

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

a) wdrożenie

Poprzez wdrożenie Zamawiający rozumie jako:

- instalację w szafie rack wskazanej przez Zamawiającego
- konfigurację urządzenia zgodnie z dobrymi praktykami i zaleceniami producenta w środowisku Zamawiającego

b) system kopii bezpieczeństwa i archiwizacji

Lp.	Parametr wymagany
1.	Urządzenie musi być przeznaczone do deduplikacji i przechowywania kopii zapasowych.
2.	Urządzenie na poziomie systemu operacyjnego urządzenia musi mieć możliwość replikacji do użytkowanego przez Zamawiającego systemu PowerProtect DD6400.
3.	Dostarczone urządzenie musi oferować przestrzeń min. 48TB netto (powierzchni użytkowej) bez uwzględniania mechanizmów protekcji.
4.	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 przemieszczone (w postaci zdeduplikowanej) na dodatkową warstwę. Wymagane wsparcie dla AWS oraz Microsoft Azure. Wymagana enkrypcja danych przechowywanych na warstwie typu Cloud. Wymagane dostarczenie licencji na przestrzeń min. 200TB netto dla warstwy CLOUD. Wymagana funkcjonalność powinna wspierać eksploatowaną przez Zamawiającego aplikację Networker.
5.	Oferowane urządzenie musi posiadać minimum 8 portów Eth 10 Gb/s RJ45. Wymagana możliwość obsługi w każdym z w/w portów protokołów CIFS, NFS, deduplikacja na źródle. Wymagana jest możliwość rozbudowy o 2 porty FC 16Gb/s. Wymagana obsada wszystkich portów wkładkami, wymagana możliwość obsługi poprzez porty FC protokołów VTL oraz deduplikacja na źródle.
6.	Oferowane urządzenie musi umożliwiać jednoczesny dostęp wszystkimi poniższymi protokołami: <ul style="list-style-type: none"> • CIFS, NFS • zapewniającym deduplikację na źródle, wymagane wsparcie dla eksploatowanych przez Zamawiającego aplikacji Networker i Avamar • VTL (min. 10 jednocześnie).
7.	Wymagane jest dostarczenie licencji, pozwalającej na jednoczesną obsługę protokołów CIFS, NFS, deduplikacja na źródle, VTL do oferowanej pojemności urządzenia.
8.	Oferowane pojedyncze urządzenie musi osiągać zagregowaną wydajność (dla maksymalnej konfiguracji) protokołami: NFS co najmniej 10 TB/h (dane podawane przez producenta) oraz co najmniej 20 TB/h z wykorzystaniem deduplikacji na źródle (dane podawane przez producenta).
9.	Urządzenie musi pozwalać na jednoczesną obsługę minimum 250 strumieni w tym jednocześnie: <ul style="list-style-type: none"> • zapis danych minimum 150 strumieniami,

	<ul style="list-style-type: none"> • odczyt danych minimum 50 strumieniami, • replikacja minimum 50 strumieniami, <p>pochodzących z różnych aplikacji oraz dowolnych protokołów (CIFS, NFS, VTL, deduplikacja na źródle) oraz dowolnych interfejsów (FC, LAN) w tym samym 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) muszą mieścić się w przedziale oficjalnie rekomendowanym i wspieranym przez producenta urządzenia. Wszystkie zapisywane strumienie muszą podlegać globalnej deduplikacji przed zapisem na dysk (in-line).</p>
10.	<p>Oferowane urządzenie musi mieć możliwość emulacji następujących bibliotek taśmowych:</p> <ul style="list-style-type: none"> • StorageTek L180 lub • IBM TS 3500
11.	<p>Oferowane urządzenie musi mieć możliwość emulacji napędów taśmowych min. LTO5 oraz LTO7</p>
12.	<p>Urządzenie musi umożliwiać (w przypadku VTL'a) emulację minimum 250 napędów, emulację min. 30 000 slotów w przypadku poj. biblioteki taśmowej oraz emulację sumarycznie min. 60 000 slotów.</p>
13.	<p>Oferowane urządzenie musi deduplikować dane in-line przed zapisem na nośnik dyskowy. Na wewnętrznych dyskach urządzenia nie mogą być zapisywane dane w oryginalnej postaci (niezdeduplikowanej) z jakiegokolwiek fragmentu strumienia danych przychodzącego do urządzenia.</p>
14.	<p>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.</p>
15.	<p>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.</p>

	W przypadku niespełnienia opisanego powyżej wymogu globalnej deduplikacji, przy spełnieniu pozostałych wymaganych funkcjonalności, oferowane urządzenie powinno oferować przestrzeń min. 300TB netto (powierzchni użytkowej) bez uwzględniania mechanizmów protekcji
16.	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.
17.	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)
18.	Wszystkie unikalne bloki przed zapisaniem na dysk muszą być dodatkowo kompresowane.
19.	Oferowane urządzenie musi wspierać (wymagane formalne wsparcie producenta urządzenia), co najmniej następujące aplikacje: Networker, Avamar, Veeam Backup and Replication, RMAN, Microsoft SQL Server Management Studio. W przypadku współpracy z każdą z poniższych aplikacji: <ul style="list-style-type: none"> • Networker • Avamar • Veeam Backup and Replication • RMAN (dla ORACLE) • Microsoft SQL Server Management Studio (dla Microsoft SQL) urządzenie musi umożliwiać deduplikację na źródle i przesłanie nowych, nie znajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN. Deduplikacja w wyżej wymienionych przypadkach musi zapewniać aby z zabezpieczanych serwerów do urządzenia były transmitowane poprzez sieć LAN jedynie fragmenty danych nie znajdujące się dotychczas na urządzeniu.
20.	W przypadku przyjmowania backupów z Networker, Veeam Backup and Replication, Oracle RMAN oraz Microsoft MSSQL (przy wykorzystaniu Microsoft SQL Server Management Studio), urządzenie musi umożliwiać deduplikację na źródle 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.	W przypadku systemów LINUX (min.: RedHat oraz SuSE) oraz Windows urządzenie powinno umożliwiać deduplikację na źródle na poziomie systemu plików. Dane kopiowane na wydzielony system plików (bez pośrednictwa aplikacji backupowej) powinny podlegać deduplikacji.
22.	Oferowane urządzenie powinno umożliwiać uruchamianie maszyn wirtualnych VMware bezpośrednio z danych backupowych bez konieczności odtwarzania danych, funkcjonalność ta powinna być wspierana przez aplikację backupową Networker.
23.	Wymagana funkcjonalność Load Balancing oraz Link Failover w obrębie portów wykorzystywanych przez aplikację backupową, wymagane wsparcie tej funkcjonalności dla aplikacji backupowej Networker, Avamar, Veeam Backup and Replication.

24.	Wymagane wsparcie dla backupów typu Virtual Synthetics w przypadku eksploatowanej aplikacji Networker.
25.	W przypadku deduplikacji na źródle poprzez sieć IP (LAN oraz WAN), wymagana możliwość szyfrowania komunikacji kluczem minimum 256 bitów.
26.	Urządzenie powinno umożliwiać zaszyfrowanie przechowywanych danych, wymagane licencje umożliwiające zaszyfrowanie i przechowywanie zaszyfrowanych danych w obrębie maksymalnej pojemności oferowanego urządzenia.
27.	Urządzenie musi wspierać deduplikację na źródle poprzez sieć FC (SAN) minimum dla następujących systemów operacyjnych: <ul style="list-style-type: none"> • Windows • Linux (RedHat, SuSE)
28.	Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych do drugiego urządzenia takiego samego typu. Konfiguracja replikacji musi być możliwa w każdym z trybów: <ul style="list-style-type: none"> * 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. Licencja na replikację jest przedmiotem postępowania.
29.	Urządzenie musi umożliwiać wydzielenie określonych portów Ethernet dedykowanych do replikacji.
30.	W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami.
31.	W przypadku replikacji danych między dwoma urządzeniami oferowanego typu, wymagana możliwość kontroli przez: Microsoft SQL Server Management Studio, muszą być możliwe do uzyskania jednocześnie wszystkie następujące funkcjonalności: <ul style="list-style-type: none"> • replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału serwerów pośredniczących • replikacji podlegają tylko te fragmenty danych, 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
32.	Oferowane urządzenie musi działać poprawnie przy zapełnieniu danymi na poziomie co najmniej 90%. Dokumentacja urządzenia nie może wskazywać na ew. problemy, obostrzenia, które są efektem zapełnieniu urządzenia zabezpieczanymi danymi, na poziomie mniejszym niż 90%.
33.	Wymagana możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami – oferowane urządzenie powinno być wyposażone w mechanizm umożliwiający zarządzaniem stopnia wykorzystania pasma na potrzeby replikacji.
34.	Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6 bądź równoważnej.
35.	Oferowane urządzenie musi umożliwiać wykonywanie 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).
36.	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.
37.	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).
38.	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.
39.	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.
40.	Wymagana możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia, jako niezależnego urządzenia dostępnego za pośrednictwem: <ul style="list-style-type: none"> • CIFS • NFS • VTL • deduplikacja na źródle
41.	<p>Urządzenie powinno 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):</p> <ol style="list-style-type: none"> 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) lub ISO Standard 15489-1 w zakresie ochrony danych <p>Licencje na blokadę usunięcia/zmiany przechowywanych plików muszą być dostarczone wraz z urządzeniem.</p> <p>W przypadku braku wymaganej funkcjonalności WORM, wymagana dostawa dodatkowej macierzy typu NAS (NFS/CIFS) o pojemności netto dwukrotnie większej od wymaganej pojemności netto deduplikatora (40TB x 2 = 80TB netto), o wydajności nie mniejszej od deduplikatora będącego przedmiotem zapytania, wyposażona w funkcjonalność WORM macierz musi spełniać wymagania dot. ochrony danych określone normami SEC 17a-4(f) lub ISO Standard 15489-1.</p>

	W każdym przypadku 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.
42.	Urządzenie musi mieć możliwość przechowywania danych niezmiennych: <ul style="list-style-type: none"> • Video • Grafika • Nagrania dźwiękowe • Pliki pdf na udziałach CIFS/NFS.
43.	Urządzenie musi weryfikować dane po zapisie (nie chodzi o ew. weryfikację danych indeksowych generowanych przez urządzenie ale o weryfikację wszystkich zabezpieczonych danych backup'owych). Każda zapisana na dyskach porcja danych musi być odczytana i porównana z danymi otrzymanymi przez urządzenie. Powyższa weryfikacja powinna być realizowana w locie, czyli przed usunięciem z pamięci oryginalnych danych (otrzymanych z aplikacji backupowej), musi być realizowana w trybie ciągłym (a nie ad-hoc), wymagane parametry wydajnościowe urządzenia muszą uwzględniać tę funkcjonalność. Wymagane potwierdzenie opisanej funkcjonalności w oficjalnej dokumentacji producenta oferowanego urządzenia.
44.	Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia.
45.	Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu).
46.	Wymagana możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora).
47.	Wymagana możliwość zdefiniowania harmonogramu wg. którego wykonywany jest proces usuwania przeterminowanych danych (czyszczenia), realizowany równolegle z procesami backup/restore/replication.
48.	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).
49.	Urządzenie musi umożliwiać systemowo (wbudowana funkcjonalność) - realizację procesu pierwszego czyszczenia dopiero po przekroczeniu 75% zajętości oferowanej przestrzeni.
50.	Urządzenie musi mieć możliwość zarządzania poprzez <ul style="list-style-type: none"> • Interfejs graficzny dostępny z przeglądarki internetowej • Poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell)
51.	Oprogramowanie do zarządzania musi rezydować na oferowanym na urządzeniu deduplikacyjnym.
52.	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.

53.	Urządzenie musi być rozwiązaniem kompletnym, apłiancem 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.
54.	Oferowane urządzenie powinno być objęte 3 letnim wsparciem producenta działającym w trybie zgłaszania awarii: 24x7 oraz reakcji on-site w trybie NBD.