UNIWERSYTET KARDYNAŁA STEFANA WYSZYŃSKIEGO W WARSZAWIE

Załącznik nr 3 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest dostawa systemu BACKUP wraz z wymaganą infrastrukturą.

a) Serwer kopii zapasowych – spełniający wymagania z **Tabeli 1** – 1 sztuka;

b) Serwer repozytorium kopii zapasowych – spełniający wymagania z **Tabeli 2** – 1 sztuka;

c) Urządzenie repozytorium kopii zapasowych typu deduplikator – spełniające wymagania z **Tabeli 3** – 1 sztuka;

d) Urządzenie repozytorium kopii zapasowych typu automatyka taśmowa – spełniające wymagania z **Tabeli 4** – 1 sztuka;

e) Urządzenie sieciowe typu przełączniki w sieci SAN – spełniające wymagania z **Tabeli 5** – 2 sztuki;

f) Oprogramowanie kopii zapasowych – spełniające wymagania z **Tabeli 6**;

g) Usługa wdrożeniowa – spełniająca wymagania z **Tabeli 7**.

Tabela 1. Wymagania dla 1 sztuki „Serwer kopii zapasowych”

Lp.	Nazwa komponentu	Wymagane parametry
1.	**Typ**	Serwer stelażowy
2.	**Obudowa**	Maksymalnie 1U RACK 19 cali (wraz ze wszystkimi elementami niezbędnymi do zamontowania serwera w szafie serwerowej 19” oraz wysuwania w celach serwisowych – ramię na przewody).
3.	**Procesor**	Minimum szesnastordzeniowy pracujący z częstotliwością niemniejszą niż 2.0GHz, obsługujący pamięci minimum 4400MT/s o poborze mocy maksymalnej 150W. Ilość procesorów: 1 sztuka
4.	**Pamięć RAM**	Minimum 128 GB RDIMM/LRDIMM DDR5 w modułach minimum 32GB. Możliwość instalacji w serwerze minimum4TB pamięci RAM per procesor. Minimum 32 sloty na pamięć na płycie głównej serwera. Zabezpieczenia pamięci: Advanced ECC.
5.	**Dysk twardy**	Zainstalowane wewnątrz serwera dyski:

		• 2 x 480GB NVMe na potrzeby systemu operacyjnego skonfigurowane w sprzętowy RAID 1
6.	**Karta graficzna**	Zintegrowana karta graficzna
7.	**Sloty PCIe**	Serwer w standardzie z minimum 2 slotami PCI-Express Generacji 5 w tym: 2 działające z prędkością x16 (bus width). Wszystkie sloty pozwalające na instalacje kart z portami zewnętrznymi. Możliwość rozbudowy o dodatkowy slot PCI-Express Generacji 5 działający z prędkością x16 (bus width).
8.	**Karty sieciowe**	Serwer musi być wyposażony w karty: - 1 kartę 2-portową 10/25Gb z wkładkami 10 Gb SFP + nie zajmującą slotów PCIe - 1 kartę 2-portową 32 Gb FC z wkładkami Zamawiający nie dopuszcza zaoferowania jednej karty z różnymi typami portów.
9	**Porty**	Minimum 3 x USB 3.0 (w tym jeden wewnętrzny) Nie dopuszcza się stosowania spliterów oraz kart zajmujących wolne sloty PCIe w serwerze w celu osiągniecia wymaganych liczby portów USB. 1x VGA
10.	**Zasilacz**	Minimum 2 sztuki każdy, minimum 1000W typu Hot-Plug, klasy minimum Titanium.
11.	**Karta/moduł zarządzający**	Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalne funkcjonalności poniżej: • monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne) • wparcie dla pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP • dostęp do karty zarządzającej poprzez - dedykowany port RJ45 z tyłu serwera lub - przez współdzielony port zintegrowanej karty sieciowej serwera • dostęp do karty możliwy - z poziomu przeglądarki webowej (GUI)

		- z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP) - poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface) • wbudowane narzędzia diagnostyczne • zdalna konfiguracja serwera(BIOS) i instalacji systemu operacyjnego • obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie • wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników • przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough) • obsługa zdalnego serwera logowania (remote syslog) • wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i wirtualnych folderów • mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie • funkcja zdalnej konsoli szeregowej przez SSH (wirtualny port szeregowy) • monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji • konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping) • zdalna aktualizacja oprogramowania (firmware) • zarządzanie grupami serwerów, w tym: - tworzenie i konfiguracja grup serwerów - sterowanie zasilaniem (wł./wył.) - ograniczenie poboru mocy dla grupy (power caping) - aktualizacja oprogramowania (firmware) - wspólne wirtualne media dla grupy • możliwość równoczesnej obsługi przez minimum 2 administratorów • autentykacja dwuskładnikowa (Kerberos)

		• wsparcie dla Microsoft Active Directory • obsługa TLS i SSH • wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API • możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)
12.	**Wymagany system operacyjny**	Serwer musi zostać dostarczony wraz z system operacyjnym Windows Server 2025 Standard.
13.	**Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych**	Microsoft Windows Server 2022 lub nowszy Red Hat Enterprise Linux (RHEL) 9.0 lub nowszy SUSE Linux Enterprise Server (SLES) 15 SP4 lub nowszy VMware ESXi 8.0 lub nowszy.
14.	**Wsparcie serwisowe**	Usługi będą w szczególności wykonywane w następujący sposób: • Okres wsparcia serwisowego producenta – 60 miesięcy realizowane w trybie NBD (next business day). • Czas reakcji serwisu na awarię – następny dzień roboczy. • Naprawy realizowane są zdalnie lub na miejscu w siedzibie Zamawiającego. • Uszkodzone dyski pozostają własnością Zamawiającego. W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z urządzeniem oraz oprogramowania wewnętrznego urządzenia. Gwarancja na sprzęt musi być dostarczona i realizowana przez organizację serwisową producenta sprzętu. Wykonawca musi zapewnić proces sprzedaży i serwisu urządzeń storage zgodnie z posiadanym przez producenta certyfikatem ISO 9001:2015 Serwis musi być realizowany przez producenta sprzętu w języku polskim.
15.	**Inne**	Oferowane urządzenie musi być fabrycznie nowe, wyprodukowane w 2025 roku i pochodzić z oficjalnego kanału dystrybucyjnego producenta na rynek Unii Europejskiej. Zamawiający zastrzega sobie, aby Wykonawca na żądanie Zamawiającego przedłożył oświadczenie Producenta oferowanego sprzętu, w języku polskim, potwierdzające pochodzenie sprzętu z autoryzowanego kanału dystrybucji obejmującego rynek Unii Europejskiej. Serwer musi posiadać ramkę typu bezel zamykaną na klucz oraz czujnik otwarcia obudowy serwera.

16.	**Usługi instalacyjne**	Wykonawca dostarczy i zainstaluje serwer w szafie rack. Ponadto dokona aktualizacji firmware oraz sterowników do najnowszej dostępnej wersji na dzień dostawy. Instalacja realizowana przez certyfikowanego inżyniera producenta serwera.

Tabela 2. Wymagania dla 1 sztuki „Serwer repozytorium kopii zapasowych”

Lp.	Nazwa komponentu	Wymagane parametry
1.	**Typ**	Serwer stelażowy
2..	**Obudowa**	Maksymalnie 2U RACK 19 cali (wraz ze wszystkimi elementami niezbędnymi do zamontowania serwera w szafie serwerowej 19”).
3.	**Procesor**	Minimum szesnastordzeniowy pracujący z częstotliwością niemniejszą niż 2.0GHz, obsługujący pamięci minimum 4400MT/s o poborze mocy maksymalnej 150W. Ilość procesorów: 1 sztuka
4..	**Pamięć RAM**	Minimum 128 GB RDIMM/LRDIMM DDR4 w modułach minimum 32GB. Możliwość instalacji w serwerze minimum 4TB pamięci RAM. Minimum 24 sloty na pamięć. Zabezpieczenia pamięci: Advanced ECC.
5.	**Dysk twardy**	Zainstalowane wewnątrz serwera dyski: • 2 x 480GB NVMe na potrzeby systemu operacyjnego skonfigurowane w sprzętowy RAID 1 • 16 x 16 TB SAS 7.2k 3,5” HDD Możliwość zainstalowania w serwerze 24 dysków SAS/SATA/SSD 3.5” typu Hot-Plug oraz do 6 dysków typu NVMe poprzez jego rozbudowę lub wymianę komponentów.
6.	**Kontroler**	Serwer wyposażony w kontroler sprzętowy z minimum 8GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, 32 portowy (32 dedykowane linie SAS/SATA/NVme do podłączenia nośników), obsługujący poziomy: RAID 0/1/10/5/50/6/60. Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD (HBA) jednocześnie. Kontroler z możliwością rozbudowy o funkcjonalnością szyfrowania wolumenów logicznych stworzonych na podłączonych dyskach (szyfrowanie realizowane przez kontroler RAID, a nie przez oprogramowanie zainstalowane na systemie operacyjnym) lub kontroler z funkcja współpracy z dyskami samoszyfrującymi SED. W przypadku zastosowania kontrolera RAID z funkcją współpracy z dyskami samoszyfrującymi SED wszystkie zastosowane/dostarczone dyski muszą być dyskami SED.
7.	**Karta graficzna**	Zintegrowana karta graficzna

8.	**Sloty PCIe**	Serwer w standardzie z minimum 3 slotami PCI-Express Generacji 5 w tym: minimum 3 działające z prędkością x16 (bus width). W przypadku rozbudowy o 2 procesor, wymaga się możliwości rozbudowy o minimum 3 sloty PCI-Express Generacji 5 w tym: 2 działające z prędkością x16 (bus width). Wszystkie sloty pozwalające na instalacje kart z portami zewnętrznymi.
9.	**Karty sieciowe**	Serwer musi być wyposażony w karty: - 1 kartę 2-portową 10/25Gb z wkładkami 10Gb SFP+ nie zajmującą slotów PCIe - 1 kartę 2-portową 32Gb FC z wkładkami Zamawiający nie dopuszcza zaaferowania jednej karty z różnymi typami portów.
10.	**Porty**	3 x USB 3.0 (w tym jeden wewnętrzny) Nie dopuszcza się stosowania spliterów oraz kart zajmujących wolne sloty PCIe w serwerze w celu osiągniecia wymaganych liczby portów USB. 1x VGA
11.	**Zasilacz**	Minimum 2 sztuki, każdy minimum 1000W typu Hot-Plug, klasy minimum Titanium.
12.	**Karta/moduł zarządzający**	Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: • monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne) • wparcie dla pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP • dostęp do karty zarządzającej poprzez - dedykowany port RJ45 z tyłu serwera lub - przez współdzielony port zintegrowanej karty sieciowej serwera • dostęp do karty możliwy - z poziomu przeglądarki webowej (GUI) - z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP) - poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface)

		• wbudowane narzędzia diagnostyczne • zdalna konfiguracji serwera(BIOS) i instalacji systemu operacyjnego • obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie • wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników • przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough) • obsługa zdalnego serwera logowania (remote syslog) • wirtualna zadalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i i wirtualnych folderów • mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie • funkcja zdalnej konsoli szeregowej przez SSH (wirtualny port szeregowy) • monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji • konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping) • zdalna aktualizacja oprogramowania (firmware) • zarządzanie grupami serwerów, w tym: tworzenie i konfiguracja grup serwerów sterowanie zasilaniem (wł./wył.) ograniczenie poboru mocy dla grupy (power caping) aktualizacja oprogramowania (firmware) wspólne wirtualne media dla grupy • możliwość równoczesnej obsługi przez minimum 2 administratorów • autentykacja dwuskładnikowa (Kerberos) • wsparcie dla Microsoft Active Directory • obsługa TLS i SSH • wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API

		• możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)
13.	**Wymagany system operacyjny**	Serwer musi zostać dostarczony wraz z system operacyjnym Windows Server 2025 Standard.
14.	**Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych**	Microsoft Windows Server 2022 lub nowszy Red Hat Enterprise Linux (RHEL) 9.0 lub nowszy SUSE Linux Enterprise Server (SLES) 15 SP4 lub nowszy VMware ESXi 8.0 lub nowszy.
15.	**Wsparcie serwisowe**	Usługi będą w szczególności wykonywane w następujący sposób: • Okres wsparcia serwisowego producenta – 60 miesięcy realizowane w trybie NBD (next business day) • Czas reakcji serwisu na awarię – następny dzień roboczy. • Naprawy realizowane są zdalnie lub na miejscu w siedzibie Zamawiającego. • Uszkodzone dyski pozostają własnością Zamawiającego. W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z urządzeniem oraz oprogramowania wewnętrznego urządzenia. Gwarancja na sprzęt musi być dostarczona i realizowana przez organizację serwisową producenta sprzętu. Wykonawca musi zapewnić proces sprzedaży i serwisu urządzeń storage zgodnie z posiadanym przez producenta certyfikatem ISO 9001:2015 Serwis musi być realizowany przez producenta sprzętu w języku polskim.
16.	**Inne**	Oferowane urządzenie musi być fabrycznie nowe, wyprodukowane w 2025 roku i pochodzić z oficjalnego kanału dystrybucyjnego producenta na rynek Unii Europejskiej. Zamawiający zastrzega sobie, aby Wykonawca na żądanie Zamawiającego przedłożył oświadczenie Producenta oferowanego sprzętu, w języku polskim, potwierdzające pochodzenie sprzętu z autoryzowanego kanału dystrybucji obejmującego rynek Unii Europejskiej. Serwer musi posiadać ramkę typu bezel zamykaną na klucz.
17.	**Usługi instalacyjne**	Wykonawca dostarczy i zainstaluje serwer w szafie rack. Ponadto dokona aktualizacji firmware oraz sterowników do najnowszej dostępnej wersji na dzień dostawy. Instalacja realizowana przez certyfikowanego inżyniera producenta serwera.

Tabela 3. Wymagania dla 1 sztuki „Urządzenie repozytorium kopii zapasowych typu deduplikator”

Lp.	Nazwa komponentu	Wymagane parametry
1.	**Definicja**	Urządzenie musi być kompletnym rozwiązaniem sprzętowym typu „appliance”, pochodzącym od jednego producenta. Nie dopuszcza się rozwiązania zbudowanego z niezależnych komponentów sprzętowo-programowych. Urządzenie powinno być oficjalnie dostępne w ofercie producenta przed ukazaniem się niniejszego postepowania.
2.	**Obudowa**	Urządzenie musi być przystosowane do montażu w szafie rack 19”.
3.	**Przestrzeń dyskowa na dane**	Urządzenie musi oferować minimum 180TiB przestrzeni użytkowej dla danych (bez deduplikacji).
4.	**Bezpieczeństwo danych**	Dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą mechanizmu RAID zabezpieczającej przed utratą spójności danych w przypadku jednoczesnej awarii dwóch dowolnych dysków. Urządzenie musi weryfikować ewentualne przekłamanie danych w wyniku działań systemu plików / mechanizmów RAID zaimplementowanych w urządzeniu. Wymaga się, aby urządzenie sprawdzało sumy kontrolne zapisywanych fragmentów danych po przejściu danych przez system plików / mechanizmy RAID. Urządzenie musi automatycznie rozpoznawać i naprawiać błędy w locie. Urządzenie musi umożliwiać bezpieczne usuwanie danych poprzez mechanizm wielokrotnego nadpisania przeterminowanych danych. Jeżeli dla realizacji powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla nieograniczonej pojemności dostarczanego urządzenia.
5.	**Interfejsy do hostów**	Urządzenie musi posiadać minimum: • 2 porty Ethernet 10 Gb/s BaseT na cele zarządzania; • 2 porty Fibre Channel 32Gb z możliwością obsługi każdym portem protokołów CIFS, NFS i VTL oraz deduplikacji na źródle. Do każdego z portów należy dostarczyć wkładkę 32Gb SW. Urządzenie musi umożliwiać podwojenie ilości portów Ethernet 10/25 Gb/s oraz Fibre Channel 32Gb.

6.	**Wydajność**	Urządzenie musi osiągać w maksymalnej konfiguracji wydajność backupu co najmniej 25 TB/hr z wykorzystaniem deduplikacji na źródle (dane podawane przez producenta). Urządzenie nie może zmniejszać swojej wydajności w czasie przybywania kolejnych danych. Urządzenie musi pozwalać na jednoczesną obsługę minimum **250** strumieni (zapis danych, odczyt danych, replikacja danych).
7.	**Sposób udostępniania zasobów**	Urządzenie musi umożliwiać jednoczesny dostęp do całej pojemności urządzenia wszystkimi poniższymi protokołami: • CIFS, NFS, VTL i deduplikacja na źródle (OST/Boost/Catalyst) dla interfejsów Ethernet, • VTL i deduplikacja na źródle (OST/Boost/Catalyst) dla interfejsów FC. Urządzenie musi posiadać obsługę mechanizmów deduplikacji dla danych otrzymywanych wszystkimi protokołami (CIFS, NFS, VTL, deduplikacja na źródle) przechowywanych w obrębie urządzenia. Oferowane urządzenie musi mieć możliwość emulacji napędów taśmowych LTO oraz emulacji bibliotek taśmowych. Urządzenie musi umożliwiać przyporządkowanie do pojedynczej biblioteki taśmowej minimum 100 napędów oraz 1 000 slotów na taśmy. Urządzenie musi umożliwiać udostępniania zasobów w trybie VTL po protokole FC i iSCSI. Jeżeli dla realizacji powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla nieograniczonej pojemności dostarczanego urządzenia.
8.	**Deduplikacja danych**	Urządzenie musi deduplikować dane inline przed zapisem na nośnik dyskowy. Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych. Oznacza to, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości. Proces deduplikacji musi odbywać się inline – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Rozwiązanie nie może w żadnej fazie korzystać (w całości lub częściowo) z dodatkowego bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej). Wszystkie unikalne, zdeduplikowane bloki przed zapisaniem na dysk muszą być kompresowane.

		Jeżeli dla realizacji powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla nieograniczonej pojemności dostarczanego urządzenia.
9.	**Replikacja danych**	Urządzenie musi umożliwiać replikację danych do drugiego urządzenia. Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane muszą być tylko te fragmenty danych (bloki), które nie znajdują się na docelowym urządzeniu. W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami. Musi istnieć możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami. Zarządzanie całym procesem kopiowania danych oraz wszystkimi kopiami musi być możliwy z poziomu oprogramowania backupowego. Jeżeli dla realizacji powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla nieograniczonej pojemności dostarczanego urządzenia.
10.	**Szyfrowanie danych**	Urządzenie musi mieć zaimplementowaną funkcjonalność wewnętrznego mechanizmu szyfrowania danych AES-256 realizowaną na poziomie urządzenia przy pomocy certyfikowanego algorytmu zgodnego ze standardem FIPS 140-2. Jeżeli dla realizacji powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla nieograniczonej pojemności dostarczanego urządzenia.
11	**Usuwanie przeterminowanych danych**	Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nienależące do backupów o aktualnej retencji) w procesie czyszczenia. Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu i odtwarzania danych.
12.	**Sposób zarządzania**	Urządzenie musi mieć możliwość zarządzania poprzez interfejs graficzny dostępny z przeglądarki internetowej. Oprogramowanie do zarządzania musi rezydować na oferowanym na urządzeniu deduplikacyjnym. Urządzenie musi umożliwiać ustawienie powiadomień administratora o problemach w urządzeniu za pomocą poczty elektronicznej.
13.	**Kompatybilność**	Urządzenie musi wspierać (wymagane formalne wsparcie producenta urządzenia) co najmniej następujące aplikacje backupujące

		bezpośrednio na oferowane urządzenie: Veeam, Commvault, Micro Focus Data Protector, Microsoft SQL, Oracle RMAN i SAP HANA. W przypadku przyjmowania backupów od powyżej wymienionych aplikacji kopii zapasowych urządzenie musi umożliwiać deduplikację na źródle i przesłanie tylko nowych, unikalnych bloków danych poprzez sieć FC i Ethernet.
14.	**Redundancja**	Redundantne zasilacze i wentylatory.
15.	**Dodatkowe wymagania**	Oferowane urządzenie musi być fabrycznie nowe, wyprodukowane w 2025 roku i pochodzić z oficjalnego kanału dystrybucyjnego producenta na rynek Unii Europejskiej. Zamawiający zastrzega sobie, aby Wykonawca na żądanie Zamawiającego przedłożył oświadczenie Producenta oferowanego sprzętu, w języku polskim, potwierdzające pochodzenie sprzętu z autoryzowanego kanału dystrybucji obejmującego rynek Unii Europejskiej.
16.	**Gwarancja**	Usługi będą w szczególności wykonywane w następujący sposób: • Okres wsparcia serwisowego producenta – 60 miesięcy realizowane w trybie NBD (next business day) • Czas reakcji serwisu na awarię – następny dzień roboczy. • Naprawy realizowane są zdalnie lub na miejscu w siedzibie Zamawiającego. • Uszkodzone dyski pozostają własnością Zamawiającego. W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z urządzeniem oraz oprogramowania wewnętrznego urządzenia. Gwarancja na sprzęt musi być dostarczona i realizowana przez organizację serwisową producenta sprzętu. Wykonawca musi zapewnić proces sprzedaży i serwisu urządzeń storage zgodnie z posiadanym przez producenta certyfikatem ISO 9001:2015 Serwis musi być realizowany przez producenta sprzętu w języku polskim.
17.	**Usługi instalacyjne**	Wykonawca dostarczy i zainstaluje deduplikator w szafie rack. Ponadto dokona aktualizacji firmware oraz sterowników do najnowszej dostępnej wersji na dzień dostawy. Instalacja realizowana przez certyfikowanego inżyniera producenta serwera.

Tabela 4. Wymagania dla 1 sztuki „Urządzenie repozytorium kopii zapasowych typu automatyka taśmowa”

Lp.	Nazwa komponentu	Wymagane parametry
1.	**Typ obudowy**	Urządzenie musi być przystosowane do montażu w szafie rack 19”.
2.	**Napędy taśmowe**	Posiadać minimum 1 napęd LTO-9 FC
3.	**Sposób pracy napędu**	Napęd z mechanizmem automatycznie dostosowującym prędkość przesuwu taśmy magnetycznej do wartości strumienia danych przekazywanych do napędu w zakresie minimum 101-300MB/s (dla zapisu bez kompresji).
4.	**Rodzaj obsługiwanych taśm LTO**	LTO-9 RW
5.	**Bezpieczeństwo**	Obsługa taśm typu WORM uniemożliwiających zmianę zapisanych danych. Urządzenie musi umożliwiać rozbudowę o szyfrowanie danych zapisywanych na taśmach czy to poprzez dedykowany zestaw USB czy poprzez licencję do serwera kluczy szyfrujących.
6.	**Sloty na taśmy**	Minimum 24 sloty na tamy LTO-9 oraz możliwość konfiguracji minimum 1 slotu typu mail, umożliwiającego wymianę pojedynczej taśmy bez konieczności wyjmowania całego magazynka z taśmami.
7.	**Możliwość rozbudowy**	Minimum o dodatkowy napęd LTO.
8.	**Podłączenie sieciowe**	Wymagane porty: • 1 x Ethernet dla interfejsu zarządzania; • 1 x 8Gb FC z wkładką.
9.	**Niezawodność**	MSBF – minimum 2 miliony cykli. MTBF – minimum 100 000 godzin. Urządzenie powinno posiadać możliwość proaktywnego monitorowania biblioteki, napędów oraz taśm pod kątem minimum utylizacji oraz wydajności. Jeżeli funkcjonalność ta jest dodatkowo licencjonowania, to należy ją dostarczyć wraz z urządzeniem.
10.	**Czytnik kodów taśmowych**	Urządzenie musi być wyposażone w czytnik kodów kreskowych umożliwiający na bieżąco odczyt barcodów taśm magnetycznych.

11.	**Partycjonowanie**	Urządzenie powinny umożliwiać partycjonowanie, tj. podział biblioteki na biblioteki o pojemności określonej przez użytkownika „biblioteki logiczne" a następnie podłączenie ich do różnych systemów wykorzystujących różne rodzaje oprogramowania do wykonywania kopii zapasowych czy archiwizacji. Podział możliwy dla maksymalnych parametrów fizycznych urządzenia, tj. dla ilości napędów i slotów.
12.	**Wsparcie dla oprogramowania**	Urządzenie musi wspierać (wymagane formalne wsparcie producenta urządzenia) co najmniej następujące aplikacje backupujące bezpośrednio na oferowane urządzenie: Veeam, Commvault, Micro Focus Data Protector.
13.	**Sposób zarządzania**	Urządzenie musi posiadać: • Możliwość zarządzania poprzez WWW; • Możliwość zdalnego monitorowania; • Wbudowany panel LED oraz zestaw diód LED informujący o stanie urządzenia.
14.	**Dodatkowe wymagania**	Oferowane urządzenie musi być fabrycznie nowe, wyprodukowane w 2025 roku i pochodzić z oficjalnego kanału dystrybucyjnego producenta na rynek Unii Europejskiej. Zamawiający zastrzega sobie, aby Wykonawca na żądanie Zamawiającego przedłożył oświadczenie Producenta oferowanego sprzętu, w języku polskim, potwierdzające pochodzenie sprzętu z autoryzowanego kanału dystrybucji obejmującego rynek Unii Europejskiej.
15.	**Gwarancja**	Usługi będą w szczególności wykonywane w następujący sposób: • Okres wsparcia serwisowego producenta – 60 miesięcy realizowane w trybie NBD (next business day) • Czas reakcji serwisu na awarię – następny dzień roboczy. • Naprawy realizowane są zdalnie lub na miejscu w siedzibie Zamawiającego. W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z urządzeniem oraz oprogramowania wewnętrznego urządzenia. Gwarancja na sprzęt musi być dostarczona i realizowana przez organizację serwisową producenta sprzętu. Wykonawca musi zapewnić proces sprzedaży i serwisu urządzeń storage zgodnie z posiadanym przez producenta certyfikatem ISO 9001:2015 Serwis musi być realizowany przez producenta sprzętu w języku polskim.

16.	**Usługi instalacyjne**	Wykonawca dostarczy i zainstaluje bibliotekę wraz z napędami w szafie rack. Ponadto dokona aktualizacji firmware oraz sterowników do najnowszej dostępnej wersji na dzień dostawy. Instalacja realizowana przez certyfikowanego inżyniera producenta serwera.
17.	**Media**	Wraz z urządzeniem należy dostarczyć: • 12 sztuk taśm LTO-9 typu RW; • 1 sztukę taśmy czyszczącej; • barcode dla minimum w/w ilości taśm.

Tabela 5. Wymagania dla 1 sztuki „Urządzenie sieciowe typu przełączniki w sieci SAN”

Lp.	Nazwa komponentu	Wymagane parametry
1.	**Przełączniki SAN**	Zamawiający informuje, iż w aktualnie posiadanym środowisku IT sieć typu SAN wdrożona jest w oparciu o rozwiązania firmy CISCO MDS 9000. Tym samym dostarczenie urządzeń firmy Bracoade nie jest możliwe, gdyż celem Zamawiającego jest rozbudowa posiadanej sieci SAN i uzyskanie pełnej kompatybilności pomiędzy urządzeniami. Zamawiający dopuszcza rozwiązania OEM.
2.	**Obudowa**	Urządzenie musi być przystosowane do montażu w szafie rack 19”.
3.	**Ilość portów**	Minimum 16, z czego 8 portów aktywnych. 32Gb FC Możliwość rozbudowania o 8 portów poprzez licencje oraz o dodatkowe 16 portów poprzez dedykowany moduł fizyczny i niezbędne licencje.
4.	**Ilość i typ wkładek**	Minimum 8 sztuk wkładek 32Gb FC Short Wave SFP+ Minimum 2 sztuki wkładek 32Gb FC Long Wave SFP+
5.	**Oprogramowanie**	Urządzenie powinno być dostarczone z systemem CISCO MDS 9000 NX-OS, z wsparciem dla minimum extended fabrics oraz hardware-enforced zoning.
6.	**Redundancja**	Redundantne zasilacze.
7.	**Dodatkowe wymagania**	Oferowane urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 12 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z oficjalnego kanału dystrybucyjnego producenta na rynek Unii Europejskiej (w tym kanału typu OEM).
8.	**Gwarancja**	Usługi będą w szczególności wykonywane w następujący sposób: • Okres wsparcia serwisowego producenta – 60 miesięcy realizowane w trybie NBD (next business day) • Czas reakcji serwisu na awarię – następny dzień roboczy. • Naprawy realizowane są zdalnie lub na miejscu w siedzibie Zamawiającego. W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z urządzeniem oraz oprogramowania wewnętrznego urządzenia. Gwarancja na sprzęt musi być dostarczona i realizowana przez organizację serwisową producenta sprzętu.

		Producent sprzętu musi posiadać certyfikat ISO 9001:2015 dla przedstawicielstwa w Polsce na sprzedaż oraz serwis urządzeń storage. Serwis musi być realizowany przez producenta sprzętu w języku polskim.
9.	**Usługi instalacyjne**	Wykonawca dostarczy i zainstaluje przełącznik SAN w szafie rack. Ponadto dokona aktualizacji firmware oraz sterowników do najnowszej dostępnej wersji na dzień dostawy. Instalacja realizowana przez certyfikowanego inżyniera producenta serwera. Na żądanie Zamawiającego, Wykonawca musi przedstawić certyfikaty inżyniera.

Tabela 6. Wymagania dla „Oprogramowanie kopii zapasowych”

Lp.	Nazwa komponentu	Wymagane parametry
1.	**Oprogramowanie do kopii zapasowych infrastruktury IT**	Zamawiający wymaga 200 sztuk/instancji licencji, do dowolnego wykorzystania zarówno na maszyny wirtualnej jak i systemy fizyczne. Zamawiający nie dopuszcza osobnego licencjonowania dla maszyn wirtualnych i systemów fizycznych. Licencje powinny uprawniać do wieczystego użytkowania oraz posiadać 5-cio letnie wsparcie producenta z możliwością zgłaszania problemów w trybie 24/7 i prawem do aktualizacji produktu w okresieobowiązywania wsparcia. Szczegółowy opis rozwiązania: Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter i powinno znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner Peer Insights i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5, Oprogramowanie musi spełniać następujące wymagania: - współpracować z infrastrukturą VMware w wersji 7.x i 8.0 oraz Microsoft Hyper-V 2016, 2019, 2022 i 2025. - zapewnić, aby wszystkie funkcjonalności wymienione w specyfikacji były dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej - współpracować z infrastrukturą Nutanix w wersji 6.5.x - 7.0, Red Hat Virtualization 4.4 SP1, Oracle Linux Virtualization 4.5.4 lub nowszy oraz Proxmox VE 8.2 lub nowszy. - zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure, Microsoft Azure Data Lake, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux. - posiadać niezależność sprzętową i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej

		- umożliwiać tworzenie “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków - posiadać mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji - zabronić przechowywania 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. - mieć warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla co najmniej trzech pamięci masowych to takiej puli. - zezwalać na przechowywanie kopii bezpieczeństwa w chmurze producenta. - 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. - wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu. - nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania - 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) - zapewniać możliwość delegacji uprawnień do odtwarzania na portalu - umożliwiać integrację z innymi systemami poprzez wbudowane RESTful API

		- mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji - posiadać wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji - zapewniać mechanizmy chroniące przed utratą hasła szyfrowania - posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych. - dysponować natywnym mechanizmem uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej - żądać autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np skasowanie backupu, dodanie kolejnego administratora) - dysponować możliwością integracji z systemami zarządzania kluczami szyfrującymi (KMS) - zapewniać integracje z systemami typu SIEM - mieć asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji. - wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej - uruchamiać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych. - oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna co najmniej dla platformy VMware i Hyper-V - 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.

		- posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware. - wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592). - mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) - pozwalać na bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard. - współpracować z 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. - umożliwiać kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN. - dysponować możliwością 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. - zapewniać 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 punku w ramach ustalonego parametru RPO. - mieć umożliwiać przechowywanie punktów przywracania dla replik - gwarantować możliwość wykorzystania istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding) - pozwalać na wykorzystanie wszystkich oferowanych przez hypervisor trybyów transportu (sieć, hot-add, LAN Free-SAN) - zapewnić jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, 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 uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) - 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 - zezwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre - akceptować 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. - zapewniać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków - umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform. - pozwalać na 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 - mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V. - wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell oraz przywracanie plików z partycji Linux LVM - umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.

		- dopuszczać 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. - umożliwiać backup i odtwarzanie usługi Entra ID. W szczególności użytkowników, grupy, role, jednostki administracyjne, entrprise applications oraz logi audytowe i sign-in. - pozwalać na granularne odtwarzanie Microsoft Exchange 2016 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego. - mieć mozliwość granularnego odtwarzanie Microsoft SQL 2016 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur. - wspierać granularne odtwarzanie Microsoft Sharepoint 2016 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji. - zapewniać 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. - dać możliwość granularnego odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux. - zapewniać granularne odtwarzanie baz danych MongoDB. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux. - wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji oraz pozwalać na specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN - posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN, SAP HANA, SAP Oracle, MS SQL VDI, IBM Db2 - mieć możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna

		umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych - 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 - zapewniać 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. - posiadać swój wbudowany program antywirusowy zoptymalizowany do przeszukiwania kopii backpowych - analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware - mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania Oprogramowanie, bazując na wyuczonym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków - posiadać mechanizm wykrywania oznak ataku hakerskiego tzw Indicators of Compromise - umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego. - zapewniać możliwość integracji z innymi systemami bezpieczeństwa - minimum Splunk, Palo Alto Networks XSOAR Rozwiązanie musi: - wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego oraz wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych

		- wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE, Rocky Linux, AlmaLinux oraz system operacyjny macOS Oprogramowanie musi umożliwiać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix Rozwiązanie musi zapewniać możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą) - wspierać systemy oparte o Microsoft Failover Cluster oraz umozliwiać odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów Rozwiązanie powinno wspierać: - backup podłączonych dysków USB - deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym - kontrolę pasma sieciowego - ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych - ograniczenia wykonywania backupów dla połączeń VPN - śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft - technologię BitLocker - szyfrowanie - uruchamianie z nośnika odtwarzania - odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2016 i nowszych, Microsoft Sharepoint 2016 i nowszych, Microsoft SQL 2016 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych - odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych - -odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform - możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne

		- tworzenie wielu zadań backupowych Rozwiązanie musi posiadać: - funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego - ochronę przed ransomware poprzez automatyczne odmontowanie - możliwość utworzenia nośnika po wykonanym backupie stacji klienckiej Rozwiązanie musi umożliwiać: - 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) - natychmiastowe publikowanie baz MS SQL, Oracle I PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu. - monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich - monitorowanie środowiska wirtualizacyjnego VMware w wersji, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie System musi umożliwiać: - monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2016, 2019, 2022 oraz 2025 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. - kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter - układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel - podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk - monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna - możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego

		- możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta - monitorowanie obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji - weryfikację odzyskiwalności maszyn wirtualnych. - granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy Vmware - raportowanie środowiska wirtualizacyjnego VMware w wersji 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie - raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2016, 2019, 2022 oraz 2025 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie - eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF - ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc - ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach - uwzględniania informacji o zmianach konfiguracji monitorowanych systemów - generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych - analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury - generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta - generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych - generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’ - granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy Vmware - generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots) - generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie

		System musi mieć wbudowane: - predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora - połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów - predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych - centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard) System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu. System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów. System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V

Tabela 7. Wymagania dla „Usługa wdrożeniowa”

Lp.	Nazwa komponentu	Wymagane parametry
1.	**Usługa wdrożeniowa**	Zamawiający wymaga dostawy wymienionych urządzeń, wraz z wyspecyfikowaną w nich usługą instalacji. Na etapie podpisania umowy Zamawiający wskaże lokalizacje w których poszczególne urządzenia powinny zostać zainstalowane. Podane lokalizacje to kampusy Zamawiającego znajdują się przy: 1. ul. Wóycickiego 1/3, Warszawa 2. ul. Dewajtis 5, Warszawa 3. ul. Marii Konopnickiej 1, Dziekanów Leśny Ponadto zamawiający wymaga usługi wdrożenia dostarczonego oprogramowania do kopii zapasowych. Usługę wdrożenia powinien przeprowadzić inżynier posiadający certyfikaty producenta minimum na poziomie inżyniera.
2.	**Szczegółowy opis usługi**	1. Przygotowanie projektu technicznego. 2. Instalacja urządzeń we wskazanych przez Zamawiającego lokalizacjach (w tym estetyczne ułożenie przewodów oraz oetykietowanie okablowania). 3. Aktualizacja oprogramowania układowego urządzeń (firmware) oraz niezbędnych sterowników. 4. Instalacja systemów operacyjnych (jeżeli są przedmiotem niniejszego postępowania). 5. Instalacja oprogramowania do kopii zapasowych. 6. Konfiguracja systemu kopii zapasowych oraz wdrożenie polityk retencyjnych zgodnie z projektem technicznym. 7. Przygotowanie środowiska i polityk testowania poprawności odtwarzania wybranych maszyn wirtualnych. 8. Wybrane testy odtworzenia. 9. Przygotowanie dokumentacji powykonawczej. 10. Szkolenia stanowiskowe z obsługi dostarczonych urządzeń (maksymalnie 8h roboczych) oraz oprogramowania do kopii zapasowych (maksymalnie 16h roboczych).