

Szczegółowy opis przedmiotu zamówienia

Dostawa systemu kopii bezpieczeństwa i archiwizacji wraz z wdrożeniem

1. PRZEDMIOT ZAMÓWIENIA

Przedmiotem zamówienia jest **dostawa systemu kopii bezpieczeństwa i archiwizacji wraz z wdrożeniem** na potrzeby obsługi jednostek obsługiwanych przez Zamawiającego – Warmińsko-Mazurskie Centrum Nowych Technologii.

2. WYMAGANIA SZCZEGÓŁOWE:

a) System kopii bezpieczeństwa i archiwizacji

(Urządzenie musi spełniać wymagania wyspecyfikowane w niniejszej tabeli.)

Lp.	Parametr wymagany
1.	Urządzenie musi być przeznaczone do deduplikacji i przechowywania kopii zapasowych.
2.	Urządzenie, na poziomie systemu operacyjnego oferowanego urządzenia, musi posiadać funkcjonalność replikacji do użytkowanego przez Zamawiającego systemu PowerProtect DD6400.
3.	Urządzenie musi być w pełni kompatybilne z użytkowanym przez Zamawiającego systemem do monitorowania, zarządzania predykcji zdarzeń Dell APEX AIOps oraz oprogramowaniem do backupu Dell Networker.
4.	Dostarczone urządzenie musi oferować przestrzeń min. 80TB netto (powierzchni użytkowej) bez uwzględniania mechanizmów protekcji – przestrzeń dedykowana do gromadzenia deduplikatów, wymagana skalowalność do min. 250TB netto (powierzchni użytkowej widocznej po założeniu systemu plików)
5.	Dostarczone urządzenie powinno 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 zdedykowanej) na dodatkową warstwę, wymagane wsparcie dla AWS, Microsoft Azure oraz Google GCP. Wymagana enkrypcja danych przechowywanych na warstwie typu Cloud. Wymagane dostarczenie potwierdzenia dostępności przestrzeni min. 160TB netto dla warstwy CLOUD. Wymagana funkcjonalność powinna wspierać eksploatowaną przez Zamawiającego aplikację Networker.
6.	Oferowane urządzenie musi posiadać minimum 4 porty 10/25Gb/s Eth OP - wymagana możliwość obsługi w każdym z w/w portów protokołów CIFS, NFS, deduplikacja na źródle
7.	Oferowane urządzenie musi umożliwiać jednoczesny dostęp wszystkimi poniższymi protokołami: - CIFS, NFS - zapewniając deduplikację na źródle, wymagane wsparcie dla aplikacji Commvault (co najmniej na poziomie Media Server a także Client Direct przy użyciu storage accelerator), Veeam Backup and Replication (co najmniej na

	poziomie Veeam Data Mover), NetWorker na poziomie standardowego klienta - wymagane wsparcie dla eksploatowanych przez Zamawiającego aplikacji NetWorker i Avamar - VTL (min. 10 jednocześnie)
8.	Wymagana jest pełna funkcjonalność, pozwalającej na jednoczesną obsługę protokołów CIFS, NFS, deduplikacja na źródle, VTL do oferowanej pojemności urządzenia
9.	Oferowane pojedyncze urządzenie musi osiągać zagregowaną wydajność (dla maksymalnej konfiguracji) protokołami: NFS co najmniej 25 TB/h (dane podawane przez producenta) oraz co najmniej 50 TB/h z wykorzystaniem deduplikacji na źródle (dane podawane przez producenta).
10.	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 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) musi mieścić 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.
11.	Oferowane urządzenie musi mieć możliwość emulacji następujących bibliotek taśmowych: - StorageTek L180 - IBM TS 3500
12.	Oferowane urządzenie musi mieć możliwość emulacji napędów taśmowych min. LTO5 oraz LTO7
13.	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.
14.	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.
15.	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.
16.	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.
17.	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 i CIFS bez użycia jakiegokolwiek aplikacji backup’owej również muszą być deduplikowane w sposób in-line
18.	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)
19.	Wszystkie unikalne bloki przed zapisaniem na dysk muszą być dodatkowo kompresowane.
20.	Tryb zapisu zabezpieczanych danych nie może umożliwiać nadpisywania danych, dane mogą być zapisywane jedynie w trybie append-only, dane dla których wygasa retencja powinny zostać usunięte podczas procesu czyszczenia tzw. Cleaning, wymaganie dotyczy wszystkich danych zapisanych na urządzeniu a nie wybranych grup danych objętych działaniem blokad zabezpieczających przed usunięciem/modyfikacją danych.
21.	Oferowane urządzenie musi wspierać (wymagane formalne wsparcie producenta urządzenia), co najmniej następujące aplikacje: Commvault, Veeam Backup and Replication, NetWorker. W przypadku współpracy z każdą z poniższych aplikacji: • Commvault • Veeam Backup and Replication • NetWorker Oferowane urządzenie musi umożliwiać deduplikację na źródle (w przypadku Commvault: co najmniej na poziomie Media Server a także Client Direct przy użyciu storage accelerator, w przypadku Veeam Backup and Replication co najmniej na poziomie Veeam Data Mover, w przypadku NetWorker na poziomie standardowego klienta) 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.
22.	W przypadku przyjmowania backupów z Commvault, Veeam Backup and Replication, NetWorker, urządzenie musi umożliwiać deduplikację na źródle (co najmniej na poziomie Media Server dla CommVault, Data Mover dla Veeam, klienta

	dla NetWorker) i przestanie nowych, nieznajdujących się jeszcze na urządzeniu bloków poprzez sieć FC. Deduplikacja w wyżej wymienionych przypadkach musi zapewniać aby do oferowanego urządzenia były transmitowane poprzez sieć FC jedynie fragmenty danych nie znajdujące się dotychczas na urządzeniu.
23.	Oferowane urządzenie musi umożliwiać uruchamianie maszyn wirtualnych VMware bezpośrednio z danych backupowych bez konieczności odtwarzania danych.
24.	Oferowane urządzenie musi umożliwiać funkcjonalność Load Balancing oraz Link Failover w obrębie portów (Eth) wykorzystywanych przez aplikację backupową.
25.	Urządzenie musi posiadać wsparcie dla backupów typu Virtual Synthetics w przypadku aplikacji Commvault, Veeam Backup and Replication oraz NetWorker.
26.	W przypadku deduplikacji na źródle poprzez sieć IP (LAN oraz WAN), urządzenie musi posiadać możliwość szyfrowania komunikacji kluczem minimum 256 bitów.
27.	Urządzenie powinno umożliwiać zaszyfrowanie przechowywanych danych, wymagane licencje umożliwiające zaszyfrowanie i przechowywanie zaszyfrowanych danych w obrębie maksymalnej pojemności oferowanego urządzenia.
28.	Urządzenie musi wspierać deduplikację na źródle poprzez sieć FC (SAN) minimum dla następujących systemów operacyjnych: • Windows • Linux (RedHat, SuSE)
29.	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. Oferowana funkcjonalność na replikację jest przedmiotem postępowania.
30.	Urządzenie musi umożliwiać wydzielenie określonych portów Ethernet dedykowanych do replikacji.
31.	W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami.
32.	W przypadku replikacji danych między dwoma urządzeniami oferowanego typu, wymagana możliwość kontroli przez: Commvault oraz 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
33.	Oferowane urządzenie musi działać poprawnie przy zapętnieniu danymi na poziomie co najmniej 90%. Dokumentacja urządzenia nie może wskazywać na ew. problemy, obostrzenia, które są efektem zapętnieniu urządzenia zabezpieczanymi danymi, na poziomie mniejszym niż 90%.



34.	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.
35.	Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6 bądź równoważnej.
36.	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).
37.	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.
38.	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).
39.	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.
40.	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.
41.	Wymagana możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia, jako niezależnego urządzenia dostępnego za pośrednictwem: • CIFS • NFS • VTL • deduplikacja na źródle
42.	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 wymaganej blokady przez aplikację Commvault, Veeam Backup and Replication oraz NetWorker – wymagane potwierdzenie na oficjalnych stronach w/w aplikacji backup'owych oraz producenta oferowanego deduplikatora Dostęp do funkcjonalności WORM (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.
43.	Urządzenie musi mieć możliwość przechowywania danych niezmiennych: • Video • Grafika • Nagrania dźwiękowe • Pliki pdf na udziałach CIFS/NFS.
44.	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.
45.	Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia.
46.	Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu).
47.	Wymagana możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora).
48.	Wymagana możliwość zdefiniowania harmonogramu wg. którego wykonywany jest proces usuwania przeterminowanych danych (czyszczenia), realizowany równolegle z procesami backup/restore/replication.
49.	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.
50.	Urządzenie musi umożliwiać systemowo (wbudowana funkcjonalność) - realizację procesu pierwszego czyszczenia dopiero po przekroczeniu 75% zajętości oferowanej przestrzeni.
51.	Urządzenie musi mieć możliwość zarządzania poprzez • Interfejs graficzny dostępny z przeglądarki internetowej • Poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell).
52.	Oprogramowanie do zarządzania musi rezydować na oferowanym urządzeniu deduplikacyjnym.
53.	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.
54.	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.
55.	Oferowane urządzenie powinno być objęte 5 letnim wsparciem producenta działającym w trybie Next Business Day. Uszkodzone nośniki pozostają u Zamawiającego bez ponoszenia dodatkowych kosztów.
56.	Oferowane urządzenie musi być nie starsze niż 6 miesięcy od daty dostawy do Zamawiającego.

57.	Producent musi zapewnić możliwość pobrania aktualizacji oprogramowania urządzenia z portalu wsparcia producenta bez konieczności tworzenia zgłoszenia serwisowego.
58.	Wymagane dostarczenie wzoru umowy powierzenia przetwarzania danych dla warstwy CLOUD, pomiędzy producentem dostarczonego rozwiązania a Zamawiającym.
59.	Urządzenie i jego komponenty muszą być oznakowane przez producenta w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.

b) wdrożenie:

Poprzez wdrożenie Zamawiający rozumie:

- instalację i konfigurację urządzenia w miejscu instalacji wskazanym przez Zamawiającego;
- integrację z posiadanymi systemami Dell Networker, Dell Avamar oraz Dell AI Ops;
- konfigurację urządzenia zgodnie z dobrymi praktykami i zaleceniami producenta w środowisku Zamawiającego, a w szczególności musi zostać skonfigurowana i uruchomiona funkcjonalność replikacji z posiadanym przez Zamawiającego systemu PowerProtect DD6400;
- wszystkie prace wdrożeniowe muszą odbyć się fizycznie u Zamawiającego w miejscu instalacji – nie dopuszcza się uruchomienia i konfiguracji zdalnej na żadnym etapie wdrożenia;