie procesu Bare Metal Restore z dowolnego bootowalnego nośnika danych.	TAK / NIE
10. Rozwiązanie powinno wspierać odtwarzanie danych w scenariuszach P2P, P2V, V2P, V2V.	TAK / NIE
11. Rozwiązanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie (RAW, VHD, VHDX, VMDK).	TAK / NIE
12. Rozwiązanie musi umożliwiać odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL) oraz z prawami dostępu. Funkcjonalność ta musi być możliwa do skonfigurowania przez administratora na etapie konfiguracji procesu przywracania danych.	TAK / NIE

	13. Rozwiązanie musi umożliwiać przywracanie plików pomiędzy różnymi systemami operacyjnymi i systemami plików (np. odtwarzanie danych plikowych Linux na systemie Windows).	TAK / NIE
Środowiska wirtualne		
Środowiska wirtualne	1. System musi wspierać kopię w trybie application-aware dla wszystkich wspieranych wirtualizatorów.	TAK / NIE
	2. System musi umożliwiać wykonywanie kopii maszyn wirtualnych z zastosowanie zaawansowanych metod transportu (HotAdd, SAN, LAN), w tym metodami LAN-Free, tj. takimi, które podczas wykonywania backupu nie obciążają interfejsów sieciowych maszyn wirtualnych.	TAK / NIE
	3. System kopii zapasowej musi wykorzystywać mechanizmy Change Block Tracking oraz Replica Change Tracking dla wspieranych przez producenta platformach wirtualizacyjnych.	TAK / NIE
	4. Rozwiązanie producenta musi być certyfikowane przez dostawcę platformy wirtualizacyjnej, tj. producent musi uczestniczyć w programie Technology Alliance Partner.	TAK / NIE
	5. System kopii zapasowej musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od	TAK / NIE

	rodzaju storage-u użytego do przechowywania kopii zapasowych.	
	6. Dla środowiska vSphere i Hyper-V rozwiązanie powinno umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).	TAK / NIE
	7. System kopii zapasowej musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere.	TAK / NIE
	8. System kopii zapasowej musi umożliwiać weryfikację odtwarzalności wirtualnych maszyn według własnego harmonogramu w dowolnym środowisku.	TAK / NIE
Aplikacje SaaS		
	1. Ochrona z tej samej konsoli dla Microsoft 365 minimum na poziomie, skrzynek pocztowych, onedrive, kontaktów, kalendarza.	TAK / NIE
	2. Rozwiązanie musi umożliwiać przywracanie danych Microsoft 365: do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku .pst oraz do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji)	TAK / NIE
	3. System musi umożliwiać granularne odtwarzanie danych, tj. pojedynczych plików z kopii obrazu dysku oraz pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365.	TAK / NIE
	4. System musi umożliwiać zabezpieczanie środowisk Git, w tym GitHub, GitLab oraz Bitbucket.	TAK / NIE

	5. System musi umożliwiać zabezpieczenie środowisk Jira	TAK / NIE
Licencjonowanie i wsparcie techniczne		
Licencjonowanie i wsparcie techniczne	1. Wszystkie linie supportu muszą być obsługiwane w języku polskim.	TAK / NIE
	2. Wsparcie techniczne musi być świadczone bezpośrednio przez główną siedzibę producenta.	TAK / NIE
	3. Możliwość zgłaszania ticketów supportowych bezpośrednio z poziomu interfejsu zarządzania w formie czatu.	TAK / NIE
	4. Producent wraz z rozwiązaniem musi udostępnić materiały samopomocowe w j. polskim (minimum dostęp do bazy wiedzy, materiałów wideo oraz kart produktów)	TAK / NIE
	5. Wsparcie techniczne musi umożliwiać korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego.	TAK / NIE
	6. W ramach wsparcia technicznego Zamawiający musi mieć dostęp do tzw. Dedicated Customer Success Managera, tj. osoby po stronie Dostawcy dedykowanej do obsługi zgłoszeń technicznych, doraźnej pomocy i bieżącej pomocy w utrzymania infrastruktury Zamawiającego.	TAK / NIE
	7. W ramach dokumentacji posprzedażowej Dostawca musi dostarczyć bezpośredni numer telefonu oraz adres e-mail do Dedicated Customer Success Managera.	TAK / NIE

	8. Licencje w ramach rozwiązania powinny pozwalać na zabezpieczenie: nielimitowanej ilości maszyn wirtualnych, nielimitowanej ilości serwerów fizycznych, nielimitowanej ilości stacji roboczych.	TAK / NIE
	9. Licencje powinny być dostępne w opcji wieczystej. Wsparcie techniczne nie powinno być wymagane dla poprawnego działania systemu.	TAK / NIE
	10. Wsparcie techniczne musi obowiązywać analogicznie przez cały okres trwania gwarancji NBD na warstwę sprzętową.	TAK / NIE
	11. Licencje powinny umożliwiać replikacje na własne zasoby.	TAK / NIE
	12. Licencje powinny umożliwiać korzystanie z przestrzeni chmurowej dostarczonej bezpośrednio przed producenta, min. 4,8TB przez cały okres trwania gwarancji NBD na warstwę sprzętową.	TAK / NIE
Anty-ransomware i bezpieczeństwo		
Anty-ransomware i bezpieczeństwo	1. System plików rozwiązania musi być odporny na ataki Ransomware (zapewnić ochronę przed szyfrowaniem end-to-end, kopie zapasowe nie mogą być nadpisywane - "niezmienny system plików").	TAK / NIE
	2. System powinien umożliwiać wykorzystanie wbudowanego menadżera haseł do przechowywania wszelkich sekretów (haseł, danych dostępowych, kluczy szyfrujących) wykorzystywanych przez System	TAK / NIE

	3. System powinien umożliwiać przywrócenie hasła głównego administratora w przypadku jego utraty.	TAK / NIE
Gwarancja na sprzęt		
	NBD na warstwę sprzętową do 18 czerwca 2028 roku	TAK / NIE
Wdrożenie		
Zakres wdrożenia	Dostawa montaż konfiguracja zgodnie z zaleceniami Zamawiającego	
Dokładny opis:	Przygotowanie szczegółowej dokumentacji wykonywania kopii – zawierającej procedury opisy i scenariusze – w odniesieniu do całości środowiska wirtualnego Zamawiającego. Weryfikacja dostępności docelowego środowiska na przyjęcie maszyn wirtualnych. Testowanie i Wdrażanie • Przetestowanie planów backupu i replikacji, aby upewnić się, że są one zgodne z oczekiwaniami i spełniają wymagania czasu przywracania. • Wdrożenie skonfigurowanych i przetestowanych planów na produkcji, monitorując ich wydajność i skuteczność.	

3. Termin realizacji zamówienia:

   3.1. Realizacja każdego zadania z 2.1 do 2.9 wynosi do 60 dni kalendarzowych.

4. Okres gwarancji: określone dokładnie przy danej pozycji
5. Warunki płatności:

   Zamawiający przewiduje płatności po wykonaniu każdej zadania w ramach realizacji zamówienia zgodnie z zaoferowaną stawką.

   Płatność przelewem 30 dni od dnia otrzymania prawidłowo wystawionych faktury VAT wraz z protokołem odbioru konkretnego zadania – protokół potwierdzony przez przedstawiciela Zamawiającego.

6. Inne istotne warunki zamówienia:

   Wymagania dla wdrożenia zostały opisane pod danym zadaniem.
7. Kryterium oceny ofert: cena 100%.

8. Zamawiający informuje, że:

1.1. Zadania 2.1 do 2.9 mogą zostać wyodrębnione jako odrębne części w ramach realizacji zamówienia,

1.2. w toku badania i oceny ofert może żądać od Wykonawcy pisemnych wyjaśnień dotyczących treści złożonej oferty lub innych składanych dokumentów lub oświadczeń. Wykonawca będzie zobowiązanych do przestawienia wyjaśnień w terminie określonym przez Zamawiającego pod rygorem odrzucenia oferty.

9. Sposób przygotowania oferty:

9.1. Ofertę należy sporządzić w języku polskim, na formularzu określonym w załączniku nr 1 do niniejszego zapytania ofertowego i złożyć za pośrednictwem bazy konkurencyjności.

9.2. **Do oferty należy dołączyć uzupełniony OPZ oraz załącznik nr 4 Wykaz oferowanego sprzętu, oprogramowania oraz licencji**

9.3. formularz oferty oraz załączniki muszą być podpisane elektronicznie przez osobę upoważnioną do reprezentowania Wykonawcy.

10. **Ofertę należy złożyć w terminie do dnia 24 września 2024 r. do godz. 12:00.**

Stanisław Józef Legierski

Elektronicznie podpisany przez Stanisław Józef Legierski
Data: 2024.09.16 15:13:25 +02'00'