

Opis przedmiotu zamówienia (OPZ) na Wdrożenie pełnego systemu kopii zapasowej w modelu 3-2-1

1.1 Przedmiot zamówienia

Przedmiotem zamówienia jest dostarczenie sprzętowego urządzenia deduplikacyjne, serwera rack, usługi wdrożenia i szkolenia dla Administratorów.

Lp.	Nazwa	Liczba sztuk
1	Sprzętowe urządzenia deduplikacyjne	2
2	Serwer rack	1
3	Integracja oprogramowania	1
4	Usługa wdrożenia oraz szklenia	1

1.2 Wymagania sprzętowe: urządzenia deduplikacyjne

Lp.	Parametr wymagany
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 minimum 12TB netto (powierzchni użytkowej widocznej po założeniu systemu plików) bez uwzględnienia mechanizmów protekcji – przestrzeń dedykowana do gromadzenia deduplikatorów, wymagana skalowalność do minimum 170TB netto (powierzchni użytkowej widocznej po założeniu systemu plików).
3	Dostarczone urządzenie musi umożliwiać 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 przemieszczane (w postaci zdeduplikowanej) na dodatkową warstwę, wymagane wsparcie dla AWS, MS Azure oraz Google GCP. Wymagana enkrypcja danych przechowywanych w warstwie typu Cloud. Wymagane dostarczenie licencji na przestrzeń minimum 60TB netto dla warstwy Cloud. Wymagana funkcjonalność i kompatybilność z aplikacją Veeam Backup and Replication oraz aplikacją NetWorker.
4	Oferowane urządzenie musi posiadać minimum: 8 portów 10Gb/s Ethernet OP. Wymagana możliwość obsługi każdym z wyżej wymienionych portów protokołów: CIFS, NFS, deduplikacja na źródle. Wymagana możliwość dodania do wyżej wymienionej konfiguracji portów: 2 porty FC 16Gb/s. Wymagana możliwość obsługi poprzez porty FC protokołów VTL oraz deduplikacji na źródle.
5	Oferowane urządzenie musi umożliwiać jednoczesny dostęp wszystkimi poniższymi protokołami: - CIFS, NFS, - Zapewniającym deduplikację na źródle, wymagane wsparcie dla aplikacji Veeam Backup and Replication oraz aplikacji NetWorker, - VTL (minimum 10 jednocześnie).
6	Wymagane jest dostarczenie licencji, pozwalającej na jednoczesną obsługę protokołów CIFS, NFS, deduplikacja na źródle, VTL do oferowanej pojemności urządzenia.
7	Oferowane pojedyncze urządzenie musi osiągać zagregowaną wydajność (dla maksymalnej konfiguracji) protokołami: NFS co najmniej 10TB/h (dane podawane przez producenta) oraz co najmniej 20TB/h z wykorzystaniem deduplikacji na źródle (dane podawane przez producenta).
8	Urządzenie musi pozwalać na jednoczesną obsługę minimum 250 strumieni w tym jednocześnie: - zapis danych minimum 150 strumieniami, - odczyt danych minimum 50 strumieniami, - replikacja minimum 50 strumieniami, pochodzących z różnych aplikacji oraz dowolnych protokołów (CIFS, NFS, VTL, deduplikacja na źródle) oraz dowolnych interfejsów (FC, LAN) w tym samy czasie. Wymienione wartości 250 jednoczesnych strumieni dla wszystkich protokołów (czyli jednocześnie 150 dla zapisu i jednocześnie 50 strumieni dla odczytu i jednocześnie 50 strumieni dla replikacji)

	musi mieścić się w przedziale oficjalnie rekomendowanym i wspieranym przez producenta urządzenia. Wszystkie zapisywane strumienie muszą podlegać globalnej deduplikacji przed zapisem na dysk (in-line) jak opisano w niniejszej specyfikacji.
9	Oferowane urządzenie musi mieć możliwość emulacji następujących bibliotek taśmowych: • StorageTek L180, • IBM TS 3500.
10	Oferowane urządzenie musi mieć możliwość emulacji napędów taśmowych minimum LT05 oraz LT07.
11	Urządzenie musi umożliwiać (w przypadku VTL'a) emulację minimum 250 napędów, emulację minimum 30 000 slotów w przypadku pojedynczej biblioteki taśmowej oraz emulację sumaryczną minimum 60 000 slotów.
12	Oferowane urządzenie musi deduplikować dane in-line przed zapisem na nośniku dyskowym. Na wewnętrznych dyskach urządzenia nie mogą być zapisywane dane w oryginalnej postaci (niezdeduplikowane) z jakiegokolwiek fragmentu strumienia danych przychodzącego do urządzenia.
13	Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku jednak o wielkości 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.
14	Oferowany produkt musi posiadać obsługę mechanizmów globalnej deduplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, VTL, deduplikacja na źródle) przechowywanych w obrębie całego 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.
15	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. 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.

16	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).
17	Wszystkie unikalne bloki przed zapisaniem na dysk muszą być dodatkowo kompresowane.
18	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.
19	Oferowane urządzenie musi wspierać (wymagane formalne wsparcie producenta urządzenia), co najmniej następujące aplikacje: Veeam Backup and Replication, Veeam Enterprise, NetWorker, W przypadku współpracy z każdą z poniższych aplikacji: • Veeam Backup and Replication, • Veeam Enterprise • NetWorker, urządzenie musi umożliwiać deduplikację na źródle (w przypadku Veeam B&R i Veeam Enterprise: na poziomie – proxy Data Mover, w przypadku NetWorker na poziomie – Client i przesłanie nowych, nie znajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN. Deduplikacja w wyżej wymienionych przypadkach musi zapewniać, aby do oferowanego urządzenia były transmitowane poprzez sieć – LAN jedynie fragmenty danych nie znajdujące się dotychczas na urządzeniu.
20	W przypadku przyjmowania backupów z Veeam Backup and Replication, Veeam Enterprise, NetWorker urządzenie musi umożliwiać deduplikację na źródle (w przypadku Veeam B&R i Veeam Enterprise: na poziomie - proxy Data Mover, w przypadku NetWorker na poziomie - Client i przesłanie nowych, nieznajdujących się jeszcze na urządzeniu bloków poprzez sieć FC. Deduplikacja w wyżej wymienionych przypadkach musi zapewniać, aby z serwerów do urządzenia były transmitowane poprzez sieć FC tylko fragmenty danych nie znajdujące się dotychczas na urządzeniu.
21	Oferowane urządzenie musi umożliwiać uruchamianie maszyn wirtualnych VMware bezpośrednio z danych backupowych bez konieczności odtwarzania danych, funkcjonalność ta musi być wspierana przez Veeam Backup and Replication, Veeam Enterprise oraz NetWorker.
22	Wymagana funkcjonalność Load Balancing oraz Link Failover w obrębie portów wykorzystywanych przez aplikację backupową, wymagane wsparcie tej funkcjonalności dla Veeam Backup and Replication, Veeam Enterprise oraz NetWorker.
23	Wymagane wsparcie dla backupów typu Virtual Synthetics w przypadku aplikacji Veeam Backup and Replication, Veeam Enterprise oraz NetWorker.
24	W przypadku deduplikacji na źródle poprzez sieć IP (LAN oraz WAN), wymagana możliwość szyfrowania komunikacji kluczem minimum 256 bitów.
25	Urządzenie musi umożliwiać zaszyfrowanie przechowywanych danych, wymagane licencje umożliwiające zaszyfrowanie i przechowywanie zaszyfrowanych danych w obrębie maksymalnej pojemności oferowanego urządzenia.
26	Urządzenie musi wspierać deduplikację na źródle poprzez sieć FC (SAN) minimum dla następujących systemów operacyjnych:

	• Windows, • Linux (RedHat, SuSE).
27	Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych do drugiego urządzenia takiego samego typu. Konfiguracja replikacji musi być możliwa w każdym z trybów: * jeden do jednego, * wiele do jednego, * jeden do wielu, * kaskadowej (urządzenie A replikuje dane do urządzenia B, które te same dane replikuje do urządzenia C). 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 jest przedmiotem postępowania.
28	Urządzenie musi umożliwiać wydzielenie określonych portów Ethernet dedykowanych do replikacji.
29	W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami.
30	W przypadku replikacji danych między dwoma urządzeniami oferowanego typu, wymagana możliwość kontroli przez: NetWorker, muszą być możliwe do uzyskania jednocześnie wszystkie następujące funkcjonalności: • replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału serwerów pośredniczących, • replikacji podlegają tylko te fragmenty danych (na poziomie bloków używanych do deduplikacji), które nie znajdują się na docelowym urządzeniu, • replikacja zarządzana jest z poziomu wymaganej aplikacji, • aplikacja posiada informację o obydwu kopiach zapasowych znajdujących się w obydwu urządzeniach bez konieczności przeprowadzania procesu inwentaryzacji.
31	Oferowane urządzenie musi działać poprawnie przy wypełnieniu danymi na poziomie co najmniej 90%. Dokumentacja urządzenia nie może wskazywać na ew. problemy, obostrzenia, które są efektem wypełnienia urządzenia zabezpieczanymi danymi, na poziomie mniejszym niż 90%.
32	Wymagana możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami oferowanego typu — oferowane urządzenie powinno być wyposażone w mechanizm umożliwiający zarządzaniem stopnia wykorzystania pasma na potrzeby replikacji.
33	Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6 bądź równoważnej.
34	Oferowane urządzenie musi pozwalać na 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).
35	Urządzenie musi pozwalać na przechowywanie minimum 500 Snapshotów jednocześnie w obrębie oferowanej przestrzeni, przy zachowaniu globalnej deduplikacji oraz standardowego trybu pracy urządzenia — umożliwiającego wykorzystanie wszystkich dostępnych funkcjonalności.

36	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).
37	Urządzenie musi mieć możliwość podziału na minimum 10 logicznych części pracujących równolegle. Producent musi oficjalnie wspierać pracę minimum 10 logicznych części pracujących równolegle z pełną wydajnością urządzenia.
38	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.
39	Wymagana możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia jako niezależnego urządzenia dostępnego za pośrednictwem: • CIFS, • NFS, • VTL, • deduplikacja na źródle.
40	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): 1. Możliwość zdjęcia blokady przed upływem ważności danych 2. Brak możliwości zdjęcia blokady przed upływem ważności danych (COMPLIANCE), w tym wypadku wymagane wsparcie norm SEC 17a-4(f) oraz ISO Standard 15489-1 w zakresie ochrony danych, wymagane oficjalne wsparcie aplikacji Veeam Backup and Replication oraz NetWorker. Licencje na blokadę usunięcia/zmiany przechowywanych plików muszą być dostarczone wraz z urządzeniem. Wymagana możliwość automatycznego uruchamiania blokady (podczas zapisu) WORM dla danych zapisywanych na obszar objęty działaniem wspomnianej blokady. W każdym przypadku wymagana również możliwość używania blokady WORM dla obrazu danych uzyskanych poprzez użycie wymaganej funkcjonalności SnapShot. Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności.
41	Urządzenie musi mieć możliwość przechowywania danych niezmiennych: • Video, • Grafika, • Nagrania dźwiękowe, • Pliki pdf, na udziałach CIFS/NFS.
42	Urządzenie musi weryfikować dane po zapisie (nie chodzi o ew. weryfikację danych indeksowych generowanych przez urządzenie, ale o weryfikację wszystkich zabezpieczanych danych backup'owych). Każda zapisana na dyskach porcja danych musi być odczytana i porównana z danymi otrzymanymi przez urządzenie. Powyższa weryfikacja musi być realizowana w locie, czyli przed usunięciem z pamięci oryginalnych danych (otrzymanych z aplikacji backupowej), musi być realizowana w trybie ciągłym (a nie ad-hoc), wymagane parametry wydajnościowe urządzenia muszą uwzględniać tę funkcjonalność. Wymagane potwierdzenie opisanej funkcjonalności w oficjalnej dokumentacji producenta oferowanego urządzenia. Zamawiający zastrzega możliwość prośby o dostarczenie

	ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności).
43	Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia.
44	Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu).
45	Wymagana możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora), wymagane potwierdzenie w ogólnodostępnej dokumentacji. Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności).
46	Wymagana możliwość zdefiniowania harmonogramu wg. którego wykonywany jest proces usuwania przeterminowanych danych (czyszczenia), realizowany równolegle z procesami backup/restore/replication.
47	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).
48	Urządzenie musi umożliwiać systemowo (wbudowana funkcjonalność) - realizację procesu pierwszego czyszczenia dopiero po przekroczeniu 75% zajętości oferowanej przestrzeni.
49	Urządzenie musi mieć możliwość zarządzania poprzez: • interfejs graficzny dostępny z przeglądarki internetowej, • poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell).
50	Oprogramowanie do zarządzania musi rezydować na oferowanym na urządzeniu deduplikacyjnym.
51	Oferowane urządzenie musi mieć możliwość sprawdzenia pakietu upgrade'ującego firmware urządzenia (GUI lub CLI), to znaczy sprawdzenia czy nowa wersja systemu nie spowoduje problemów z urządzeniem.
52	Urządzenie musi być rozwiązaniem kompletnym, apliancem sprzętowym pochodzącym od jednego producenta. Zamawiający nie dopuszcza stosowania rozwiązań typu gateway. Oferowany typ urządzenia musi być oficjalnie dostępne w ofercie producenta przed ukazaniem się niniejszego postępowania.
53	Oferowane urządzenie powinno być objęte 5-cio letnim wsparciem producenta działającym w trybie zgłaszania awarii: 24x7 oraz reakcją NBD.

1.3 Wymagania sprzętowe: serwer rack

Lp	Typ	Parametr wymagany
1	Obudowa	- Obudowa Rack o wysokości max 1U z możliwością instalacji min. 10 dysków 2,5". - Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze. - Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/Apple iOS) przy użyciu jednego z protokołów BLE/WIFI.
2	Płyta główna	- Płyta główna z możliwością zainstalowania do dwóch procesorów. - Płyta główna powinna obsługiwać do 8TB pamięci RAM. - Na płycie głównej powinno znajdować się minimum 32 sloty przeznaczone do instalacji pamięci. - Płyta główna musi być kompatybilna z zaprojektowanym rozwiązaniem - Możliwość obsługi procesorów 40 rdzeniowych
3	Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
4	Procesor	Zainstalowany jeden procesor, klasy x86, dedykowane do pracy z zaoferowanym serwerem, umożliwiające osiągnięcie wyniku min. 261 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
5	RAM	256GB DDR4 RDIMM 3200MT/s.
6	Funkcjonalność pamięci RAM	- Advanced ECC, - Memory Page Retire, - Fault Resilient Memory, - Memory Self-Healing lub PPR, - Partial Cache Line Sparing.
7	Kontroler RAID	- Sprzętowy kontroler dyskowy, posiadający: - min. 8GB nieulotnej pamięci cache, - możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60, - wsparcie dla dysków samoszyfrujących.
8	Dyski twarde	- Zainstalowane: 8 dysków SSD SATA o pojemności min. 3.84TB, 2,5"Hot-Plug (1 DWPD), - zainstalowane dwa dyski M.2 SATA o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. - Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnek na dyski twarde.
9	Gniazda PCI	Minimum trzy sloty PCIe x16 generacji 4.
10	Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 4 interfejsy sieciowe 10Gb Ethernet w standardzie Fiber Optic (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
11	Wbudowane porty	Przednie: min. 1x VGA, min. 1x USB 2.0, min. 1x micro-USB dedykowane dla karty zarządzającej.

		• Tylne: min. 1x VGA, min. 2x USB w tym 1x USB 3.0.
12	Zasilacze	• Redundantne, Hot-Plug min. 1100W każdy.
13	Elementy montażowe	• Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. • Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych.
14	Video	• Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200.
15	Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła. • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 V3. • Możliwość dynamicznego włączania i wyłączania portów USB na obudowie — bez potrzeby restartu serwera. • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera — niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem. • Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
16	Karta zarządzania	• Niezależna od zainstalowanego na serwerze systemu operacyjnego, karta zarządzająca, posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: ○ zdalny dostęp do graficznego interfejsu Web karty zarządzającej; ○ zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); ○ szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika; ○ możliwość podmontowania zdalnych wirtualnych napędów; ○ wirtualną konsolę z dostępem do myszy, klawiatury; ○ wsparcie dla IPv6; ○ wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; ○ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; ○ możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; ○ integracja z Active Directory; ○ możliwość obsługi przez dwóch administratorów jednocześnie; ○ wsparcie dla dynamic DNS; ○ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. ○ możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera ○ możliwość zarządzania do 100 serwerów

		bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności o: ○ Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej ○ Przesyłanie danych telemetrycznych w czasie rzeczywistym ○ Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze ○ Automatyczna rejestracja certyfikatów (ACE)
17	Oprogramowanie do zarządzania	• Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: ○ Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych o integracja z Active Directory ○ Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta ○ Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish ○ Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram ○ Szczegółowy opis wykrytych systemów oraz ich komponentów ○ Możliwość eksportu raportu do CSV, HTML, XLS, PDF ○ Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. ○ Grupowanie urządzeń w oparciu o kryteria użytkownika ○ Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji ○ Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach ○ Szybki podgląd stanu środowiska ○ Podsumowanie stanu dla każdego urządzenia ○ Szczegółowy status urządzenia/elementu/komponentu ○ Generowanie alertów przy zmianie stanu urządzenia. ○ Filtry raportów umożliwiające podgląd najważniejszych zdarzeń ○ Integracja z service desk producenta dostarczonej platformy sprzętowej ○ Możliwość przejęcia zdalnego pulpitu ○ Możliwość podmontowania wirtualnego napędu ○ Kreator umożliwiający dostosowanie akcji dla wybranych alertów ○ Możliwość importu plików MIB ○ Przesyłanie alertów „as-is” do innych konsol firm trzecich ○ Możliwość definiowania ról administratorów ○ Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów ○ Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) ○ Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta ○ Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów ○ Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i

		gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. ○ Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. ○ Wdrażanie serwerów, rozwiązań modułowych oraz przełączników sieciowych w oparciu o profile ○ Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. ○ Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. ○ Zdalne uruchamianie diagnostyki serwera. ○ Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. ○ Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
18	Oprogramowanie do monitorowania	Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności: • Monitoring: ○ ilość podłączonych oraz rozłączonych systemów ○ stan podłączonych urządzeń ○ informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów ○ Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia ○ informacje o statusie gwarancji dla poszczególnych urządzeń ○ informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń ○ informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. ○ Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych ○ Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. ○ Monitorowanie wydajności, przepustowości oraz opóźnień dla systemu pamięci masowych. ○ Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. ○ Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. ○ Monitoring parametrów serwerów z informacją o minimum: ▪ Obciążeniu procesora ▪ Zużyciu pamięci RAM ▪ Temperaturze procesorów

		▪ Temperaturze powietrza wlotowego ▪ Zużyciu prądu ▪ Zmianach w fizycznej konfiguracji serwera ▪ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ○ Monitoring parametrów pamięci masowych z informacją o minimum: ▪ Opóźnieniach ▪ IOPS ▪ Przepustowości ▪ Utylizacji kontrolerów ▪ Pojemność całkowita i dostępna ▪ Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów. ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ▪ Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata ▪ Informacje o poziomie redukcji danych ▪ Informacje o statusie replikacji oraz snapshotów ○ Monitoring parametrów przełączników sieciowych z informacją o minimum: ▪ Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny ▪ Stanie komponentów: zasilacze, wentylatory ▪ Podłączonych hostach ▪ Ilości i statusu portów ▪ Utylizacji procesora ▪ Utylizacji poszczególnych portów ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ○ Aktualizacja firmware ▪ możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania ▪ możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania ▪ możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiązań HCI, wraz z informacją o zalecanych wersjach oprogramowania ▪ możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania ▪ możliwość aktualizacji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania • Raporty ○ Możliwość generowania raportów dla serwerów zawierających informację o: ▪ Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole
--	--	---

		- komunikacyjnym z systemem pamięci masowej ▪ Średnim obciążeniu: procesorów, pamięci RAM, IO, ○ Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: ▪ Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji ○ Generowanie raportów do plików CSV i PDF • Cyberbezpieczeństwo ○ Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa a oraz sposobie ich zabezpieczenia. ○ Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. ○ Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. ○ Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. • Wspierane urządzenia ○ Urządzenie Producenta dostarczane w ramach postępowania ○ Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) • Wirtualny asystent ○ Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; • Możliwość rozszerzenia funkcjonalności ○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. • Inne ○ Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android • Certyfikaty ○ Oferowana platforma musi być zaprojektowana zgodnie ze standardami: ▪ ISO 27001 ▪ NIST Security and Privacy Controls for Federal Information Systems and Organization ▪ CSA Cloud Control Matrix
19	Wspierany system operacyjny	• Canonical* Ubuntu" Server LTS • Citrix" Hypervisor" • Microsoft® Windows Server® with Hyper-V • Red Hat® Enterprise Linux • SUSE* Linux Enterprise server • VMware® ESXi®
20	Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE.

		- Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25- gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Bronze według normy wprowadzonej w 2019 roku - Wykonawca złoży dokument potwierdzający spełnianie wymogu. - Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022.
21	Dokumentacja użytkowa	- Zamawiający wymaga dokumentacji w języku polskim lub angielskim. - Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
22	Warunki gwarancji	- Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 5 lat. - Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. - Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych) - Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. - Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon/aplikacja /portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. - Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. - Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. - Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także

		ocena bezpieczeństwa cybernetycznego. • 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. • Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: ○ Możliwości utworzenia zgłoszenia serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. ○ Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. ○ Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. ○ Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. ○ Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. • Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzeń — dokumenty potwierdzające należy załączyć do oferty.
--	--	---

1.4 Integracja oprogramowania

Lp	Opis wymagań
1	• Zamawiający posiada oprogramowanie do backupu. Wymagana jest integracja oprogramowania Zamawiającego z proponowanym rozwiązaniem. • Zamawiający obecnie używa oprogramowania: Veeam w wersji Enterprise
2	• Zamawiający wymaga integracji oprogramowania z „Dobrymi praktykami”. • Wymagana jest wcześniejsza analiza obecnego oprogramowania posiadanego przez Zamawiającego.

1.5 Wymagania: Usługa wdrożenia oraz szkolenia

Zamawiający wymaga wykonania poniższych usług, gwarantujących składowania kopii na 3 urządzeniach z gwarancją bezpieczeństwa (brak możliwości modyfikacji i skasowania, zgodnie z założonymi czasami blokady).

Lp	Opis
Etap 1.	Montaż i okablowania urządzeń deduplikujących oraz serwera dla bezpiecznego repozytorium w szafie.
Etap 2.	Instalacja i konfiguracja systemu na serwerze.
Etap 3.	Integracja serwera z systemem backupowym z włączeniem blokady kasowania i modyfikacji danych.
Etap 4.	Instalacja i konfiguracja deduplikatorów: • konfiguracja niezbędnych użytkowników • zabezpieczenie urządzeń przed uszkodzeniem/skasowaniem z poziomu konsoli zarządzania urządzeniem • włączenie polityk bezpieczeństwa • włączenie blokady kasowania danych dla wszystkich logicznych części urządzenia biorących udział w procesie składowania danych • ustawienie monitoringu zajętości logicznych części urządzenia na dane składowane po kompresji • integracja z systemem backupowym Veeam • konfiguracja agregacji portów ETH po stronie urządzenia • konfiguracja zabezpieczeń obiektów/stref • wykonanie replikacji pomiędzy urządzeniami • wykonanie testowych odtworzeń dla 5 wskazanych maszyn przez klienta • wykonanie dokumentacji powdrożeniowej systemu backup obejmującej (system backup, serwer, deduplikatory)
Etap 5.	Integracja oprogramowania do backupu Zamawiającego z zaproponowanym rozwiązaniem
Etap 6.	Instruktaż powdrożeniowy dla Administratorów systemu: min. 8h w terminach wcześniej ustalonych i potwierdzonych przez Zamawiającego.