



Fundusze  
Europejskie  
Polska Cyfrowa



Rzeczpospolita  
Polska

Unia Europejska  
Europejski Fundusz  
Rozwoju Regionalnego



AT.ZP.271.26.2024 ZCH.RMN

Załącznik nr 2 -4 do SWZ

**ZAMAWIAJĄCY:**

Miasto Słupsk  
Plac Zwycięstwa 3  
76-200 Słupsk

**FORMULARZ OFERTOWY - CZĘŚĆ 4**

**Dostawa fabrycznie nowego sprzętu i oprogramowania na potrzeby  
Miejskiego Ośrodka Pomocy Rodzinie w Słupsku**

*W postępowaniu o udzielenie zamówienia publicznego prowadzonego w trybie podstawowym bez przeprowadzenia negocjacji na podstawie art. 275 pkt 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2024 r., poz. 1320 ) pn. **Dostawa sprzętu i oprogramowania wzmacniającego odporność na zagrożenia cyfrowe w Urzędzie Miejskim w Słupsku oraz jednostkach podległych.***

**Dane Wykonawcy:**

Nazwa: .....

Siedziba: .....

Adres poczty elektronicznej: .....

Numer telefonu: .....

REGON - ....., NIP - .....

Status przedsiębiorcy (średni, mały, mikro - na mocy Rozporządzenia Komisji Europejskiej nr 364 z dnia 25.02.2004 r.) .....

*(w przypadku ubiegania się o udzielenie zamówienia przez wykonawców występujących wspólnie należy podać pełne dane wszystkich wykonawców oraz wskazać pełnomocnika)*

Oferuję wykonanie niniejszego zamówienia w zakresie i na zasadach określonych w SWZ:

Oferuję wykonanie przedmiotu zamówienia zgodnie ze specyfikacją warunków zamówienia

za cenę: brutto :.....zł

Zgodnie z poniższą tabelą:

Lp.	Nazwa	Ilość (w szt.)	Cena jednostkowa brutto (w zł)	Wartość brutto (kol. 3 x kol. 4) (w zł)
1	2	3	4	5
1	UPS z kartą sieciową	1		
2	UTM z licencją na 2 lata	1		
3	Switch z licencjami na 2 lata	3		
4	Licencje CAL per user	40		
5	Oprogramowanie antywirusowe z usługą chmurową	250		
6	Oprogramowanie do tworzenia oraz zarządzania kopiami bezpieczeństwa	1		
Suma (wartość oferty brutto):				

**- Termin realizacji zamówienia - w wymiarze\*:**

- \* do 14 dni od podpisania umowy - 40 pkt
- \* od 15 do 21 dni od podpisania umowy - 20 pkt
- \* od 21 do 30 dni od podpisania umowy - 0 pkt
- \*(właściwe podkreślić)

**Pozycja 1 - UPS z kartą sieciową**

Parametr	Parametr oferowany
Model zasilacza UPS**	
Rodzaj obudowy**	
Moc pozorna**	
Moc rzeczywista**	
Współczynnik mocy**	
Topologia**	
Liczba oraz typ gniazd wyjściowych**	
Typ gniazda wejściowego**	
Czas podtrzymania dla 100% obciążenia**	

Napięcie znamionowe**	
Tolerancja napięcia prostownika**	
Częstotliwość znamionowa**	
Tolerancja częstotliwości**	
Napięcie znamionowe wyjściowe**	
Częstotliwość wyjściowa**	
Baterie wymieniane przez użytkownika "na gorąco":	TAK/NIE*
Ochrona przed przeładowaniem	TAK/NIE*
Ochrona przed głębokim rozładowaniem	TAK/NIE*
Okresowy automatyczny test baterii	TAK/NIE*
Zimny start	TAK/NIE*
wymiary UPS**	
Poziom hałasu w odl. 1m**	

\* niepotrzebne skreślić

\*\* należy uzupełnić parametr

## Pozycja 2 - UTM z licencją na 2 lata

Parametr	Parametr oferowany
Model urządzenia UTM**	
W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS - istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.	TAK/NIE*
Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.	TAK/NIE*
Monitoring stanu realizowanych połączeń VPN.	TAK/NIE*
System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.	TAK/NIE*
System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: •16 portami Gigabit Ethernet RJ-45. •8 gniazdami SFP 1 Gbps. •2 gniazdami SFP+ 10 Gbps	TAK/NIE*

System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB	TAK/NIE*
System jest wyposażony w zasilanie AC.	TAK/NIE*
Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.	TAK/NIE*
Kontrola Aplikacji.	TAK/NIE*
Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.	TAK/NIE*
Ochrona przed malware.	TAK/NIE*
Ochrona przed atakami - Intrusion Prevention System.	TAK/NIE*
Kontrola stron WWW.	TAK/NIE*
Kontrola zawartości poczty - Antyspam dla protokołów SMTP, POP3.	TAK/NIE*
Zarządzanie pasmem (QoS, Traffic shaping).	TAK/NIE*
Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).	TAK/NIE*
Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.	TAK/NIE*
Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.	TAK/NIE*
Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.	TAK/NIE*
Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).	TAK/NIE*
Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.	TAK/NIE*

System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP.	TAK/NIE*
W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.	TAK/NIE*
Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.	TAK/NIE*
Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.	TAK/NIE*
Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.	TAK/NIE*
Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. • Amazon Web Services (AWS). • Microsoft Azure. • Cisco ACI. • Google Cloud Platform (GCP). • OpenStack. • VMware NSX. • Kubernetes.	TAK/NIE*
System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: • Wsparcie dla IKE v1 oraz v2. • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19, 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. • Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. • Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. • Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling” dla połączeń Client-to-Site.	TAK/NIE*

System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia 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 posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.	TAK/NIE*
Obsługa routingu statycznego.	TAK/NIE*
Obsługa Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).	TAK/NIE*
Obsługa protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPv2), OSPF (w tym OSPFv3), BGP oraz PIM.	TAK/NIE*
Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.	TAK/NIE*
ECMP (Equal cost multi-path) - wybór wielu równoważnych tras w tablicy routingu.	TAK/NIE*
BFD (Bidirectional Forwarding Detection).	TAK/NIE*
Obsługa monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.	TAK/NIE*
System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.	TAK/NIE*
SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).	TAK/NIE*
System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.	TAK/NIE*
System daje możliwość określania pasma dla poszczególnych aplikacji.	TAK/NIE*
System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.	TAK/NIE*
System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.	TAK/NIE*

Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).	TAK/NIE*
Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.	TAK/NIE*
System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.	TAK/NIE*
System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.	TAK/NIE*
System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).	TAK/NIE*
Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.	TAK/NIE*
System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.	TAK/NIE*
System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.	TAK/NIE*
Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.	TAK/NIE*
Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.	TAK/NIE*
Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.	TAK/NIE*
System chroni przed atakami na aplikacje pracujące na niestandardowych portach.	TAK/NIE*
Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.	TAK/NIE*
System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.	TAK/NIE*

Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).	TAK/NIE*
Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.	TAK/NIE*
Wykrywanie i blokowanie komunikacji C&C do sieci botnet.	TAK/NIE*
Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.	TAK/NIE*
Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.	TAK/NIE*
Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.	TAK/NIE*
Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.	TAK/NIE*
Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.	TAK/NIE*
Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).	TAK/NIE*
System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).	TAK/NIE*
Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne	TAK/NIE*
W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy	TAK/NIE*
Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.	TAK/NIE*
Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków - białe/czarne listy dla adresów URL.	TAK/NIE*
Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).	TAK/NIE*



Filtr WWW daje możliwość wykonania akcji typu „Warning” - ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.	TAK/NIE*
Funkcja Safe Search - przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.	TAK/NIE*
Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.	TAK/NIE*
System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.	TAK/NIE*
System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.	TAK/NIE*
System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.	TAK/NIE*
Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.	TAK/NIE*
Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.	TAK/NIE*
Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.	TAK/NIE*
Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.	TAK/NIE*
System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.	TAK/NIE*
System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.	TAK/NIE*

Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.	TAK/NIE*
Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.	TAK/NIE*
Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).	TAK/NIE*
Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.	TAK/NIE*
Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.	TAK/NIE*
W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.	TAK/NIE*
Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.	TAK/NIE*
Możliwość włączenia logowania per reguła w polityce firewall.	TAK/NIE*
System zapewnia możliwość logowania do serwera SYSLOG.	TAK/NIE*
Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.	TAK/NIE*
Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 24 miesięcy.	TAK/NIE*

System jest objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne. Obsługa zgłoszenia w tym zwrot uszkodzonego urządzenia do producenta, bez dodatkowych kosztów po stronie zamawiającego, realizowana przez producenta lub autoryzowanego dystrybutora przez okres wymaganej gwarancji.	TAK/NIE*
--	----------

\* niepotrzebne skreślić

\*\* należy uzupełnić parametr

### Pozycja 3 - Switch z licencjami na 2 lata

Parametr	Parametr oferowany
Model przełącznika**	
Wymiary urządzenia pozwalają na montaż w szafie rack 19".	TAK/NIE*
Obudowa nie wyższa niż 1U.	TAK/NIE*
Zasilanie AC 230V.	TAK/NIE*
24 porty GE RJ-45.	TAK/NIE*
4 porty 10 GE SFP+.	TAK/NIE*
Wbudowany port konsoli szeregowej do pełnego zarządzania.	TAK/NIE*
Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).	TAK/NIE*
Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.	TAK/NIE*
Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.	TAK/NIE*
Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.	TAK/NIE*
Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).	TAK/NIE*
Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.	TAK/NIE*

Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.		TAK/NIE*
Automatycznie wykonywane rewizje konfiguracji.		TAK/NIE*
Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.		TAK/NIE*
Obsługa Jumbo Frames.		TAK/NIE*
Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).		TAK/NIE*
Agregacja portów zgodna ze standardem 802.3ad.		TAK/NIE*
Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.		TAK/NIE*
Port-mirroring.		TAK/NIE*
Uwierzytelnianie 802.1x na poziomie portu.		TAK/NIE*
Uwierzytelnianie 802.1x w oparciu o adres MAC.		TAK/NIE*
W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).		TAK/NIE*
W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.		TAK/NIE*
W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.		TAK/NIE*
Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:	Centralne zarządzanie konfiguracją urządzenia.	TAK/NIE*
	Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania.	TAK/NIE*
	Centralne zarządzanie sieciami VLAN.	TAK/NIE*
	Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u.	TAK/NIE*

	Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.	TAK/NIE*
	Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.	TAK/NIE*
	Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.	TAK/NIE*
	Automatyczna detekcja i rekomendacje konfiguracji.	TAK/NIE*
	Przesyłanie logów na zewnętrzny serwer syslog.	TAK/NIE*
	Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.	TAK/NIE*
	Obsługa białych i czarnych list adresów MAC.	TAK/NIE*
	Wykrywanie aplikacji komunikujących się w sieci.	TAK/NIE*
Możliwe redundantne połączenie z elementami zarządzającymi.		TAK/NIE*

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

\* niepotrzebne skreślić

\*\* należy uzupełnić parametr

#### Pozycja 4 - Licencje CAL per user

Parametr	Parametr oferowany
Nazwa licencji dostępowej**	
Licencja dostępowa per użytkownik dedykowana do systemu operacyjnego posiadanego przez zamawiającego Windows Server Standard 2022	TAK/NIE*

\* niepotrzebne skreślić

\*\* należy uzupełnić paramet

#### Pozycja 5 - Oprogramowanie antywirusowe z usługą chmurową

Parametr	Parametr oferowany
Nazwa oprogramowania antywirusowego z usługą chmurową	TAK/NIE*
Rozwiązanie jest dostępne w chmurze producenta oprogramowania antywirusowego.	TAK/NIE*
Rozwiązanie umożliwia dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.	TAK/NIE*
Rozwiązanie jest zabezpieczone za pośrednictwem protokołu SSL.	TAK/NIE*
Rozwiązanie posiada mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.	TAK/NIE*
Rozwiązanie posiada możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.	TAK/NIE*

Rozwiązanie posiada możliwość zarządzania urządzeniami mobilnymi - MDM.	TAK/NIE*
Rozwiązanie posiada możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.	TAK/NIE*
Rozwiązanie posiada możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji posiada możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.	TAK/NIE*
Rozwiązanie posiada minimum 80 szablonów raportów, przygotowanych przez producenta.	TAK/NIE*
Rozwiązanie posiada możliwość tworzenia grup statycznych i dynamicznych komputerów.	TAK/NIE*
Grupy dynamiczne są tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki zawierają co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.	TAK/NIE*
Rozwiązanie posiada możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.	TAK/NIE*
Rozwiązanie wspiera systemy operacyjne Windows (Windows 10/Windows 11).	TAK/NIE*
Rozwiązanie wspiera architekturę ARM64.	TAK/NIE*
Rozwiązanie zapewnia wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.	TAK/NIE*
Rozwiązanie posiada wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.	TAK/NIE*
Rozwiązanie zapewnia wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.	TAK/NIE*
Rozwiązanie zapewni skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.	TAK/NIE*

Rozwiązanie zapewnia skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.	TAK/NIE*
Rozwiązanie zapewnia skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.	TAK/NIE*
Rozwiązanie posiada opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.	TAK/NIE*
Rozwiązanie integruje się z Intel Threat Detection Technology.	TAK/NIE*
Rozwiązanie zapewnia 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).	TAK/NIE*
Rozwiązanie zapewnia skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.	TAK/NIE*
Rozwiązanie posiada wbudowane dwa niezależne moduły heurystyczne - jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Istnieje możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie - z użyciem jednej lub obu metod jednocześnie.	TAK/NIE*
Rozwiązanie zapewnia 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.	TAK/NIE*
Rozwiązanie posiada 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.	TAK/NIE*



<p>Moduł HIPS posiada możliwość pracy w jednym z pięciu trybów:</p> <ul style="list-style-type: none"> <li>•tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,</li> <li>•tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,</li> <li>•tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,</li> <li>•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,</li> <li>•tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.</li> </ul>	TAK/NIE*
<p>Rozwiązanie jest 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.</p>	TAK/NIE*
<p>Funkcja, generująca taki log, posiada przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.</p>	TAK/NIE*
<p>Rozwiązanie posiada automatyczną, inkrementacyjną aktualizację silnika detekcji.</p>	TAK/NIE*
<p>Rozwiązanie posiada tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).</p>	TAK/NIE*
<p>Rozwiązanie posiada funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.</p>	TAK/NIE*
<p>Rozwiązanie posiada ochronę antyspamową dla programu pocztowego Microsoft Outlook.</p>	TAK/NIE*

<p>Zapora osobista rozwiązania pracuje w jednym z czterech trybów:</p> <ul style="list-style-type: none"> <li>•tryb automatyczny - rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,</li> <li>•tryb interaktywny - rozwiązanie pyta się o każde nowo nawiązywane połączenie,</li> <li>•tryb oparty na regułach - rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,</li> <li>•tryb uczenia się - rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator posiada możliwość konfigurowania czasu działania trybu.</li> </ul>	TAK/NIE*
Rozwiązanie jest wyposażone w moduł bezpiecznej przeglądarki.	TAK/NIE*
Przeglądarka automatycznie szyfruje wszelkie dane wprowadzane przez Użytkownika.	TAK/NIE*
Praca w bezpiecznej przeglądarce jest wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.	TAK/NIE*
Rozwiązanie jest wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.	TAK/NIE*
Rozwiązanie posiada możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.	TAK/NIE*
Rozwiązanie zapewnia ochronę przed zagrożeniami 0-day.	TAK/NIE*
W przypadku stacji roboczych rozwiązanie posiada możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.	TAK/NIE*
Rozwiązanie wspiera systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, Ubuntu Server 18.04 LTS i nowsze, Debian 10, Debian 11 i Debian 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux 8 oraz Amazon Linux.	TAK/NIE*
Rozwiązanie zapewnia ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami	TAK/NIE*

Rozwiązanie zapewnia wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.		TAK/NIE*
Rozwiązanie zapewnia możliwość skanowania dysków sieciowych typu NAS.		TAK/NIE*
Rozwiązanie posiada wbudowane dwa niezależne moduły heurystyczne - jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie posiada możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie - z użyciem jednej lub obu metod jednocześnie.		TAK/NIE*
Rozwiązanie wspiera automatyczną, inkrementacyjną aktualizację silnika detekcji.		TAK/NIE*
Rozwiązanie posiada możliwość wykluczania ze skanowania procesów.		TAK/NIE*
Rozwiązanie posiada możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.		TAK/NIE*
Dodatkowe wymagania dla ochrony serwerów Windows	Rozwiązanie posiada możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.	TAK/NIE*
	Rozwiązanie posiada system zapobiegania włamaniom działający na gości (HIPS).	TAK/NIE*
	Rozwiązanie wspiera skanowanie magazynu Hyper-V.	TAK/NIE*
	Rozwiązanie posiada funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.	TAK/NIE*

	Rozwiązanie 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.	TAK/NIE*
	Rozwiązanie automatycznie wykrywa usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.	TAK/NIE*
	Rozwiązanie posiada wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych	TAK/NIE*
	Rozwiązanie zapewnia możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.	TAK/NIE*
	Rozwiązanie posiada ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.	TAK/NIE*
Dodatkowe wymagania dla ochrony serwerów Linux:	Rozwiązanie pozwala, na uruchomienie lokalnej konsoli	TAK/NIE*

	Lokalna konsola administracyjna nie wymaga do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.	TAK/NIE*
	Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, w pełni wspiera rozwiązanie Dell EMC Isilon.	TAK/NIE*
	Rozwiązanie działa w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta zapewnia podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.	TAK/NIE*
Ochrona urządzeń mobilnych opartych o system Android	Rozwiązanie zapewnia skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.	TAK/NIE*
	Rozwiązanie zapewnia co najmniej 2 poziomy skanowania: inteligentne i dokładne.	TAK/NIE*
	Rozwiązanie zapewnia automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).	TAK/NIE*

	Rozwiązanie posiada możliwość skonfigurowania zaufanej karty SIM	TAK/NIE*
	Rozwiązanie zapewnia możliwość wystania na urządzenie komendy z konsoli centralnego zarządzania, która umożliwia: a. usunięcie zawartości urządzenia, b. przywrócenie urządzenia do ustawień fabrycznych, c. zablokowania urządzenia, d. uruchomienie sygnału dźwiękowego, e. lokalizację GPS.	TAK/NIE*
	Rozwiązanie zapewnia administratorowi podejrzenie listy zainstalowanych aplikacji.	TAK/NIE*
	Rozwiązanie posiada blokowanie aplikacji w oparciu o: a. nazwę aplikacji, b. nazwę pakietu, c. kategorię sklepu Google Play, d. uprawnienia aplikacji, e. pochodzenie aplikacji z nieznanego źródła.	TAK/NIE*

\* niepotrzebne skreślić

## Pozycja 6 - Oprogramowanie do tworzenia oraz zarządzania kopiami bezpieczeństwa

Parametr	Parametr oferowany
Nazwa oprogramowania do tworzenia oraz zarządzania kopiami bezpieczeństwa**	
Oprogramowanie z licencją umożliwiającą obciążenie w ilości 5 maszyn wirtualnych.	TAK/NIE*
Oprogramowanie jest produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt znajduje się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: <a href="https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions">https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions</a> i spełnia minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5.	TAK/NIE*
Oprogramowanie współpracuje z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji są dostępne na wszystkich wspieranych platformach wirtualizacyjnych.	TAK/NIE*
Oprogramowanie zapewnia tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.	TAK/NIE*
Oprogramowanie jest niezależne sprzętowo i umożliwia wykorzystanie dowolnej platformy serwerowej i dyskowej.	TAK/NIE*
Oprogramowanie tworzy "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków.	TAK/NIE*
Oprogramowanie posiada mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie skutkuje utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji.	TAK/NIE*
Oprogramowanie przechowuje danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie prowadzi do utraty możliwości odtworzenia backupu. Metadane deduplikacji są przechowywane w plikach backupu.	TAK/NIE*

Oprogramowanie zapewnia warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe	TAK/NIE*
Oprogramowanie pozwala na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie wspiera archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.	TAK/NIE*
Oprogramowanie wspiera niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.	TAK/NIE*
Oprogramowanie instaluje żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania.	TAK/NIE*
Oprogramowanie oferuje portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time).	TAK/NIE*
Oprogramowanie zapewnia możliwość delegacji uprawnień do odtwarzania na portalu.	TAK/NIE*
Oprogramowanie posiada możliwość integracji z innymi systemami poprzez wbudowane RESTful API.	TAK/NIE*
Oprogramowanie posiada wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.	TAK/NIE*
Oprogramowanie posiada wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji.	TAK/NIE*
Oprogramowanie posiada mechanizmy chroniące przed utratą hasła szyfrowania.	TAK/NIE*
Oprogramowanie posiada architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.	TAK/NIE*



Oprogramowanie posiada natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej.	TAK/NIE*
Oprogramowanie wymaga autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np. skasowanie backupu, dodanie kolejnego administratora).	TAK/NIE*
Oprogramowanie posiada integracje z systemami zarządzania kluczami szyfrującymi (KMS).	TAK/NIE*
Oprogramowanie posiada integracje z systemami typu SIEM.	TAK/NIE*
Oprogramowanie posiada asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji.	TAK/NIE*
Oprogramowanie wykorzystuje mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą są certyfikowane przez dostawcę platformy wirtualizacyjnej.	TAK/NIE*
Oprogramowanie wykorzystuje mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.	TAK/NIE*
Oprogramowanie oferuje możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta jest dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastoru.	TAK/NIE*
Oprogramowanie zapewnia tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Zapewnia też odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie wymaga użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność działa w środowisku VMware.	TAK/NIE*
Oprogramowanie posiada wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.	TAK/NIE*
Oprogramowanie wspiera kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592).	TAK/NIE*

Oprogramowanie posiada możliwość tworzenia retencji GFS (Grandfather-Father-Son).	TAK/NIE*
Oprogramowanie wspiera bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.	TAK/NIE*
Oprogramowanie wspiera BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność jest zapewniona dla repozytoriów opartych o linuxowy system plików XFS.	TAK/NIE*
Oprogramowanie posiada możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.	TAK/NIE*
Oprogramowanie posiada możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie posiada możliwość użycia plików kopii zapasowych jako źródła replikacji.	TAK/NIE*
Oprogramowanie posiada możliwość replikacji ciągłej, opartej o VMware VAI, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej posiada możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punktu w ramach ustalonego parametru RPO.	TAK/NIE*
Oprogramowanie umożliwia przechowywanie punktów przywracania dla replik.	TAK/NIE*
Oprogramowanie umożliwia wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding).	TAK/NIE*
Oprogramowanie wykorzystuje wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN).	TAK/NIE*

Oprogramowanie umożliwia jednocześnie uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność jest oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych. Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność umożliwia uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).	TAK/NIE*
Oprogramowanie pozwala na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja odbywa się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie realizuje taką migrację swoimi mechanizmami.	TAK/NIE*
Oprogramowanie pozwala na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere.	TAK/NIE*
Oprogramowanie pozwala na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana jest migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.	TAK/NIE*
Oprogramowanie umożliwia pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków.	TAK/NIE*
Oprogramowanie umożliwia pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.	TAK/NIE*
Oprogramowanie umożliwia odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie jest ograniczona wielkością i liczbą przywracanych plików.	TAK/NIE*
Oprogramowanie posiada możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.	TAK/NIE*

Oprogramowanie wspiera odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell.	TAK/NIE*
Oprogramowanie wspiera przywracanie plików z partycji Linux LVM.	TAK/NIE*
Oprogramowanie umożliwia szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.	TAK/NIE*
Oprogramowanie wspiera granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwala na odtworzenie haseł.	TAK/NIE*
Oprogramowanie wspiera granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie jest możliwe bezpośrednio do środowiska produkcyjnego.	TAK/NIE*
Oprogramowanie wspiera granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie jest możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur.	TAK/NIE*
Oprogramowanie wspiera granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie jest możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji.	TAK/NIE*
Oprogramowanie wspiera granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta jest dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.	TAK/NIE*
Oprogramowanie wspiera granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta jest dostępna dla baz uruchomionych w środowiskach Linux.	TAK/NIE*
Oprogramowanie wspiera granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji.	TAK/NIE*

Oprogramowanie posiada natywną integrację dla backupów wykonywanych poprzez Oracle RMAN.	TAK/NIE*
Oprogramowanie posiada natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle.	TAK/NIE*
Oprogramowanie posiada natywną integrację dla backupów wykonywanych poprzez MS SQL VDI.	TAK/NIE*
Oprogramowanie posiada natywną integrację dla backupów wykonywanych poprzez IBM Db2.	TAK/NIE*
Oprogramowanie wspiera także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN.	TAK/NIE*
Oprogramowanie daje możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność umożliwia uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) Dla VMware'a oprogramowanie pozwala na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.	TAK/NIE*
Oprogramowanie umożliwia weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy uwzględniają możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy są przeprowadzane bez interakcji z administratorem.	TAK/NIE*
Oprogramowanie umożliwia integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja jest zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.	TAK/NIE*
Oprogramowanie analizuje indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware.	TAK/NIE*

Oprogramowanie posiada możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania.	TAK/NIE*
Oprogramowanie, bazując na wyuczonym modelu maszynowym (machine learning) w locie wykrywa oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków.	TAK/NIE*
Oprogramowanie umożliwia dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.	TAK/NIE*

\* niepotrzebne skreślić

\*\* należy uzupełnić paramet

### **OŚWIADCZAMY, ŻE:**

- 1) zapoznaliśmy się z SWZ, nie wnosimy żadnych zastrzeżeń oraz uzyskaliśmy niezbędne informacje do przygotowania oferty,
- 2) wyżej wskazana cena obejmuje cały zakres zamówienia określony w SWZ i załącznikach, uwzględnia wszystkie wymagane opłaty oraz podatki i koszty niezbędne do zrealizowania całości przedmiotu zamówienia, bez względu na okoliczności i źródła ich powstania.
- 3) określone w SWZ wymagania stawiane wykonawcy oraz ogólne warunki umowy zostały przez nas zaakceptowane bez zastrzeżeń i zobowiązujemy się w przypadku wyboru naszej oferty do zawarcia umowy na warunkach, w terminie i miejscu wskazanym przez zamawiającego,
- 4) zaoferowany przedmiot jest zgodny z minimalnymi wymaganiami określonymi przez zamawiającego w „Opisie przedmiotu zamówienia”, a także w SWZ i warunkami opisanymi w ustawie Pzp,
- 5) zamówienie wykonamy w terminie wymaganym przez zamawiającego,
- 6) akceptujemy warunki płatności określone we wzorze umowy,
- 7) uważamy się za związanych niniejszą ofertą przez czas określony w SWZ,
- 8) Zamierzamy/ nie zamierzamy\* powierzyć podwykonawcom następujące części zamówienia:
  - a) ..... ,
  - b) ..... .

(Uwaga: nie wypełnienie tej części świadczyć będzie o braku podwykonawcy w realizacji zamówienia).

W przypadku powierzenia podwykonawcom wykonania części przedmiotu zamówienia należy również podać nazwę i adres podwykonawcy:

- a) ..... ,
- b) ..... ,

oraz wskazać procentową część zamówienia ....., jaka zostanie powierzona podwykonawcy lub podwykonawcom.

- 9) na podstawie art. 25 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy

95/46/WE (ogólne rozporządzenie o ochronie danych) oświadczam, że wdrażam odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń.

Załącznikami do niniejszej oferty, stanowiącymi jej integralną część, są:

.....  
.....  
.....  
.....

.....  
(miejscowość, data)

.....  
Podpis(y) osoby(osób) upoważnionej (ych) do podpisania  
niniejszej oferty w imieniu Wykonawcy(ów)\*

*\*Dokument należy wypełnić i podpisać kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.*