

1. Serwer EZD RP

Ilość: 1 szt.

Parametr	Charakterystyka (wymagania minimalne)	Oferowane parametry techniczne
<b>Obudowa</b>	<ul style="list-style-type: none"> <li>Obudowa Rack o wysokości max 2U z możliwością instalacji min. 12 dysków 3.5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.</li> <li>Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.</li> <li>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.</li> </ul>	
<b>Płyta główna</b>	<ul style="list-style-type: none"> <li>Płyta główna z możliwością zainstalowania do dwóch procesorów.</li> <li>Obsługa procesorów 56 rdzeniowych.</li> <li>Na płycie głównej powinno znajdować się minimum 32 sloty przeznaczone do instalacji pamięci.</li> <li>Płyta główna powinna obsługiwać do 8TB pamięci RAM.</li> </ul>	
<b>Chipset</b>	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych	
<b>Procesor</b>	Zainstalowane dwa procesory min. 28-rdzeniowe klasy x86, min. 2GHz, dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 460 w teście SPECrate2017_int_base, dostępnym na stronie <a href="http://www.spec.org">www.spec.org</a> dla konfiguracji dwuprocesorowej.	
<b>RAM</b>	Minimum 256GB	

<b>Funkcjonalność pamięci RAM</b>	<ul style="list-style-type: none"> <li>• Demand Scrubbing,</li> <li>• Patrol Scrubbing,</li> <li>• Permanent Fault Detection (PFD)</li> </ul>	
<b>Gniazda PCI</b>	Min. 8 slotów PCIe w tym minimum 6 slotów FH	
<b>Interfejsy sieciowe/FC/SAS</b>	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT, 2 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28	
<b>Dyski twarde</b>	<ul style="list-style-type: none"> <li>• Zainstalowane: <ul style="list-style-type: none"> <li>○ 4x dyski SAS o pojemności min. 4TB, 12Gb, Hot-Plug</li> <li>○ 2x dyski SSD SATA o pojemności min. 960GB, 6Gb, Hot-Plug</li> </ul> </li> <li>• Możliwość zainstalowania dwóch dysków M.2 NVMe SSDs o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1.</li> </ul>	
<b>Kontroler RAID</b>	<ul style="list-style-type: none"> <li>• Sprzętowy kontroler dyskowy, posiadający <ul style="list-style-type: none"> <li>○ Min. 8GB nieulotnej pamięci cache,</li> <li>○ Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.</li> <li>○ Wsparcie dla dysków samoszyfrujących</li> </ul> </li> </ul>	
<b>Wbudowane porty</b>	<ul style="list-style-type: none"> <li>• 4x USB, w tym min. 1 porty USB 3.0</li> <li>• 2x port VGA (jeden na panelu przednim)</li> <li>• Możliwość rozbudowy o Serial Port</li> </ul>	
<b>Video</b>	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024	
<b>Wentylatory</b>	Redundantne, Hot-Plug	
<b>Zasilacze</b>	Redundantne, Hot-Plug min. 1100W klasy Titanium	
<b>System operacyjny/dodatki oprogramowanie</b>	<p>Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego.</p> <p>Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na zoferowanym serwerze. Wymaga się aby</p>	

	<p>oferowane licencje umożliwiają korzystanie 10 użytkownikom.</p> <p>Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.</p> <ol style="list-style-type: none"> <li>1) Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.</li> <li>2) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.</li> <li>3) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.</li> <li>4) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.</li> <li>5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.</li> <li>6) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.</li> <li>7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.</li> <li>8) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.</li> <li>9) Wbudowane wsparcie instalacji i pracy na wolumenach, które: <ol style="list-style-type: none"> <li>a) pozwalają na zmianę rozmiaru w czasie pracy systemu,</li> <li>b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,</li> </ol> </li> </ol>	
--	---	--

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

	<p>polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..</p> <p>20) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&amp;Play).</p> <p>21) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.</p> <p>22) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.</p> <p>23) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).</p> <p>24) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.</p> <p>25) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:</p> <p>a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,</p> <p>b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:</p> <p>I. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,</p> <p>II. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,</p> <p>III. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.</p>	
--	--	--

	<p>IV. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.</p> <p>c) Zdalna dystrybucja oprogramowania na stacje robocze.</p> <p>d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej</p> <p>e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego umożliwiające:</p> <p>I. Dystrybucję certyfikatów poprzez http</p> <p>II. Konsolidację CA dla wielu lasów domeny,</p> <p>III. Automatyczne rejestrowanie certyfikatów pomiędzy różnymi lasami domen,</p> <p>IV. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.</p> <p>f) Szyfrowanie plików i folderów.</p> <p>g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).</p> <p>h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.</p> <p>i) Serwis udostępniania stron WWW.</p> <p>j) Wsparcie dla protokołu IP w wersji 6 (IPv6),</p> <p>k) Wsparcie dla algorytmów Suite B (RFC 4869),</p> <p>l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,</p> <p>m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej</p>	
--	--	--

	<p>funkcjonalności. Mechanizmy virtualizacji mają zapewnić wsparcie dla:</p> <p>I. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,</p> <p>II. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.</p> <p>III. Obsługi 4-KB sektorów dysków</p> <p>IV. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra</p> <p>V. Możliwości virtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.</p> <p>VI. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)</p> <p>26) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.</p> <p>27) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).</p> <p>28) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.</p> <p>29) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.</p> <p>30) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.</p>	
<b>Bezpieczeństwo</b>	<ul style="list-style-type: none"> <li>• Zatrask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.</li> <li>• Możliwość wyłączenia w BIOS funkcji przycisku zasilania.</li> <li>• BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą</li> </ul>	

	<p>zasilania, panelem sterowania oraz zmianą hasła</p> <ul style="list-style-type: none"> <li>• Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.</li> <li>• Moduł TPM 2.0</li> <li>• Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera</li> </ul> <p>Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem</p>	
<b>Karta Zarządzania</b>	<ul style="list-style-type: none"> <li>• Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: <ul style="list-style-type: none"> <li>○ zdalny dostęp do graficznego interfejsu Web karty zarządzającej;</li> <li>○ zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);</li> <li>○ szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika;</li> <li>○ możliwość podmontowania zdalnych wirtualnych napędów;</li> <li>○ wirtualną konsolę z dostępem do myszy, klawiatury;</li> <li>○ wsparcie dla IPv6;</li> <li>○ wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;</li> <li>○ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;</li> <li>○ możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;</li> <li>○ integracja z Active Directory;</li> <li>○ możliwość obsługi przez dwóch administratorów jednocześnie;</li> <li>○ wsparcie dla dynamic DNS;</li> <li>○ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.</li> </ul> </li> </ul>	



	<ul style="list-style-type: none"> <li>○ możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera</li> <li>○ możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności o: <ul style="list-style-type: none"> <li>○ Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej</li> <li>○ Przesyłanie danych telemetrycznych w czasie rzeczywistym</li> <li>○ Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze</li> <li>○ Automatyczna rejestracja certyfikatów (ACE)</li> </ul> </li> </ul>	
<b>Oprogramowanie do zarządzania</b>	<ul style="list-style-type: none"> <li>• Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: <ul style="list-style-type: none"> <li>○ Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych</li> <li>○ integracja z Active Directory</li> <li>○ Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta</li> <li>○ Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish</li> <li>○ Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram</li> <li>○ Szczegółowy opis wykrytych systemów oraz ich komponentów</li> <li>○ Możliwość eksportu raportu do CSV, HTML, XLS, PDF</li> <li>○ Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.</li> <li>○ Grupowanie urządzeń w oparciu o kryteria użytkownika</li> <li>○ Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów</li> </ul> </li> </ul>	

	<p>PCie, pozostałego czasu gwarancji</p> <ul style="list-style-type: none"> <li>○ Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach</li> <li>○ Szybki podgląd stanu środowiska</li> <li>○ Podsumowanie stanu dla każdego urządzenia</li> <li>○ Szczegółowy status urządzenia/elementu/komponentu</li> <li>○ Generowanie alertów przy zmianie stanu urządzenia.</li> <li>○ Filtry raportów umożliwiające podgląd najważniejszych zdarzeń</li> <li>○ Integracja z service desk producenta dostarczonej platformy sprzętowej</li> <li>○ Możliwość przejęcia zdalnego pulpitu</li> <li>○ Możliwość podmontowania wirtualnego napędu</li> <li>○ Kreator umożliwiający dostosowanie akcji dla wybranych alertów</li> <li>○ Możliwość importu plików MIB</li> <li>○ Przesyłanie alertów „as-is” do innych konsol firm trzecich</li> <li>○ Możliwość definiowania ról administratorów</li> <li>○ Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów</li> <li>○ Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)</li> <li>○ Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta</li> <li>○ Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów</li> <li>○ Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja</li> </ul>	
--	--	--

	<p>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.</p> <ul style="list-style-type: none"> <li>○ Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.</li> <li>○ Wdrażanie serwerów, rozwiązań modularnych oraz przetłączników sieciowych w oparciu o profile</li> <li>○ Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.</li> <li>○ Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.</li> <li>○ Zdalne uruchamianie diagnostyki serwera.</li> <li>○ Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.</li> <li>○ Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.</li> </ul>	
<b>Certyfikaty</b>	<ul style="list-style-type: none"> <li>• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001</li> <li>• Serwer musi posiadać deklaracja CE.</li> <li>• Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami – załączyć do ofert dokumentację techniczną potwierdzającą spełnienie normy lub oświadczenie producenta serwera o spełnieniu normy.</li> </ul>	

	<ul style="list-style-type: none"> <li>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.</li> </ul>	
<b>Dokumentacja użytkownika</b>	<ul style="list-style-type: none"> <li>Zamawiający wymaga dokumentacji w języku polskim lub angielskim.</li> <li>Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</li> </ul>	
<b>Warunki gwarancji</b>	<ul style="list-style-type: none"> <li>Min 7 lat gwarancji producenta, z czasem reakcji do do 4 godzin od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta</li> <li>Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.</li> <li>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)</li> <li>Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania.</li> <li>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.</li> <li>Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.</li> <li>Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem</li> </ul>	

	<p>części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.</p> <ul style="list-style-type: none"> <li>• 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 cybernetycznego</li> <li>• Zamawiający wymaga od podmiotu realizującego 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.</li> <li>• Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.</li> </ul>	
--	--	--

## 2. Urządzenie do składowania kopii bezpieczeństwa

Ilość: 1 szt.

LP	Wymagane parametry techniczne	Oferowane parametry techniczne
1	Urządzenie musi być przeznaczone do deduplikacji i przechowywania kopii zapasowych. Urządzenie musi spełniać wymagania wyspecyfikowane w niniejszej tabeli.	
2	Dostarczone urządzenie musi oferować przestrzeń min. 8TB netto (powierzchni użytkowej) bez uwzględniania mechanizmów protekcji.	
3	Oferowane urządzenie musi posiadać minimum 4 porty Eth 10 Gb/s BaseT wymagana możliwość obsługi każdym portem Ethernet protokołów CIFS, NFS, deduplikacja na źródle;	
4	Dostarczone urządzenie musi umożliwiać dodatkową rozbudowę o warstwę typu CLOUD dedykowaną do długotrwałego przechowywania danych (tzw. Long Term Retention) – dane o określonej retencji (zgodnie z założoną polityką retencyjną), bez pośrednictwa dodatkowych urządzeń (typu GATEWAY) powinny zostać przemigrowane (w postaci zdeduplikowanej) na dodatkową warstwę (wymagane wsparcie dla AWS, Microsoft Azure, Google GCP). Wymagana enkrypcja danych przechowywanych na warstwie typu Cloud. Skalowanie w przypadku wykorzystywanej przestrzeni warstwy typu Cloud musi stanowić równoważność co najmniej dwukrotnej pojemności netto oferowanego urządzenia (bez uwzględnienia warstwy CLOUD), czyli $8TB \times 2 = 16TB$ .	
5	Oferowane urządzenie musi umożliwiać jednoczesny dostęp wszystkimi poniższymi protokołami: <ul style="list-style-type: none"> <li>• CIFS, NFS,</li> <li>• zapewniającym deduplikację na źródle - wymagane wsparcie dla co najmniej Veeam Backup and Replication oraz NetWorker</li> </ul> VTL (po doposażeniu w porty FC)	
6	Oferowane pojedyncze urządzenie musi osiągać zagregowaną wydajność (dla maksymalnej konfiguracji) protokołami CIFS, NFS: co najmniej 3 TB/h (dane podawane przez producenta) oraz co najmniej 7 TB/h z wykorzystaniem deduplikacji na źródle (dane podawane przez producenta).	
7	Urządzenie musi pozwalać na jednoczesną obsługę minimum 90 strumieni jednocześnie, w tym 30 dedykowanych do zapisu 30 dedykowanych do odczytu 30 dedykowanych do replikacji wszystkie zapisywane strumienie muszą podlegać globalnej deduplikacji przed zapisem na dysk (in-line) jak opisano w niniejszej specyfikacji.	
8	Oferowane urządzenie musi deduplikować dane in-line przed zapisem na nośnik dyskowy. Na wewnętrznych dyskach urządzenia nie mogą być zapisywane dane w oryginalnej postaci (niezdeduplikowanej) z jakiegokolwiek fragmentu strumienia	

	danych przychodzącego do urządzenia, powyższe wymaganie nie będzie spełnione jeżeli deduplikacja in-line realizowana będzie przez zewnętrzną aplikację backup'ową. Wymaganie deduplikacji in-line dotyczy zapisu danych przez każdy z wymaganych interfejsów, w przypadku interfejsów: NFS, CIFS oraz VTL realizacja deduplikacji in-line nie może w żadnym stopniu zależeć od konkretnej aplikacji backup'owej, dane zapisywane poprzez interfejsy NFS CIFS bez użycia jakiegokolwiek aplikacji backup'owej również muszą być deduplikowane w sposób in-line	
<b>9</b>	Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych co oznacza, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości, bez konieczności podejmowania czynności mających na celu ustalenie predefiniowanej długości bloków używanych do deduplikacji danych określonego typu.	
<b>10</b>	Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku jednak o długości nie większej niż 12 kB Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych co oznacza, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości, bez konieczności podejmowania czynności mających na celu ustalenie predefiniowanej długości bloków używanych do deduplikacji danych określonego typu. Deduplikacja zmiennym, dynamicznym blokiem oznacza, że wielkość każdego bloku (na jaki są dzielone dane pojedynczego strumienia backupowego) może być inna niż poprzedniego oraz jest indywidualnie ustalana przez algorytm deduplikacji zastosowany w urządzeniu, oferowane urządzenie nie może dzielić jakiegokolwiek pojedynczego strumienia danych backupowych na bloki o ustalonej, tej samej długości.	
<b>11</b>	Oferowane urządzenie musi posiadać obsługę mechanizmów globalnej deduplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, VTL, deduplikacja na źródle) przechowywanych w obrębie całej przestrzeni urządzenia co oznacza, że przechowywany na urządzeniu fragment danych nie może być ponownie zapisany bez względu na to, jakim protokołem zostanie ponownie otrzymany. Wszystkie emulowane jednocześnie w obrębie urządzenia biblioteki wirtualne (VTL) oraz udziały NFS/CIFS również powinny podlegać globalnej deduplikacji – blok danych otrzymany i zapisany w wirtualnej bibliotece „A”, nie może zostać ponownie zapisany jeśli trafi do innej wirtualnej biblioteki „B” w obrębie tego samego urządzenia (to samo dotyczy udziałów NFS/CIFS). Przestrzeń składowania zdeduplikowanych danych musi być jedna dla wszystkich protokołów dostępowych, co oznacza zastosowanie pojedynczej bazy deduplikatów bez względu na ilość/rodzaj używanych jednocześnie protokołów dostępowych.	
<b>12</b>	Przestrzeń składowania zdeduplikowanych danych musi być jedna dla wszystkich protokołów dostępowych, co oznacza	

	zastosowanie pojedynczej bazy deduplikatów bez względu na ilość/rodzaj używanych jednocześnie protokołów dostępowych.	
<b>13</b>	Proces deduplikacji musi odbywać się in-line – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Zapisowi na system dyskowy muszą podlegać tylko unikalne bloki danych nie zapisane jeszcze na system dyskowy urządzenia. Dotyczy to każdego fragmentu przychodzących do urządzenia danych.	
<b>14</b>	Proponowane rozwiązanie nie może w żadnej fazie korzystać (w całości lub częściowo) z bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej) w celu ich późniejszej deduplikacji (wymagana deduplikacja in-line)	
<b>15</b>	Wszystkie unikalne bloki przed zapisaniem na dysk muszą być kompresowane jedną z metod do wyboru: gz, lz.	
<b>16</b>	Tryb zapisu zabezpieczanych danych nie może umożliwiać nadpisywania danych, dane mogą być zapisywane jedynie w trybie append-only, dane dla których wygasła retencja powinny zostać usunięte podczas procesu czyszczenia tzw. Cleaning, wymagane dotyczy wszystkich danych zapisanych na urządzeniu a nie wybranych grup danych objętych działaniem blokad zabezpieczających przed usunięciem/modyfikacją danych.	
<b>17</b>	Oferowane urządzenie musi wspierać (wymagane formalne wsparcie producenta urządzenia), co najmniej następujące aplikacje: Veeam, NetWorker, Oracle RMAN, Microsoft SQL Server Management Studio.	
<b>18</b>	<p>W przypadku współpracy z każdą z poniższych aplikacji:</p> <ul style="list-style-type: none"> <li>• RMAN (dla ORACLE)</li> <li>• Microsoft SQL Server Management Studio (dla Microsoft SQL)</li> <li>• Veeam Backup and Replication</li> <li>• NetWorker</li> </ul> <p>urządzenie musi umożliwiać deduplikację na źródle (w przypadku Veeam na poziomie Veeam Data Mover, w przypadku NetWorker na poziomie standardowego klienta na wszystkich wspieranych OS) i przesłanie nowych, nie znajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN.</p> <p>Deduplikacja w wyżej wymienionych przypadkach musi zapewniać aby z serwera do urządzenia były transmitowane poprzez sieć tylko fragmenty danych nie znajdujące się dotychczas na urządzeniu</p>	
<b>19</b>	W przypadku deduplikacji na źródle poprzez sieć IP (LAN oraz WAN), wymagana możliwość szyfrowania komunikacji kluczem minimum 256 bitów.	
<b>20</b>	Oferowane urządzenie musi umożliwiać uruchamianie maszyn wirtualnych VMware bezpośrednio z danych backupowych bez konieczności odtwarzania danych, funkcjonalność ta powinna być wspierana co najmniej przez Veeam Backup and Replication oraz NetWorker. Spełnienie wymagania nie może być ograniczone dla wybranych grup danych ze względu na miejsce składowania czy konkretną retencję.	



<b>21</b>	Wymagane wsparcie dla backupów typu Virtual Synthetics co najmniej w przypadku aplikacji Veeam Backup and Replication oraz NetWorker.	
<b>22</b>	Urządzenie nie może zmniejszać swojej wydajności w czasie przybywania kolejnych danych.	
<b>23</b>	Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych do drugiego urządzenia takiego samego typu. Konfiguracja replikacji musi być możliwa w każdym z trybów: <ul style="list-style-type: none"> <li>* jeden do jednego</li> <li>* wiele do jednego</li> <li>* jeden do wielu</li> <li>* kaskadowej (urządzenie A replikuje dane do urządzenia B, które te same dane replikuje do urządzenia C).</li> </ul> Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane mogą być tylko te fragmenty danych (bloki) które nie znajdują się na docelowym urządzeniu. Ewentualna licencja na replikację musi być dostarczona w ramach postępowania.	
<b>24</b>	Urządzenie musi umożliwiać wydzielenie określonych portów Ethernet dedykowanych do replikacji.	
<b>25</b>	W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami.	
<b>26</b>	Oferowane urządzenie musi działać poprawnie przy zapelnieniu danymi na poziomie co najmniej 90%. Dokumentacja urządzenia nie może wskazywać na ew. problemy, obostrzenia, które są efektem zapelnienia urządzenia zabezpieczanymi danymi, na poziomie mniejszym niż 90%.	
<b>27</b>	Wymagana możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami.	
<b>28</b>	Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6 lub równoważnej.	
<b>29</b>	Oferowane urządzenie musi umożliwiać realizację oraz przechowywanie SnapShot'ów, czyli umożliwiać zamrożenie obrazu danych (stanu backupów) w urządzeniu na określoną chwilę. Oferowane urządzenie musi również umożliwiać odtworzenie danych ze Snapshot'u. Odtworzenie danych ze Snapshot'u nie może wymagać konieczności nadpisania danych produkcyjnych jak również nie może oznaczać przerwy w normalnej pracy urządzenia (przyjmowania/odtworzenia backupów).	
<b>30</b>	Urządzenie musi pozwalać na realizację i przechowywanie minimum 300 Snapshotów jednocześnie w obrębie oferowanej przestrzeni, przy zachowaniu globalnej deduplikacji oraz standardowego trybu pracy urządzenia - umożliwiającego wykorzystanie wszystkich dostępnych funkcjonalności.	
<b>31</b>	Urządzenie musi umożliwiać podział na logiczne części. Dane znajdujące się w każdej logicznej części muszą być między sobą deduplikowane (globalna deduplikacja między logicznymi częściami urządzenia).	

<b>32</b>	Urządzenie musi mieć możliwość podziału na minimum 4 logiczne części pracujące równolegle.	
<b>33</b>	Dla każdej z w/w logicznych części oferowanego urządzenia musi być możliwość zdefiniowania oddzielnego użytkownika zarządzającego daną logiczną częścią deduplikatora. Użytkownicy zarządzający logiczną częścią A muszą widzieć tylko i wyłącznie zasoby logicznej części A i nie mogą widzieć żadnych innych zasobów oferowanego urządzenia.	
<b>34</b>	Wymagana możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia, jako niezależnego urządzenia dostępnego za pośrednictwem: <ul style="list-style-type: none"> <li>• CIFS</li> <li>• NFS</li> <li>• zapewniającym deduplikację na źródle dla co najmniej: Veeam Backup and Replication oraz NetWorker VTL</li> </ul>	
<b>35</b>	Urządzenie musi umożliwiać zdefiniowanie blokady skasowania danych (funkcjonalność WORM). Blokada skasowania danych musi chronić plik w zdefiniowanym czasie przed usunięciem pliku, modyfikacją pliku. Blokada skasowania danych musi działać w dwóch trybach (do wyboru przez administratora): <ol style="list-style-type: none"> <li>1. Możliwość zdjęcia blokady przed upływem ważności danych</li> <li>2. Brak możliwości zdjęcia blokady przed upływem ważności danych (COMPLIANCE, wymagane wsparcie dla norm: SEC 17a-4(f), ISO Standard 15489-1 )</li> </ol> <p>Licencje na blokadę skasowania/zmiany przechowywanych plików muszą być dostarczone wraz z urządzeniem.</p> <p>Wymagana możliwość automatycznego uruchamiania blokady (podczas zapisu) WORM dla danych zapisywanych na obszar objęty działaniem wspomnianej blokady, wymagana również możliwość używania blokady WORM dla obrazu danych uzyskanych poprzez użycie wymaganej funkcjonalności SnapShot.</p> <p>Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności).</p>	
<b>36</b>	Urządzenie musi weryfikować ewentualne przekłamania (zmianę danych) na poziomie systemu plików. Wymaga się aby urządzenie weryfikowało sumy kontrolne dla wszystkich fragmentów zapisywanych danych, niezależnie od używanego interfejsu.	
<b>37</b>	Urządzenie musi weryfikować dane po zapisie (nie chodzi o ew. weryfikację danych indeksowych generowanych przez urządzenie ale o weryfikację wszystkich zabezpieczanych danych backup'owych w trybie „end-to-end”). Każda zapisana na dyskach porcja danych musi być odczytana i porównana z danymi otrzymanymi przez urządzenie. Powyższa weryfikacja powinna być realizowana w locie, czyli przed usunięciem z pamięci oryginalnych danych (otrzymanych z aplikacji backupowej), musi być realizowana w trybie ciągłym (a nie ad-	

	<p>hoc), wymagane parametry wydajnościowe urządzenia muszą uwzględniać tę funkcjonalność.</p> <p>Wymagane potwierdzenie opisanej funkcjonalności w oficjalnej dokumentacji producenta oferowanego urządzenia.</p> <p>Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności)</p>	
<b>38</b>	Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia.	
<b>39</b>	Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu).	
<b>40</b>	<p>Musi istnieć możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora).</p> <p>Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności.</p>	
<b>41</b>	Wymagana możliwość zdefiniowania harmonogramu wg. którego wykonywany jest proces usuwania przeterminowanych danych (czyszczenia), realizowany równolegle z procesami backup/restore/replication.	
<b>42</b>	Standardowa częstotliwość usuwania przeterminowanych danych (czyszczenie) nie powinna być większa niż 1 raz na tydzień - minimalizując czas w którym backupy/odtworzenia narażone są na spowolnienie (weryfikacja wymagania na podstawie dokumentacji typu DOBRE PRAKTYKI publikowanej przez producenta).	
<b>43</b>	Urządzenie musi umożliwiać systemowo (wbudowana funkcjonalność) - realizację procesu pierwszego czyszczenia dopiero po przekroczeniu 75% zajętości oferowanej przestrzeni.	
<b>44</b>	Urządzenie musi mieć możliwość zarządzania poprzez Interfejs graficzny dostępny z przeglądarki internetowej Poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell)	
<b>45</b>	Oprogramowanie do zarządzania musi rezydować na oferowanym na urządzeniu deduplikacyjnym.	
<b>46</b>	<p>Urządzenie musi być rozwiązaniem kompletnym, apłiancem sprzętowym pochodzącym od jednego producenta.</p> <p>Zamawiający nie dopuszcza stosowania rozwiązań typu gateway. Oferowany typ urządzenia musi być oficjalnie dostępne w ofercie producenta przed ukazaniem się niniejszego postępowania.</p>	
<b>47</b>	Oferowane urządzenie powinno być objęte wsparciem producenta w okresie 60 miesięcy, realizowanym w trybie zgłoszeń awarii: 24x7 oraz reakcji on-site NBD 5x9, uszkodzone dyski pozostają u Zamawiającego bez ponoszenia dodatkowych kosztów.	
<b>48</b>	<p>1) Konfiguracja platformy przechowywania kopii bezpieczeństwa.</p> <p>a) instalacja i integracja urządzenia do pracy w środowisku VDP,</p>	

	<ul style="list-style-type: none"> <li>i) konfiguracja urządzenia, <ul style="list-style-type: none"> <li>(1) inicjalizacja deduplikatora,</li> <li>(2) aktualizacja deduplikatora do najnowszych zalecanej wersji,</li> <li>(3) konfiguracja Mtree, DDBoost, Storage Unit, Interface Groups,</li> </ul> </li> <li>ii) konfiguracja oprogramowania VDP w środowisku kopii bezpieczeństwa, <ul style="list-style-type: none"> <li>(1) integracja VDP z urządzeniem z wykorzystaniem protokołu DDBoost,</li> <li>(2) definicja polityk w zakresie grup, harmonogramu, retencji,</li> <li>(3) definicja polityk kopii zapasowych,</li> <li>(4) wykonanie kopii zapasowych wskazanych środowisk (maksymalnie 4VM na Hyper-V),</li> <li>(5) weryfikacja poprawności wykonywania kopii zapasowych,</li> </ul> </li> <li>b) testy uruchomionej platformy kopii bezpieczeństwa, <ul style="list-style-type: none"> <li>i) przeprowadzenie testowego odtworzenia (maksymalnie 100GB),</li> </ul> </li> </ul> <p>Przekazania środowiska w formie prezentacji dla działów IT.</p>	
--	--	--

### 3. UPS

Ilość: 1 szt.

<b>Nazwa</b>	<b>Wymagane parametry techniczne</b>	<b>Oferowane parametry techniczne</b>
<b>Moc wyjściowa</b>	min. 3 kVA	
<b>Architektura UPS</b>	line interactive lub on-line	
<b>Maks. czas przełączenia na baterię</b>	4 ms	
<b>Ilość gniazd sieciowych</b>	min. 8 IEC C13	
<b>Porty</b>	Min. 1 x USB Min. 1 x RS-232	
<b>Typ obudowy</b>	RACK	
<b>Czas podtrzymania przy obciążeniu 100 %</b>	min. 1 min.	
<b>Czas podtrzymania przy obciążeniu 50 %</b>	min. 7 min.	
<b>Gwarancja</b>	Gwarancja producenta min. 36 miesięcy	

4. Oprogramowanie do wykonywania kopii bezpieczeństwa

Ilość: 1 szt.

Parametr	Charakterystyka (wymagania minimalne)	Oferowane parametry techniczne
<b>Wymagania ogólne</b>	<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 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.</p> <p>Licencja wieczysta dla 10 serwerów (fizyczne i VM) z rocznym wsparciem producenta oprogramowania.</p>	
<b>Wymagania szczegółowe</b>	<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.</p> <p>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,</p>	

	<p>oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.</p> <p>Oprogramowanie musi wspierać niezmiennosc 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 statych 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>	
<b>Wymagania RPO</b>	<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</p>	

	<p>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.</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.</p> <p>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</p>	
--	--	--



	<p>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 jednocześnie uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdedykowanego 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.</p> <p>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)</p> <p>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</p> <p>Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere</p> <p>Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL i Oracle bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.</p> <p>Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków</p> <p>Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.</p> <p>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</p> <p>Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy</p>	

	<p>natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.</p> <p>Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell</p> <p>Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.</p> <p>Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.</p> <p>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.</p> <p>Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects").</p> <p>Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego.</p> <p>Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych.</p> <p>Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, 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 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 wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN</p>	
<p><b>Wymagania ograniczenia ryzyka</b></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 umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.</p>	
<p><b>Wymagania dla Agenta</b></p>	<p>Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego</p> <p>Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych</p> <p>Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE</p> <p>Rozwiązanie musi wspierać system operacyjny macOS</p>	

	<p>Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix</p> <p>Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą)</p> <p>Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster</p> <p>Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów</p> <p>Rozwiązanie musi wspierać backup podłączonych dysków USB</p> <p>Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym</p> <p>Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury)</p> <p>Rozwiązanie musi wspierać deduplikację oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone</p> <p>Rozwiązanie musi wspierać kontrolę pasma sieciowego</p> <p>Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych</p> <p>Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN</p> <p>Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft</p> <p>Rozwiązanie musi wspierać technologię BitLocker</p> <p>Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania</p> <p>Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzbiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych,</p>	
--	--	--

	<p>Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych</p> <p>Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych</p> <p>Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL i Oracle poprzez bezpośrednie uruchomienie ich z pliku backupu.</p> <p>Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform</p> <p>Rozwiązanie musi wspierać szyfrowanie</p> <p>Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne</p> <p>Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego</p> <p>Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej</p> <p>Rozwiązanie musi wspierać tworzenie wielu zadań backupowych</p>	
--	---	--

5. Instalacja, wdrożenie konfiguracji i wsparcie techniczne przez okres trwania projektu

Ilość: 1 szt.

Parametr	Charakterystyka (wymagania minimalne)	Oferowane parametry techniczne
Opis	<p>Ustalenie z działem IT Zamawiającego prawidłowej instalacji dostarczonych urządzeń.</p> <p>Montaż dostarczonych urządzeń oraz ich instalacja zgodnie z wytycznymi Zamawiającego.</p> <p>Podstawowa konfiguracja systemów operacyjnych</p> <p>Instalacja i konfiguracja środowiska serwerowego</p> <p>Optymalizacja zasobów sprzętowych</p> <p>Wirtualizacja posiadanego przez Zamawiającego serwera fizycznego do HYPER-V.</p> <p>Migracja obecnego środowiska VmWare do Hyper-V – min. 3 maszyny wirtualne</p> <p>Konfiguracja zapasowego kontrolera active directory</p> <p>Aktualizacja i optymalizacja posiadanych serwerów</p> <p>Test działania sieci na maszynach wirtualnych i storage</p> <p>Przygotowanie dokumentacji powykonawczej</p> <p>2) Konfiguracja platformy przechowywania kopii bezpieczeństwa.</p> <p>a) instalacja i integracja urządzenia do pracy w środowisku VDP,</p> <p>i) konfiguracja urządzenia,</p> <p>(1) inicjalizacja deduplikatora,</p> <p>(2) aktualizacja deduplikatora do najnowszych zalecanej wersji,</p> <p>(3) konfiguracja Mtree, DDBoost, Storage Unit, Interface Groups,</p> <p>ii) konfiguracja oprogramowania VDP w środowisku kopii bezpieczeństwa,</p> <p>(1) integracja VDP z urządzeniem z wykorzystaniem protokołu DDBoost,</p> <p>(2) definicja polityk w zakresie grup, harmonogramu, retencji,</p>	

	<ul style="list-style-type: none"> <li>(3) definicja polityk kopii zapasowych,</li> <li>(4) wykonanie kopii zapasowych wskazanych środowisk (maksymalnie 4VM na Hyper-V),</li> <li>(5) weryfikacja poprawności wykonywania kopii zapasowych,</li> </ul> <ul style="list-style-type: none"> <li>b) testy uruchomionej platformy kopii bezpieczeństwa, <ul style="list-style-type: none"> <li>i) przeprowadzenie testowego odtworzenia (maksymalnie 100GB),</li> </ul> </li> </ul> <p>3) Przekazania środowiska w formie prezentacji dla działów IT.</p>	
--	--	--

