

AT.ZP.271.26.2024 ZCH.RMN

Załącznik nr 1-3 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA DLA CZĘŚCI III

Dostawa fabrycznie nowego sprzętu i oprogramowania oraz wdrożenie usług informatycznych na potrzeby Słupskiego Centrum Usług Wspólnych w Słupsku

Pozycja 1	
Przedmiot zamówienia:	Serwer
Ilość:	1 sztuka
Okres gwarancji producenta:	36 m-cy
Parametry	
Obudowa	<ul style="list-style-type: none"> Obudowa Rack o wysokości max 2U z możliwością instalacji do 8 dysków 3.5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze. Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	<ul style="list-style-type: none"> Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Chipset	<ul style="list-style-type: none"> Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	<ul style="list-style-type: none"> Zainstalowany jeden procesor 16-rdzeniowy klasy x86, min. 2.4GHz, dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 28 500 na dzień 01.08.2024 w teście PassMark dostępnym na stronie internetowej: https://www.cpubenchmark.net/
RAM	<ul style="list-style-type: none"> 64GB DDR4 RDIMM 3200MT/s – w kościach 32GB
Funkcjonalność pamięci RAM	<ul style="list-style-type: none"> Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing

Gniazda PCI	<ul style="list-style-type: none"> • minimum cztery sloty PCIe
Interfejsy sieciowe/SAS	<ul style="list-style-type: none"> • Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT
Dyski twarde	<ul style="list-style-type: none"> • Zainstalowane: <ul style="list-style-type: none"> ◦ 8x dysk SSD SATA 6Gb/s 512 o pojemności min. 960GB, Hot-Plug. • Zainstalowane dwa dyski M.2 SATA o pojemności min. 240GB Hot-Plug z możliwością konfiguracji RAID 1. • Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnek na dyski twarde.
Kontroler RAID	<ul style="list-style-type: none"> • Sprzętowy kontroler dyskowy, posiadający <ul style="list-style-type: none"> ◦ Min. 8GB nieulotnej pamięci cache, ◦ Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. • Wsparcie dla dysków samoszyfrujących.
Wbudowane porty	<ul style="list-style-type: none"> • Przednie: min. 1x VGA, min. 1x USB 2.0, min. 1x micro-USB dedykowane dla karty zarządzającej, • Tylne: min. 1x VGA, min. 2x USB w tym 1x USB 3.0,
Video	<ul style="list-style-type: none"> • Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Zasilacze	<ul style="list-style-type: none"> • Redundantne, Hot-Plug min.600W
Bezpieczeństwo	<ul style="list-style-type: none"> • Zatrzaszk górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twarde. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
Karta Zarządzania	<ul style="list-style-type: none"> • Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiającą: <ul style="list-style-type: none"> ◦ zdalny dostęp do graficznego interfejsu Web karty zarządzającej; ◦ zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); ◦ szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; ◦ możliwość podmontowania zdalnych wirtualnych napędów; ◦ wirtualną konsolę z dostępem do myszy, klawiatury; ◦ wsparcie dla IPv6;

	<ul style="list-style-type: none"> ○ wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; ○ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; ○ możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; ○ integracja z Active Directory; ○ możliwość obsługi przez dwóch administratorów jednocześnie; ○ wsparcie dla dynamic DNS; ○ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. ○ możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera ○ możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera <p>oraz z możliwością rozszerzenia funkcjonalności o:</p> <ul style="list-style-type: none"> ○ Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej ○ Przesyłanie danych telemetrycznych w czasie rzeczywistym ○ Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze ○ Automatyczna rejestracja certyfikatów (ACE)
Oprogramowanie do zarządzania	<ul style="list-style-type: none"> ● Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: <ul style="list-style-type: none"> ○ Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych ○ integracja z Active Directory ○ Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta ○ Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish ○ Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram ○ Szczegółowy opis wykrytych systemów oraz ich komponentów ○ Możliwość eksportu raportu do CSV, HTML, XLS, PDF ○ Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. ○ Grupowanie urządzeń w oparciu o kryteria użytkownika ○ Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji ○ Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach ○ Szybki podgląd stanu środowiska ○ Podsumowanie stanu dla każdego urządzenia ○ Szczegółowy status urządzenia/elementu/komponentu ○ Generowanie alertów przy zmianie stanu urządzenia.

	<ul style="list-style-type: none"> ○ Filtry raportów umożliwiające podgląd najważniejszych zdarzeń ○ Integracja z service desk producenta dostarczonej platformy sprzętowej ○ Możliwość przejęcia zdalnego pulpitu ○ Możliwość podmontowania wirtualnego napędu ○ Kreator umożliwiający dostosowanie akcji dla wybranych alertów ○ Możliwość importu plików MIB ○ Przesyłanie alertów „as-is” do innych konsol firm trzecich ○ Możliwość definiowania ról administratorów ○ Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów ○ Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) ○ Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta ○ Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów ○ Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. ○ Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. ○ Wdrażanie serwerów, rozwiązań modułarnych oraz przełączników sieciowych w oparciu o profile ○ Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. ○ Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. ○ Zdalne uruchamianie diagnostyki serwera. ○ Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. ○ Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Certyfikaty	<ul style="list-style-type: none"> • Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • 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 nie-

	<p>bezpieczne 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 dokument potwierdzający spełnianie wymogu.</p> <ul style="list-style-type: none"> • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.
Dokumentacja użytkownika	<ul style="list-style-type: none"> • Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	<ul style="list-style-type: none"> • Zamawiający wymaga zapewnienia przez wykonawcę usługi wsparcia technicznego z zakresu wdrażanej technologii na okres 7 lat. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. • Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy (dla krytycznych zgłoszeń serwisowych) • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. • Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. • Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. • Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. • Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie

	<p>zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego</p> <ul style="list-style-type: none"> • Zamawiający wymaga od podmiotu realizującego dostawę, serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń. • Zamawiający wymaga, żeby Serwis urządzeń był realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
--	---

Pozycja 2	
Przedmiot zamówienia:	Licencja na serwerowy system operacyjny
Ilość:	2 sztuki
Parametry	
Opis licencji	Licencja na serwerowy system operacyjny która zapewni poniżej opisane funkcjonalności dla serwera posiadającego 16 rdzeni procesora. Zamawiający wymaga dostarczenia licencji imiennej (na organizację), umożliwiającej przeniesienie w ramach programu licencji zbiorczych. Forma licencjonowania powinna zapewniać dostęp do platformy pozwalającej zarządzać posiadanymi licencjami, pobierać pakiety instalacyjne, uzyskiwać klucze licencyjne. Nie dopuszcza się licencjonowania typu OEM (przypisanego do maszyny fizycznej).
Minimalne parametry	<ul style="list-style-type: none"> • Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego (SSO) w środowisku fizycznym i czterech wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. • Możliwość wykorzystania, do 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. • Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. • Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych. • Możliwość migracji maszyn wirtualnych z możliwością kompresji danych, bez zatrzymywania ich pracy, między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. • Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. • Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany

	<p>procesorów bez przerywania pracy.</p> <ul style="list-style-type: none"> • 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. • Wbudowane wsparcie instalacji i pracy na wolumenach, które: a. pozwalają na zmianę rozmiaru w czasie pracy systemu, b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d. umożliwiają zdefiniowanie list kontroli dostępu (ACL). • Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. • Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. • Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET • Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. • Wbudowana zaporę internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. • Graficzny interfejs użytkownika. • Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, • Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. • Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). • Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. • Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. • Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, 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, urządzenia sieciowe), z możliwością wykorzystania następujących funkcji: Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
--	--

	<p>Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza, Ustanawianie praw dostępu do określonych zasobów dla użytkowników nie dołączonych do domeny, Zdalna dystrybucja oprogramowania na stacje robocze, Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: - dystrybucję certyfikatów poprzez http, -konsolidację CA dla wielu lasów domeny, -konsolidację CA dla wielu lasów domeny, szyfrowanie plików i folderów, Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów, Serwis udostępniania stron WWW, Wsparcie dla protokołu IP w wersji 6 (IPv6), Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,</p> <ul style="list-style-type: none"> • Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: <ul style="list-style-type: none"> -Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, - Obsługi ramek typu jumbo frames dla maszyn wirtualnych, - Obsługi 4-KB sektorów dysków, - Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, • Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, • Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) • 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. • Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath). • Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. • Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. • Sterowniki i dokumentacja od producenta sprzętu
--	---

- Oprogramowanie musi być dostarczone w najnowszej wersji

Pozycja 3	
Przedmiot zamówienia:	Licencje dostępne do serwerowego systemu operacyjnego
Ilość:	40 sztuk
Parametry	
Opis	Licencja dostępowa per urządzenie dedykowana do zamawianego serwerowego systemu operacyjnego. Forma licencjonowania powinna zapewniać dostęp do platformy pozwalającej zarządzać posiadanymi licencjami, pobierać pakiety instalacyjne, uzyskiwać klucze licencyjne.

Pozycja 4	
Przedmiot zamówienia:	Switch z licencjami na 2 lata
Ilość:	2 sztuki
Okres gwarancji producenta:	24 m-cy
Parametry	
Parametry fizyczne platformy	• Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. • Zasilanie AC 230V.
Interfejsy sieciowe - wymagania minimalne	1. Wymaganiem jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości: a) 24 porty GE RJ-45. e) 4 porty 10 GE SFP+.
Zarządzanie	• Wbudowany port konsoli szeregowej do pełnego zarządzania. • Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). • 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. Wymagane funkcje • Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. • Obsługa Jumbo Frames. • Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). • Agregacja portów zgodna ze standardem 802.3ad. • Obsługa co

	najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q. • 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.
Interfejs komunikacyjnyDodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC	1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej: • Centralne zarządzanie konfiguracją urządzenia • Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania • Centralne zarządzanie sieciami VLAN. • Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u • Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.. • Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej. • Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego. • Automatyczna detekcja i rekomendacje konfiguracji. • Przesyłanie logów na zewnętrzny serwer syslog. • Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników. • Obsługa białych i czarnych list adresów MAC. • Wykrywanie aplikacji komunikujących się w sieci. 2. Musi być możliwe redundantne połączenie z elementami zarządzającymi. 3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.
Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa	• System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym. • System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.
Gwarancja oraz wsparcie	System musi być objęty 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.
Przełącznik sieciowy	W ramach postępowania wymagany jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.

Pozycja 5	
Przedmiot zamówienia:	Serwer zarządzania kopiami
Ilość:	1 sztuka
Okres gwarancji producenta:	36 m-cy

Parametry	
Obudowa	<ul style="list-style-type: none"> • tower
Płyta główna	<ul style="list-style-type: none"> • Płyta główna z możliwością zainstalowania jednego procesora. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • na płycie głównej powinny znajdować się minimum 2 sloty przeznaczonych do instalacji pamięci
Procesor	<ul style="list-style-type: none"> • Zainstalowany jeden procesor 10-rdzeniowy klasy x86, min. 1.8GHz, dedykowany do pracy z zaofertowanym serwerem umożliwiający osiągnięcie wyniku min. 25 000 na dzień 01.08.2024 w teście PassMark dostępnym na stronie internetowej: https://www.cpubenchmark.net/
Pamięć RAM	<ul style="list-style-type: none"> • 16GB DDR5 4400 MT/s
Dysk twardy	<ul style="list-style-type: none"> • 1TB SSD
Interfejs sieciowy	<ul style="list-style-type: none"> • 1x 1GE RJ45
Porty	<ul style="list-style-type: none"> • 1x USB 3.2 Gen1 Type-C • 3x USB 3.2 Gen1 Type-A • 4x USB 2.0 • 1x Audio • 1x DP • 1x HDMI
Zasilanie	<ul style="list-style-type: none"> • 180W PSU, 85% Efficient, 80 PLUS Bronze
Warunki gwarancji	<ul style="list-style-type: none"> • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. • Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy (dla krytycznych zgłoszeń serwisowych) • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. • Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. • Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. • Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. • Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cyberne-

	<p>tycznego</p> <ul style="list-style-type: none"> • Zamawiający wymaga od podmiotu realizującego serwis, dostawę lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń.
--	--

Pozycja 6	
Przedmiot zamówienia:	Dysk do serwera zarządzania kopiami oraz serwera plików NAS
Ilość:	5 sztuk
Okres gwarancji producenta:	36 m-cy
Parametry	
Przeznaczenie	Dysk dedykowany do systemów NAS oraz do pracy w trybie ciągłym.
Pojemność	8TB
Wymiary	3,5"
TBW	180TB

Pozycja 7	
Przedmiot zamówienia:	Serwer plików NAS do przechowywania kopii bezpieczeństwa
Ilość:	1 sztuka
Okres gwarancji producenta:	36 m-cy
Parametry	
Procesor	Zainstalowany jeden procesor 4-rdzeniowy klasy ARM, min. 1.7GHz, dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 1100 na dzień 01.08.2024 w teście PassMark dostępnym na stronie internetowej: https://www.cpubenchmark.net/
Pamięć RAM	2 GB, DDR4
Obudowa	Rack 1U, z 4 wnękami na dyski
Akcesoria montażowe	Szyny montażowe dedykowane do serwera
Interfejs sieciowy	<ul style="list-style-type: none"> • 2 x 10/100/1000/2500 Mbit/s • 2 x 10Gbit/s SFP+
Gniazda rozszerzeń	1 x PCIe 2.0 x 2

Pozycja 8	
Przedmiot zamówienia:	Oprogramowanie do tworzenia oraz zarządzania kopiami bezpieczeństwa
Ilość:	1 sztuka
Parametry	
Wymagania ogólne	<p>Licencja dostępowa per użytkownik systemu operacyjnego posiadanego przez zamawiającego - Windows Server Standard 2022 Oprogramowanie z licencją umożliwiającą obciążenie w ilości 5 maszyn wirtualnych.</p> <p>Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner:</p> <p>https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5,</p> <p>Oprogramowanie musi współpracować 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 muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej</p> <p>Oprogramowanie musi zapewniać 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.</p> <p>Całkowite koszty posiadania</p>

	<p>Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej</p> <p>Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków</p> <p>Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji</p> <p>Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.</p> <p>Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.</p> <p>Oprogramowanie musi pozwalać 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 musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.</p> <p>Oprogramowanie musi wspierać niezmiennność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.</p> <p>Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania</p> <p>Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time)</p> <p>Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu</p> <p>Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API</p> <p>Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji</p> <p>Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiegokolwiek funkcjonalności wymienionej w tej specyfikacji</p> <p>Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania</p> <p>Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.</p> <p>Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej</p> <p>Oprogramowanie musi wymagać autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np skasowanie backupu, dodanie kolejnego administratora)</p> <p>Oprogramowanie musi posiadać integracje z systemami zarządzania kluczami szyfrującymi (KMS)</p>
--	---

	<p>Oprogramowanie musi posiadać integracje z systemami typu SIEM</p> <p>Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji.</p>
Wymagania RPO	<p>Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej</p> <p>Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.</p> <p>Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastora</p> <p>Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware.</p> <p>Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.</p> <p>Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592).</p> <p>Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)</p> <p>Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.</p> <p>Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.</p> <p>Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.</p> <p>Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.</p> <p>Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punktu w ramach ustalonego parametru RPO.</p> <p>Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik</p> <p>Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)</p> <p>Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)</p>
Wymagania RTO	<p>Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn</p>

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, 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 powinna umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)

Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami

Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere

Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.

Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków

Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.

Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików

Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.

Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell

Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM

Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.

Oprogramowanie musi wspierać 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 pozwalać na odtworzenie haseł.

Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego.

Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli,

	<p>widoków oraz procedur.</p> <p>Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji.</p> <p>Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.</p> <p>Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.</p> <p>Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji</p> <p>Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN</p> <p>Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle</p> <p>Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI</p> <p>Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2</p> <p>Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN</p> <p>Ograniczenie ryzyka</p> <p>Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)</p> <p>Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.</p> <p>Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem</p> <p>Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.</p> <p>Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware</p> <p>Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania</p> <p>Oprogramowanie, bazując na wyuczonym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware,</p>
--	--

	ransomware) oraz cyberataków Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
--	--

Pozycja 9		
Przedmiot zamówienia:		Usługa wdrożenia serwera i oprogramowania zgodnie z wymogami KRI
Ilość:		1 sztuk
Parametry		
Zakres usługi	Konfiguracja podsieci VLAN	<p>Wdrożenie przełączników sieciowych klasy enterprise. Aktywacja i rejestracja wszystkich komponentów (urządzenia i licencję), przypisanie licencji do emaila wskazanego przez Zamawiającego. Wdrożenie przełączników sieciowych klasy enterprise w taki sposób aby były zarządzane, aktualizowane poprzez interfejs UTM. Logi z przełączników muszą być gromadzone na urządzeniu UTM. Aktualizacja do najnowszych wersji oprogramowania. Wydzielenie podsieci VLAN, w tym sieci bezprzewodowych zgodnie z wskazaniami Zamawiającego. Zabezpieczenie ruchu we wszystkich podsieciach zgodnie z wymaganiami Zamawiającego. Integracja z Istniejącym środowiskiem IT. Wdrożenie VPN na urządzeniu UTM i konfiguracja polityk w sposób nie wymagający osobnej konfiguracji z poziomu interfejsów przełączników sieciowych – konfiguracja, integracja z GPO i zabezpieczenie Tuneli VPN. Wdrożenie wydzielonej – galwanicznej sieci zarządzającej systemami IT. Wdrożenie wykonywane na miejscu. Dwuletnie nieodpłatne wsparcie ze strony pracowników Wykonawcy w w/w zakresie. Przez 24 miesiące od wykonania usługi wdrożenia, w przypadku wystąpienia błędów wdrożeniowych - Wykonawca wykona naprawę zdalnie w czasie do 5 godzin, jeżeli nie będzie możliwości wykonania naprawy zdalnie, pracownik Wykonawcy dojedzie w czasie do 24 godzin do siedziby Zamawiającego, gdzie dokona naprawy na miejscu. Wykonawca udostępni kontakt email i telefoniczny. Czas jest liczony od wysłania e-mail przez Zamawiającego.</p> <p>Usługa musi zawierać wymagane konfiguracje i zostać wykonana zgodnie z:</p> <ul style="list-style-type: none"> • Polską Normą PN-ISO/IEC 27002, • Rozporządzeniem Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. <p>Prace zostaną zakończone protokołem</p>
	Wdrożenie Serwera	Fizyczny montaż serwera w siedzibie Zamawiającego. Podłączanie do instancji elektrycznej w tym urządzeń podtrzymywania zasilania. Konfiguracja z



	wraz z kontrolerem zdalnego dostępu	<p>systemami podtrzymywania zasilania Zamawiającego. Montaż serwera z przewodnikami musi zostać wykonany w sposób umożliwiający wysunięcie w czasie pracy. Wszystkie elementy instalacyjne w tym kable sieciowe, kable elektryczne, adaptory zasilania, itp. zapewnia Wykonawca w cenie usługi. Wdrożenie zintegrowanego modułu zdalnego zarządzania serwerem. Aktywacja i rejestracja wszystkich komponentów (urządzenia i licencję), przypisanie licencji do emaila wskazanego przez Zamawiającego. Aktualizacja do najnowszej wersji oprogramowania. Zapewnienie konfiguracji wszystkich parametrów w tym macierzy dyskowych zgodnie z wymogami prawa i wytycznymi Zamawiającego. Podłączenie do podsieci zgodnie z wymaganiami Zamawiającego. Integracja z istniejącym środowiskiem IT. Dwuletnie nieodpłatne wsparcie ze strony pracowników Wykonawcy w w/w zakresie. Przez 24 miesiące od wykonania usługi wdrożenia, w przypadku wystąpienia błędów wdrożeniowych - Wykonawca wykona naprawę zdalnie w czasie do 5 godzin, jeżeli nie będzie możliwości wykonania naprawy zdalnie, pracownik Wykonawcy dojedzie w czasie do 24 godzin do siedziby Zamawiającego, gdzie dokona naprawy na miejscu. Wykonawca udostępni kontakt email i telefoniczny. Czas jest liczony od wysłania e-mail przez Zamawiającego.</p> <p>usługa musi zawierać wymagane konfiguracje i zostać wykonana zgodnie z:</p> <ul style="list-style-type: none"> • Polską Normą PN-ISO/IEC 27002, • Rozporządzeniem Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. <p>Prace zostaną zakończone protokołem</p>
	Wdrożenie funkcji hypervisor	<p>Fizyczna i techniczna instalacja oprogramowania hypervisor w siedzibie Zamawiającego wraz z pełną konfiguracją opisaną poniżej. Migracja starego środowiska na nowy Hypervisor. Migracja musi odbyć się z rozbiciem na poszczególne serwery wirtualne zgodnie z wskazaniami Zamawiającego. Proces przejścia z starego na nowy serwer trzeba wykonać po godzinie pracy instytucji - aby zachować ciągłość pracy Zamawiającego. Wdrożenie wydzielonej – galwanicznej sieci wirtualnej - zarządzającej systemami IT do wykonywania kopii serwera wirtualnego. Wdrożenie sieci wirtualnych i integracja z UTM zamawiającego. Wdrożenie wykonywane w siedzibie Zamawiającego . Usługi muszą być zgodne z:</p> <ul style="list-style-type: none"> • Polską Normą PN-ISO/IEC 27002, • Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. <p>Prace zostaną zakończone protokołem</p>
	Integracja oprogramow	<ul style="list-style-type: none"> • Analiza środowiska IT Zamawiającego: Przegląd i analiza aktualnej infrastruktury IT w celu dopasowania konfiguracji usługi zarządzania

	<p>ania zarządzające go zasilaczem UPS z funkcją hypervisor</p>	<p>zasilaniem.</p> <ul style="list-style-type: none"> • Instalacja niezbędnego oprogramowania: instalacja wszystkich komponentów programowych w tym ich rejestracja i aktywacja na dane Zamawiającego. • Konfiguracja hypervisor. Dostosowanie ustawień hypervisor do współpracy z urządzeniem UPS, w tym skonfigurowanie protokołów komunikacyjnych i automatycznych procedur wyłączania oraz załączania serwera. • Integracja z istniejącą infrastrukturą IT: Podłączenie urządzenia UPS do istniejącej infrastruktury sieciowej i zapewnienie pełnej integracji z systemami zarządzania IT. • Automatyzacja procesów zarządzania zasilaniem: Konfiguracja procedur automatycznego wyłączania serwera w przypadku awarii zasilania oraz jego ponownego uruchamiania po przywróceniu zasilania, zgodnie z wymaganiami Zamawiającego. • Testowanie i optymalizacja: Przeprowadzenie testów funkcjonalnych i obciążeniowych, aby upewnić się, że wszystkie procesy automatyzacji działają poprawnie. Optymalizacja konfiguracji na podstawie wyników testów. • Miejsce wykonywania usług: Wszystkie prace muszą zostać wykonane w siedzibie zamawiającego. <p>Wsparcie techniczne:</p> <ul style="list-style-type: none"> • Zapewnienie wsparcia technicznego przez okres 24 miesięcy od daty zakończenia wdrożenia. W przypadku awarii, wykonawca zapewni naprawę zdalną w czasie do 5 godzin, a w razie konieczności, fizyczną naprawę na miejscu w ciągu 24 godzin. <p>Kontakt:</p> <ul style="list-style-type: none"> • Wykonawca udostępni kontakt e-mail i telefoniczny do zgłaszania awarii i problemów technicznych. Czas reakcji liczony od momentu wysłania zgłoszenia przez Zamawiającego. <p>Zgodność z normami i przepisami:</p> <ul style="list-style-type: none"> • Wykonanie usługi zgodnie z Polską Normą PN-ISO/IEC 27002. • Zgodność z Rozporządzeniem Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności określającym minimalne wymagania dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalne wymagania dla systemów teleinformatycznych. <p>Prace zostaną zakończone protokołem odbioru, który będzie zawierał zestawienie wykonanych operacji oraz opis konfiguracji.</p>
--	---	---

Pozycja 10	
Przedmiot zamówienia:	Agregacja logów z systemów krytycznych (UTM, usługa katalogowa AD)
Ilość:	1 sztuka
Okres świadczenia usługi	24 miesiące

Parametry	
Opis	Przedmiot zamówienia stanowi świadczenie usług przechowywania logów systemowych pochodzących z Kontrolera Domeny i urządzenia UTM Zamawiającego, z wykorzystaniem bezpiecznego połączenia VPN. Usługa ta ma na celu zapewnienie bezpieczeństwa oraz możliwości rozliczenia działań zgodnie z obowiązującymi wymogami prawnymi.
Zakres usługi	Konfiguracja i zarządzanie połączeniem VPN, umożliwiające przesyłanie logów z systemów Zamawiającego do systemów IT przechowujące dane u Wykonawcy. Połączenie musi spełniać następujące kryteria: <ul style="list-style-type: none"> • Komunikacja sieciowa możliwa tylko w kierunku od Zamawiającego do Wykonawcy. • Zapobieganie inicjowaniu połączenia od Wykonawcy do Zamawiającego. • Wykluczenie możliwości routowania z VPN do wewnętrznych sieci komputerowych Zamawiającego.
	Zarejestrowane logi muszą zawierać szczegółowe informacje dotyczące: <ul style="list-style-type: none"> • dostępu użytkowników do systemów lub zbiorów danych, • zmian w konfiguracji zabezpieczeń, • dostępu do informacji objętych ochroną prawną, zdarzeń systemowych.
	Przechowywanie logów przez okres co najmniej 24 miesiące, nawet po zakończeniu świadczenia usługi. Wykonawca musi zapewnić przechowywanie wcześniej zebranych logów przez 24 miesiące od ich zebrania niezależnie od zaprzestania świadczenia usługi. Zamawiający może zażądać usunięcia zebranych logów poprzez przekazanie dokumentu podpisanego przez osobę uprawnioną.
Zgodność	Wykonawca dostarcza rozwiązania techniczne gwarantujące, zabezpieczenie logów przed edycją i nieautoryzowanym usunięciem.
	Usługa musi być zgodna z: <ul style="list-style-type: none"> • Polską Normą PN-ISO/IEC 27002, • Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, które określa minimalne wymagania dla rejestrów publicznych i wymiany informacji w formie elektronicznej, a także minimalne wymagania dla systemów teleinformatycznych

Pozycja 11	
Przedmiot zamówienia:	UPS z kartą sieciową
Ilość:	1 sztuka
Okres gwarancji producenta:	36 m-cy
Parametry	
Obudowa	Uniwersalna tower/rack max. 2U
Moc, napięcia, gniazda, ochrony, dodatkowe dane	Moc pozorna: 3000 VA Moc rzeczywista: 3000 W Współczynnik mocy: 1

	<p>Topologia (klasyfikacja IEC 62040-3): line-interactive Liczba, typ gniazd wyjściowych: 8 x C13, 2 x C19 Typ gniazda wejściowego: Gniazdo C20 Czas podtrzymania dla 100% obciążenia: 3 minuty Napięcie znamionowe: 230 V Tolerancja napięcia prostownika: 160 - 294 V (regulowana do 150 - 294 V) Częstotliwość znamionowa: 50/60 Hz autodetekcja Tolerancja częstotliwości: 47 - 70 Hz (system 50 Hz); 56,5 - 70 Hz (system 60 Hz); 40 Hz w trybie niskiej czułości Napięcie znamionowe wyjściowe: 230 V (domyślnie) / 200/208/220/240 V Częstotliwość wyjściowa: 50/60 Hz Baterie wymieniane przez użytkownika "na gorąco": Tak Ochrona przed przeładowaniem: Tak Ochrona przed głębokim rozładowaniem: Tak Okresowy automatyczny test baterii: Tak Zimny start: Tak Max. wymiary UPS (szer. x gł. x wys. w mm): 438 x 603 x 85,5 Poziom hałasu w odl. 1m: < 45 dBA</p>
System zarządzania pracą baterii	<p>System nieciągłego ładowania baterii. Do oferty dołączyć należy opis algorytmu ładowania nieciągłego baterii. W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni. Opis powinien być materiałem firmowym producenta lub musi być przez niego potwierdzony.</p>
Interfejs komunikacyjny	<p>USB, RS232 DB-9 żeński (HID), miniport wyłącznik awaryjny RPO, miniport wyłącznik ON/OFF, listwa zaciskowa dla przełącznika wyjściowego</p>
Panel sterowania z wyświetlaczem LCD	<p>Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPS'a) ze wskazaniem chwilowego poziomu obciążenia i poziomu naładowania baterii, z możliwością sterowania poszczególnymi segmentami odbiorów oraz pomiarem sprawności i zużycia energii przez odbiory (w kWh)</p>
Przyciski sterujące i wskaźniki diodowe LED	<p>Poziomy rząd przycisków sterowania; Poziomy rząd wskaźników stanu: trybu normalnego (zielony), trybu baterijnego (żółty), usterki (czerwony); Pasek LED sygnalizujący stan; sygnalizator akustyczny (awaria, serwis, niski stan naładowania baterii, przeciążenie); przycisk Escape (anulowanie); przyciski funkcyjne (przewijanie w górę i w dół); przycisk Enter (potwierdzający)</p>
Wypożyczenie	<p>UPS 3 kVA, instrukcja obsługi, instrukcja bezpieczeństwa; przewód zasilający; kabel RS232; kabel USB; karta SNMP; uchwyty kablowe; podstawki do montażu pionowego (wieża); 2 przewody IEC 10 A; zestaw szyn montażowych do szafy 19" Karta SNMP "cyberbezpieczeństwo (certyfikaty UL 2900-2-2 /IEC62443 /HTTPS/MQTT/NDIS/LDAP/NVD//SSH/PKI, pakiet szyfrów TLS 1.2 z minimum SHA256)"; certyfikaty CA i PKI; prędkość gigabitowa (half-duplex, full-duplex); różne poziomy nadawania dostępu do konta administratora lub użytkownika</p>
Dołączone oprogramowanie	<p>Do bezpiecznego zamykania systemów operacyjnych przy wyczerpaniu baterii (minimum: Windows: 10, 2000, XP, 2003, Vista, Server 2008, 7; Linux: Red Hat, Fedora Core, SuSE; UNIX: AIX, HP-UX, SCO, SGI Irix, Mac OS, Sun Solaris; Novell NetWare do v 6.5). Oprogramowanie musi mieć możliwość wyboru polskiej wersji językowej.</p>
Zgodność z normami UE	<p>Deklaracja zgodności producenta</p>

Dodatkowe certyfikaty	ISO9001 producenta urządzenia
-----------------------	-------------------------------

Pozycja 12	
Przedmiot zamówienia:	Oprogramowanie antywirusowe z usługą chmurową
Ilość:	40 sztuk
Parametry	
Administracja zdalna w chmurze	<ol style="list-style-type: none"> 1.Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego. 2.Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW. 3.Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL. 4.Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. 5.Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. 6.Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM. 7.Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 8.Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak. 9.Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta. 10.Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. 11.Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. 12.Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.
Ochrona stacji roboczych	<ol style="list-style-type: none"> 1.Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). 2.Rozwiązanie musi wspierać architekturę ARM64. 3.Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4.Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. 5.Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.

	<p>6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.</p> <p>7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.</p> <p>8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.</p> <p>9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.</p> <p>10. Rozwiązanie musi integrować się z Intel Threat Detection Technology.</p> <p>11. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).</p> <p>12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.</p> <p>13. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.</p> <p>14. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.</p> <p>15. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.</p> <p>16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:</p> <ul style="list-style-type: none"> • tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, • tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, • tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, • tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, • tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach. <p>17. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.</p> <p>18. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów</p>
--	--

	<p>filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.</p> <p>19.Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.</p> <p>20.Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).</p> <p>21.Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.</p> <p>22.Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.</p> <p>23.Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:</p> <ul style="list-style-type: none"> •tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące, •tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie, •tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora, •tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu. <p>24.Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.</p> <p>25.Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.</p> <p>26.Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.</p> <p>27.Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.</p> <p>28.Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.</p> <p>29.Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.</p> <p>30.W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.</p>
Ochrona serwera	<p>1.Rozwiązanie musi wspierać 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.</p> <p>2.Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.</p> <p>3.Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.</p> <p>4.Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.</p> <p>5.Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie</p>

	<p>musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.</p> <p>6.Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.</p> <p>7.Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.</p> <p>8.Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.</p> <p>Dodatkowe wymagania dla ochrony serwerów Windows:</p> <p>9.Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.</p> <p>10.Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).</p> <p>11.Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.</p> <p>12.Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.</p> <p>13.Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.</p> <p>14.Rozwiązanie musi automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.</p> <p>15.Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.</p> <p>16.Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.</p> <p>17.Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.</p> <p>Dodatkowe wymagania dla ochrony serwerów Linux:</p> <p>18.Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.</p> <p>19.Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.</p> <p>20.Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.</p> <p>21.Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonoego mikro-serwisu.</p>
Ochrona urządzeń mobilnych opartych o system Android	<p>1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.</p> <p>2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.</p> <p>3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy</p>

	<p>urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).</p> <p>4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.</p> <p>5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:</p> <ol style="list-style-type: none"> usunięcie zawartości urządzenia, przywrócenie urządzenia do ustawień fabrycznych, zablokowania urządzenia, uruchomienie sygnału dźwiękowego, lokalizację GPS. <p>6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.</p> <p>7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:</p> <ol style="list-style-type: none"> nazwę aplikacji, nazwę pakietu, kategorię sklepu Google Play, uprawnienia aplikacji, pochodzenie aplikacji z nieznanego źródła.
--	--

Powyższe wymagania należy traktować jako minimalne – akceptowane będą lepsze od żądanych.

- Jeżeli Zamawiający zaznaczył w specyfikacji, iż dany sprzęt ma współpracować lub być integralną częścią sprzętu już posiadanego przez Zamawiającego wymaga się, aby oferowany sprzęt był w pełni zgodny, kompatybilny i prawidłowo współpracował ze wskazanym sprzętem.

- W przypadku sprzętu i oprogramowania, gdzie Zamawiający określił charakterystykę sprzętu lub oprogramowania poprzez podanie znaków towarowych, patentów lub pochodzenie, a takie normy dopuszczając jednocześnie zaoferowanie produktu równoważnego a Wykonawca zaoferuje urządzenie/oprogramowanie równoważne ciężar wykazania równoważności leży po stronie Wykonawcy. Przez produkt równoważny do opisanego przedmiotu zamówienia, Zamawiający rozumie taki, który w sposób poprawny współpracuje z programami oraz z posiadanym środowiskiem sprzętowym Zamawiającego, a jego zastosowanie nie wymaga żadnych nakładów związanych z dostosowaniem programów i środowiska sprzętowego Zamawiającego lub produktu równoważnego oraz realizuje wszystkie funkcjonalności i posiada wszystkie cechy produktu określonego w OPZ.