Załącznik nr 2 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest rozwiązanie dedykowane do zabezpieczania danych, składające się z:

- OPROGRAMOWANIA
- DEDUPLIKATORA dedykowanego do składowania zabezpieczanych danych

Zarówno OPROGRAMOWANIE oraz DEDUPLIKATOR powinny zostać dostarczone wraz z 60-o miesięcznym wsparciem producenta działającym w trybie NBD umożliwiającym upgrade do najnowszych dostępnych wersji oferowanego oprogramowania oraz firmware (w przypadku deduplikatora).

OPROGRAMOWANIE będące przedmiotem zapytania musi umożliwiać:

- realizację backupów w DataCenter
- realizację backupów środowisk wirtualnych oraz zdalnych lokalizacji
- realizację monitoringu oraz raportowania środowiska backupowego
- zabezpieczanie danych w trybie Continuous Data Protection środowisk VMware vSphere

Oferowane OPROGRAMOWANIE musi licencjonować się na sumaryczną ilość CPU (min. 4 szt.) zabezpieczanego środowiska (bez względu na rozmiar backupowanego wolumenu danych, ilości serwerów, baz danych, wykorzystywanych urządzeń taśmowych czy dyskowych), musi również być zintegrowane z oferowanym DEDUPLIKATOREM, szczegółowe wymagania dotyczące OPROGRAMOWANIA oraz DEDUPLIKATORA przedstawione zostały w dalszej części dokumentu.

OPROGRAMOWANIE – wymagania dotyczące backupu serwerów (Data Center):

1.	Wymagana jest możliwość wyboru miejsca deduplikacji w przypadku składowania danych na oferowanym deduplikatorze: • na źródle • na medium backupowym
2.	Backup z dededuplikacją na źródle (przy składowaniu danych na oferowanym deduplikatorze) musi być dostępny dla wszystkich typów danych w ramach oferowanego rozwiązania: pliki, bazy danych, obrazy maszyn wirtualnych.

3.	Oprogramowanie backupowe musi zapewniać bezpośredni backup z każdej zabezpieczanej maszyny bezpośrednio na oferowany deduplikator bez pośrednictwa jakichkolwiek innych serwerów w trybie z deduplikacją na źródle oraz bez deduplikacji na źródle - wymagane obie opcje z możliwością dowolnego użycia oraz możliwością przełączania. Powyższa funkcjonalność nie może

	wymagać dodatkowej licencji poza zwykłą licencja kliencką. Funkcjonalność musi dostępna dla minimum następujących platform: Windows, RedHat, SuSE.
4.	Wymagane jest aby oprogramowanie backupowe zapewniało szybki backup blokowy wielomilionowych systemów plików na maszynach Windows oraz Linux W trakcie backupu oprogramowanie backupowe musi wykonywać kopie zapasowe fizycznych bloków a nie plików. Wymagana możliwość odtworzenia pojedynczego pliku z tak zrealizowanego backupu. W celu minimalizacji czasu backupu oprogramowanie backupowe nie może indeksować plików znajdujących się na zabezpieczanym wolumenie (zaindeksowanie wielu milionów plików powoduje duże wydłużenie czasu backupu).
5.	Wymagane jest aby oprogramowanie backupowe zapewniało szybki inkrementalny backup blokowy wielomilionowych systemów plików na maszynach Windows oraz Linux. W trakcie backupu inkrementalnego wielomilionowych systemów plików na maszynach Windows oraz Linux oprogramowanie backupowe musi odczytywać tylko te fragmenty dysku które zmieniły się od ostatniego backupu. W celu minimalizacji czasu backupu oprogramowanie backupowe nie może indeksować plików backupu inkrementalnego znajdujących się na zabezpieczanym wolumenie (zaindeksowanie wielu milionów plików powodowałoby duże wydłużenie czasu backupu).
6.	Oprogramowanie backupowe musi mieć możliwość łączenia backupu blokowego pełnego i inkrementalnego w jeden pełen backup. Łączenie backupów musi odbywać się na oferowanym deduplikatorze bez fizycznego odczytu łączonych danych (łączeniu muszą podlegać tylko metadane opisujące backup pełny oraz inkrementalny). Po połączeniu backupu pełnego i inkrementalnego muszą być dostępne dwa backupy pełne: dotychczas dostępny backup pełny i nowy backup pełny uzyskany w drodze łączenia z backupem inkrementalnym.

7.	Wymagana możliwość automatycznego łączenia backupu blokowego pełnego i inkrementalnego po wykonaniu blokowego backupu inkrementalnego w celu uzyskania aktualnego backupu pełnego.
8.	Oferowane rozwiązanie backupowe musi przechowywać całość własnych informacji (informacje o backupach, napędach taśmowych, mediach) w centralnym pojedynczym katalogu, skopiowanie

	centralnego katalogu systemu backupu na inną maszynę musi pozwolić na uruchomienie na drugiej maszynie serwera backupu identycznego z oryginalnym.
9.	Ze względów bezpieczeństwa rozwiązanie backupowe musi mieć możliwość wykonania kopii wewnętrznej bazy danych w trakcie pracy systemu bez konieczności ograniczania jego funkcjonalności.
10.	Oprogramowanie backupowe musi mieć możliwość backupu własnej bazy danych na następujące nośniki: • urządzenie dyskowe • deduplikator będący przedmiotem zapytania • nośniki taśmowe
11.	W przypadku backupu na nośniki taśmowe wymagana możliwość zdefiniowania puli taśm (zawierającej jedną lub więcej taśm) na którą będą zapisywane tylko i wyłącznie backupy wewnętrznej bazy danych systemu backupowego.
12.	Oprogramowanie backupowe musi mieć możliwość automatycznego wykonywania backupu własnej bazy danych.
13.	Oprogramowanie backupowe po każdorazowym backupie wewnętrznej bazy danych musi raportować miejsce, w którym znajduje się ostatni backup wewnętrznej bazy danych oprogramowania backupowego.
14.	Backup własnej bazy danych musi pozwalać na odtworzenie wszystkich ustawień systemu backupowego na zupełnie nowej, świeżo zainstalowanej instancji oprogramowania backupowego.

15.	W przypadku backupu systemów produkcyjnych (klientów systemu backupu) na nośniki taśmowe, oferowane oprogramowanie backupowe musi umożliwiać zapisywanie backupów o tym samym terminie ważności na jednej, tej samej, z góry zdefiniowanej puli taśm (zawierającej jedną lub więcej taśm).
16.	System musi zapisywać dane na taśmach - zoptymalizowane w sposób eliminujący potrzebę wykonywania dodatkowych działań (nawet automatycznych) w celu ich optymalizacji.
17.	W przypadku gdy w puli taśmowej zabraknie taśm na których można zapisywać nowe backupy,

	oprogramowanie backupowe musi mieć możliwość automatycznego przyporządkowania: • wolnych, nieprzyporządkowanych taśm znajdujących się w bibliotece • nieużywanych lub przeterminowanych taśm z innych pul taśmowych
18.	W przypadku użycia biblioteki taśmowej (backup, replikacja z oferowanego deduplikatora sprzętowego na taśmę), oferowany system musi generować samoopisujące się taśmy dla całości zapisywanych taśm, co oznacza to, że wyjęcie jakiejkolwiek taśmy z biblioteki i włożenie jej do zupełnie innej biblioteki zarządzanej przez zupełnie inną instancję oferowanego oprogramowania backupowego (w tym również działającą na innym systemie operacyjnym) musi pozwolić na odtworzenie danych znajdujących się na w/w taśmie.
19.	Oferowane rozwiązanie musi generować somoopisujące się zbiory danych zarówno na oferowanym deduplikatorze jak i na taśmach. Utrata wewnętrznych danych oprogramowania backupowego nie może powodować braku możliwości odtworzenia jakichkolwiek zbiorów z oferowanego deduplikatora bądź taśm.
20.	Oprogramowanie backupowe musi umożliwiać łączenie strumieni backupowych z wielu zabezpieczanych serwerów w sieci LAN i bezpośredni zapis na napędzie taśmowym (multiplexing).

21.	Oprogramowanie backupowe musi umożliwiać zarządzanie bezpośrednią replikacją backupów między deduplikatorami oferowanego typu (replikacja realizowana na poziomie deduplikatorów) - bezpośrednio z poziomu interfejsu oprogramowania backupowego przy spełnieniu wszystkich poniższych wymagań 1. replikacji podlegają tylko te bloki które nie znajdują się na docelowym oferowanym deduplikatorze 2. replikacja między deduplikatorami może nastąpić zarówno bezpośrednio po zakończeniu backupu jak również zgodnie z kalendarzem 3. oferowane oprogramowanie backupowe przechowuje informacje o wszystkich kopiach danych znajdujących się na deduplikatorach m.in. źródłowych jak i po replikacji GUI oferowanego oprogramowania backupowego powinien umożliwiać wybór urządzenia deduplikacyjnego z którego zostanie wykonane odtwarzanie - w efekcie umożliwiając odtworzenie z oryginalnej kopii backupowej bądź ze zreplikowanej kopii backupowej.
22.	Oprogramowanie backupowe musi mieć możliwość kopiowania backupów między dowolnymi mediami: • Deduplikatorami oferowanego typu • Dyskowymi (CIFS, NFS) • Taśmowymi

23.	Oprogramowanie backupowe musi zapewniać różny czas ważności danych na podstawowym nośniku i nośniku zawierającym kopię (replikę backupu). Definicja czasu przechowywania kopii (repliki) powinna być określenia w momencie definiowania zadania duplikacji/kopiowania zarówno z interfejsu graficznego jak i z command line.
24.	Oprogramowanie backupowe musi pozwalać na następujące rodzaje backupu systemu plików: • pełny • różnicowy • inkrementalny

25.	Oprogramowanie backupowe musi pozwalać na łączenie backupów pełnych i inkrementalnych w jeden pełen backup. Proces ten musi być niewidoczny dla systemu plików którego dotyczą backupy pełne i inkrementalne. Proces odtworzenia danych z połączonego backupu pełnego i inkrementalnego musi być identyczny z odtworzeniem danych z normalnie wykonanego backupu pełnego w zakresie: • zarządzania • wydajności
26.	Oprogramowanie backupowe musi pozwalać na łączenie backupów pełnych i inkrementalnych bez odczytu danych z oferowanego deduplikatora. Łączenie backupów pełnych i inkrementalnych musi być realizowane przez oferowany deduplikator, jedynie zarządzanie (start, kalendarz łączenia) procesem łączenia backupów pełnych i inkrementalnych musi być realizowany przez aplikację backupową.
27.	Oprogramowanie backupowe musi pozwalać na zatrzymanie procesu backupu oraz jego wznowienie od momentu zatrzymania.
28.	W przypadku nieudanego backupu dla systemu plików (na przykład zerwanie łączności), oprogramowanie backupowe musi pozwalać na wznowienie backupu od ostatnio poprawnie zbackupowanego: • Katalogu • Pliku
29.	W przypadku awarii fragmentu zapisanej taśmy, oprogramowanie backupowe musi umożliwiać odtworzenie całości plików, które znajdują się na nieuszkodzonej części nośnika.
30.	W przypadku konsoli oprogramowania backupowego wymagana możliwość definiowania ważności danych (backupów) na podstawie kryteriów czasowych (dni, miesiące, lata). Po okresie ważności

	backupy muszą być automatycznie usunięte.
31.	Oprogramowanie backupowe musi wspierać (wymagane wsparcie producenta) następujące systemy operacyjne: Windows (także Microsoft Cluster) , Linux (Red Hat, SUSE).

32.	Oprogramowanie backupowe musi wspierać (wymagane wsparcie producenta) backup online następujących baz danych i aplikacji: MS Exchange, MS SQL, Oracle, IBM DB2, PostgreSQL, mySQL, SharePoint.
33.	W przypadku zabezpieczania baz danych, oferowany system backupowy musi umożliwiać inicjalizację backupu poprzez określone zdarzenie: np. ilość logów, czas który upłynął od ostatniego zdarzenia lub inne zdarzenie zdefiniowane przez użytkownika
34.	Dla baz danych MSSQL wymagana możliwość inicjowania backupów przez administratora MSSQL przy spełnieniu wszystkich poniższych wymagań: • Backup jest wykonywany przez oferowane oprogramowanie backupowe • Inicjowanie backupu z graficznego interfejsu będącego częścią MSSQL Management Studio • Możliwość wyboru backupu pełnego, różnicowego oraz logów • Backup inicjowany przez administratora MSSQL bez konieczności zaangażowania administratora oferowanego rozwiązania backupowego
35.	Dla baz danych MSSQL wymagana możliwość odtworzenia backupów przez administratora MSSQL przy spełnieniu wszystkich poniższych wymagań: • Odtworzenie dowolnego backupu wykonanego przez oferowane rozwiązanie backupowe • Zarządzanie odtwarzaniem z graficznego interfejsu będącego częścią MSSQL Management Studio • Możliwość odtworzenia do dowolnego punktu w czasie wybranego przez administratora MSSQL w ramach przechowywanych przez oferowane oprogramowanie backupowe logów MSSQL • Odtworzenie bazy danych przez administratora MSSQL bez konieczności zaangażowania administratora oferowanego rozwiązania backupowego
36.	Oferowane rozwiązanie backupowe musi integrować się funkcjonalnością FRA (Fast Recovery Area) bazą danych Oracle. Wymagane spełnienie wszystkie poniższych funkcjonalności: • Administrator Oracle wykonuje backupy narzędziami RMAN do przestrzeni FRA • Oferowane rozwiązanie backupowe automatycznie kopiuje backupy z przestrzeni Oracle FRA na media zarządzane przez oferowane rozwiązanie backupowe.
	• Definiowanie parametrów zadania kopiowania backupów przestrzeni FRA na media zarządzane przez oferowane rozwiązanie backupowe z poziomu interfejsu graficznego • Odtworzenie danych możliwe przez administratora Oracle

37.	Oprogramowanie backupowe musi mieć możliwość odtwarzania pojedynczego serwera Windows bez ponownej instalacji systemu operacyjnego.
38.	Rozwiązanie backupowe musi mieć możliwość odtworzenia plików na docelową maszynę w oddziale z poziomu centralnej konsoli systemu backupowego. Nie może być wymagane logowanie się na odtwarzaną maszynę w celu odtworzenia danych z systemu backupowego.
39.	Wymagana możliwość odtworzenia danych • z zabezpieczanego serwera / komputera • z konsoli systemu backupowego

OPROGRAMOWANIE - wymagania dotyczące backupu zdalnych lokalizacji oraz środowisk wirtualnych:

40.	Oprogramowanie backupowe musi wspierać (wymagane wsparcie producenta) następujące systemy operacyjne: Windows (także Microsoft Cluster) , Linux (Red Hat, SUSE). Backup zasobów plików w przypadku powyższych systemów musi podlegać deduplikacji ze zmiennym blokiem na zabezpieczanej maszynie zgodnie z przedstawionymi wymaganiami.
41.	Oprogramowanie backupowe musi wspierać (wymagane wsparcie producenta) backup online następujących baz danych, aplikacji i środowisk: MS Exchange, MS SQL, Oracle, IBM DB2, SharePoint, VM na VMware vSphere, Hyper-V. Backup powyższych baz danych i aplikacji musi podlegać deduplikacji ze zmiennym blokiem na zabezpieczanej maszynie zgodnie z przedstawionymi wymaganiami.
42.	W przypadku zabezpieczania baz danych i aplikacji wymagana możliwość realizacji kopii zapasowej kilkoma strumieniami jednocześnie (minimum 10 jednoczesnych strumieni).
43.	Zabezpieczane serwery muszą być backupowane bezpośrednio na dyski oferowanego deduplikatora bez pośrednictwa jakichkolwiek innych urządzeń / serwerów. Dotyczy to backupów lokalnych oraz zdalnych.
44.	Oprogramowanie backupowe musi umożliwiać dla sieci lokalnej: • backup pojedynczych plików • backup całych systemów plików

	• backup baz danych w trakcie ich normalnej pracy • backup ustawień systemu operacyjnego Windows. • backup całych obrazów maszyn wirtualnych systemu VMware vSphere • backup całych obrazów maszyn wirtualnych systemu Hyper-V
45.	Rozwiązanie backupowe musi umożliwiać transfer danych bezpośrednio ze zdalnych oddziałów do oferowanego deduplikatora bez konieczności instalacji dodatkowego sprzętu w oddziale. Powyższa funkcjonalność wymagana jest dla następujących typów danych: • backup pojedynczych plików • backup całych systemów plików • backup baz danych w trakcie ich normalnej pracy
46.	Wymaga się aby oferowane rozwiązanie backupowe było w pełni konfigurowalne z konsoli znajdującej się w centrali, w szczególności backupy maszyn w oddziałach (bazy, pliki) czy też backupy laptopów muszą być konfigurowalne z poziomu centralnej konsoli bez konieczności logowania się na zabezpieczaną maszynę.
47.	Oferowane rozwiązanie backupowe musi umożliwiać odtworzenie □ plików □ baz danych na docelową maszynę w oddziale - z poziomu centralnej konsoli systemu backupowego. Wymagany scenariusz nie może wymagać logowania się na odtwarzaną maszynę celem odtworzenia danych z systemu backupowego.
48.	W celu minimalizacji ilości przesyłanych danych, oferowane rozwiązanie musi mieć możliwość przesyłania odtwarzanych danych z medium backupowego do docelowego serwera w postaci skompresowanej, odtwarzane dane powinny zostać rozkompresowane na docelowym serwerze przez agenta oferowanego systemu.
49.	Oprogramowanie backupowe musi posiadać funkcjonalność podziału danych (plików, baz danych, obrazów maszyn wirtualnych) na bloki o zmiennej długości. System musi się dopasowywać do struktury dokumentu zapewniając podział na bloki o różnej długości w ramach pojedynczego dokumentu w celu polepszenia efektywności deduplikacji. Podział na bloki musi następować bezpośrednio na zabezpieczanym serwerze.
50.	Używany algorytm deduplikacji musi generować zmienny blok w przypadku backupu pojedynczego dokumentu. Bloki wysyłane w trakcie backupu pojedynczego dokumentu z zabezpieczanej maszyny do oferowanego deduplikatora muszą wynikać i odpowiadać rozmiarem - długości bloków używanych przez oferowany deduplikator.

51.	Wymaga się aby oprogramowanie backupowe przesyłało na oferowany deduplikator tylko unikalne bloki nie znajdujące się na tym urządzeniu, w efekcie skracając czas backupu, obciążenie procesora i zmniejszając ruch w sieci WAN / LAN.

52.	Funkcjonalność deduplikacji nie może wymagać instalacji dodatkowych modułów programowych po stronie klienckiej lub serwera backupowego.
53.	Oprogramowanie backupowe nie może odczytywać tych plików z systemu dyskowego, które się nie zmieniły w stosunku do ostatniego backupu. Raz zbackupowany plik nie może być ponownie odczytywany, chyba, że zmieni się jego zawartość.
54.	Wymaga się aby oprogramowanie backupowe realizowało wyłącznie - logicznie pełne backupy systemu plików. Z zabezpieczanego systemu plików muszą odczytywane tylko nowe lub zmienione pliki, do oferowanego deduplikatora powinny być przesyłane dane po deduplikacji, jednak każdy finalny backup musi być logicznie pełnym backupem. W wewnętrznej strukturze systemu musi być przechowywana informacja o każdym backupie i należących do niego danych (blokach), dzięki czemu odtworzenie jakichkolwiek danych plikowych musi być pojedynczym zadaniem identycznym z odtworzeniem danych z pełnego backupu.
55.	Wymagana możliwość definiowania w konsoli oprogramowania backupowego ważności (retencji) danych (backupów) na podstawie kryteriów czasowych (dni, miesiące, lata). Po okresie ważności backupy musza być automatycznie usunięte.
56.	Wymagana możliwość tworzenia z poziomu GUI (konsoli graficznej) w przypadku oferowanego oprogramowania backupowego, polityk w których zdefiniowano: • Czas przechowywania backupów dziennych • Czas przechowywania backupów tygodniowych • Czas przechowywania backupów miesięcznych • Czas przechowywania backupów rocznych
57.	Oferowane rozwiązanie musi umożliwiać tworzenie wykluczeń, czyli elementów nie podlegających backupowi w ramach zadania backupowego. Wymagana możliwość tworzenia wykluczeń dla dowolnej kombinacji następujących elementów: • wybranych typów plików, np. dla plików z rozszerzeniem mp3 □ dla całych katalogów (np.: c:\windows). • dla pojedynczych plików

58.	Oferowane rozwiązanie musi mieć możliwość zdefiniowania aby ostatni backup dowolnego zbioru danych nigdy się nie przeterminował. Oznacza to, że jeśli dany zasób nie jest backupowany to automatycznie ostatni ważny backup tego zasobu będzie przechowywany bezterminowo, jedynie administrator może zdecydować o jego usunięciu.
59.	Konsola zarządzająca systemem backupowym musi integrować się z Active Directory. Musi być możliwość przydzielania użytkownikom i grupom Active Directory dostępnych ról (min. administrator, monitoring, tylko wykonywanie odtworzeń) w systemie backupowym.
60.	Wymagana możliwość generowania (poprzez konsolę) raportów określających zajętość przestrzeni przeznaczonej na składowanie deduplikatów.

61.	Bloki przesyłane z zabezpieczanych serwerów do oferowanego deduplikatora muszą być kompresowane i szyfrowane algorytmem z kluczem minimum 256-bitowym.
62.	Oprogramowanie backupowe musi pozwalać na odtwarzanie danych poprzez: wybór odtwarzanych danych, odtworzenie danych w jednym kroku.
63.	Wymagana możliwość limitowania wielkości zadania backupowego, jeśli zadanie backupowe przekroczy zdefiniowaną wielkość wówczas nie może być zapisane w systemie backupowym.
64.	Rozwiązanie backupowe musi wspierać backup i odtwarzanie środowisk VMware vSphere 7.x. Oprogramowanie backupowe musi umożliwiać w przypadku środowisk VMware następujące typy backupu: a. Backup całych maszyn wirtualnych b. Backup pojedynczych, wybranych dysków maszyny wirtualnej vmdk c. Musi istnieć możliwość zastosowania wyrażeń regularnych do określenia które wirtualne dyski VMware mają być backupowane d. W trakcie backupu odczytowi z systemu dyskowego mają podlegać tylko zmienione bloki wirtualnych maszyn systemu VMware (wymagane wykorzystanie mechanizmu CBT systemu VMware) e. Wykonywanie backupu obrazów maszyn wirtualnych VMware nie może wymagać bufora dyskowego na kopię obrazów maszyn wirtualnych (plików vmdk) Powyższe metody backupu maszyn wirtualnych muszą podlegać deduplikacji ze zmiennym blokiem przed wysłaniem danych do medium backupowego zgodnie z wymaganiami dla deduplikacji powyżej. Powyższe metody backupu muszą być wbudowane w oferowany system backupu, nie powinny wymagać tworzenia skryptów/dodatkowych komend.

65.	Oferowany system musi pozwalać na szybkie odtworzenie • całych obrazów maszyn wirtualnych • pojedynczych dysków maszyny wirtualnej z backupu całej maszyny wirtualnej
66.	Wymaga się aby oferowane rozwiązanie backupowe umożliwiało odtwarzanie obrazów maszyn wirtualnych VMware z następującymi funkcjonalnościami: a. odtwarzanie całych maszyn wirtualnych musi wykorzystywać mechanizm CBT systemu VMware – odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od ostatniego backupu b. odtwarzanie pojedynczych dysków maszyn wirtualnych musi wykorzystywać mechanizm CBT systemu VMware – odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od ostatniego backupu c. odtworzenie pojedynczych plików z backupu obrazu maszyny wirtualnej bez konieczności odtworzenia całej maszyny wirtualnej, funkcjonalność ta musi być dostępna dla obrazów maszyn wirtualnych z zainstalowanym systemem operacyjnym Windows oraz Linux. d. możliwość zamontowania na dowolnym serwerze (fizycznym lub wirtualnym)

	zbackupowanych obrazów maszyn wirtualnych Windows (plików vmdk maszyny wirtualnej Windows), w efekcie metoda ta nie odtwarza backupów a jedynie umożliwia na przeglądanie zawartości plików vmdk w backupie z poziomu Eksploratora Plików Windows na dowolnej maszynie
67.	Oferowane rozwiązanie backupowe musi umożliwiać uruchomienie maszyn wirtualnych bezpośrednio z oferowanego dedupliktora w oparciu o zrealizowany backup, bez konieczności odtwarzania backupu (tzw. Instant Access) – wymagane formalne wsparcie tej funkcjonalności zarówno od strony oferowanej aplikacji backup'owej jak i oferowanego deduplikatora.
68.	Oferowane oprogramowanie backupowe musi mieć możliwość prezentacji (bez konieczności odtworzenia) zbackupowanych obrazów maszyn wirtualnych VMware (plików vmdk) jako katalogów na maszynie fizycznej w celu ich przeszukiwania (wymagane przeszukiwanie po nazwach plików jak również zawartości plików) z poziomu systemu operacyjnego maszyny fizycznej.
69.	Oferowane oprogramowanie backupowe musi mieć możliwość backupu/odtworzenia w trybie „image backup" (backup plików vmdk) maszyn wirtualnych znajdujących się na serwerach VMware ESX bez udziału vCenter.
70.	Wymagana skalowalność rozwiązania dla środowisk VMware na poziomie: minimum 2000 maszyn wirtualnych w ramach pojedynczej instancji systemu backupu.

71.	Oferowane oprogramowanie backupowe musi mieć możliwość automatycznego sprawdzania (weryfikacji) zbackupowanych maszyn wirtualnych VMware, wymagana możliwość ustawienia kalendarza weryfikacji maszyn wirtualnych VMware. Weryfikacja maszyn wirtualnych musi zapewniać minimum: a. odtworzenie maszyny wirtualnej na zdefiniowanym Data Center/Data Store b. weryfikację podstawowych procesów c. możliwość dołączenia własnego skryptu weryfikującego wybrane elementy maszyny wirtualnej Wymagana dostępność informacji w konsoli systemu backupu o statusie (poprawna/niepoprawna) weryfikacji maszyny wirtualnej.
72.	Administrator (właściciel) danej maszyny wirtualnej VMware musi mieć możliwość samodzielnego (bez konieczności kontaktu z administratorem backupu czy tez administratorem VMware) odtworzenia pojedynczych plików z dowolnego backupu obrazu jego maszyny wirtualnej.
73.	Oprogramowanie backupowe musi zawsze przechowywać pełne backupy obrazów maszyn wirtualnych środowiska VMware dla każdej wykonanej w przeszłości kopii zapasowej. Każdy backup obrazu maszyny wirtualnej musi być backupem pełnym.
74.	Oferowane rozwiązanie backupowe musi umożliwiać na tworzenie automatycznych polityk backupowych dla: □ Folderu □ Resource Pool systemu VMware. Oznacza to, że dodanie maszyny wirtualnej do folderu, hosta czy resource pooli w systemie VMware vSphere spowoduje automatyczne backupowanie dodanej maszyny wirtualnej
	zgodnie z polityka zdefiniowana dla folderu hosta czy resource pooli w systemie VMware.
75.	Rozwiązanie backupowe musi umożliwiać zdefiniowanie polityk backupowych dostępnych dla administratora systemu VMware z poziomu vCenter. Administrator VMware musi mieć możliwość przyporządkowania nowo tworzonych maszyn wirtualnych do polityk backupowych.
76.	Wymaga się aby inicjowanie backupu oraz odtwarzanie maszyn wirtualnych VMware dostępne było z poziomu graficznego interfejsu, linii komend oraz przez REST API

77.	Oferowane oprogramowanie backupowe powinno umożliwiać dla środowisk Hyper-V: a. backup pojedynczych plików i baz danych z maszyny wirtualnej ze środka maszyny wirtualnej Hyper-V. b. backup całych maszyn wirtualnych (czyli plików vhd reprezentujących wirtualną maszynę), takie wykonanie backupu nie powinno wymagać bufora dyskowego na kopię obrazów maszyn wirtualnych (plików vhd). c. wykonywanie backupu jak w punkcie b. powinno umożliwiać na odtworzenie pojedynczych plików z obrazu maszyny wirtualnej bez konieczności odtworzenia całej maszyny wirtualnej, funkcjonalność ta powinna być dostępna dla obrazów maszyn wirtualnych z zainstalowanym systemem operacyjnym Windows. – dopuszcza się wykonywanie snapshotów vss maszyn wirtualnych i użycie ich w trakcie backupu obrazów maszyn wirtualnych. – powyższe metody backupu muszą być wbudowane w system backupu i w pełni automatyczne bez wykorzystania skryptów/dodatkowych komend. – powyższe metody backupu maszyn wirtualnych muszą podlegać deduplikacji ze zmiennym blokiem w momencie odczytu danych zgodnie z wymaganiami powyżej.
78.	Oferowane oprogramowanie backupowe musi zapewniać spójny backup Exchange / MSSQL przy backupie obrazów maszyn wirtualnych środowiska Hyper-V
79.	Wymagana możliwość odtworzenia danych • z zabezpieczanego serwera / komputera • z konsoli systemu backupowego
80.	Wymagana możliwość odtworzenia: • Pojedynczego pliku • Zabezpieczanej bazy danych
81.	W przypadku odtwarzania istniejącego systemu plików (systemu plików który utracił część zasobów) oprogramowanie backupowe musi samo, automatycznie sprawdzać których plików znajdujących się w backupie, brakuje na odtwarzanej maszynie a następnie odczytać z backupu i
	przesłać tylko te pliki które znajdują się w backupie i których brakuje na odtwarzanej maszynie.
82.	Oferowany system backupu musi być dostępny (dla backupu i odtwarzania) przez 24h na dobę 7 dni w tygodniu, wyklucza się istnienie okresów w przypadku których system backupowy nie może wykonywać backupu lub odtwarzania (tzw. BLACKOUT WINDOWS).

83.	Wymaga się aby oferowany system backupu posiadał możliwość bezpośredniego raportowania o błędach do serwisu producenta
84.	Oferowany system backupu powinien mieć możliwość instalacji agentów jako plików msi. Wymagana możliwość automatyzacji instalacji agentów poprzez uruchomienie skryptu na zabezpieczanej maszynie, przyporządkowującego maszynę automatycznie do określonej polityki backupowej.
85.	Oferowany system backupu musi mieć możliwość automatycznej aktualizacji oprogramowania agentów wykonywanej bezpośrednio z serwera backupu.
86.	Oferowany system musi pozwalać na backup serwerów NAS z następującymi funkcjonalnościami: • w trakcie backupu z systemu NAS muszą być wysyłane do medium backupowego tylko zmienione pliki od ostatniego backupu • w przypadku odtwarzania danych z backupu, uprawnienia użytkowników również są odtwarzane • integracja z protokołem NDMP systemów NAS • odtwarzanie plików z backupu NDMP bezpośrednio na platformę Windows/Linux

OPROGRAMOWANIE – wymagania dotyczących monitorowania, raportowania oraz przeszukiwania backupów:

87.	W ramach dostarczonych licencji musi być zapewniona możliwość monitorowania, raportowania, szczegółowego rozliczania z użycia komponentów systemu backupowego oraz analizy błędów dla środowiska kopii zapasowej Zamawiającego. Wymagana dostępność następujących raportów: a. Podsumowanie zadań backupowych (liczba backupów udanych, nieudanych, aktywnych, łączny rozmiar zbackupowanych danych) b. Podsumowanie zadań odtworzeniowych (liczba odtworzeń udanych, nieudanych, aktywnych, łączny rozmiar odtworzonych danych danych) c. Zbiorcze procentowe zestawienie udanych zadań backupowych z poszczególnych serwerów d. Zbiorcze zestawienie zabezpieczanych serwerów które w sposób ciągły (kilka razy pod rząd) maja problem z backupami

	e. Zestawienie zabezpieczanych systemów plików które w ogóle nie są backupowane f. Spodziewany czas odtwarzania zabezpieczanego serwera oraz potencjalnej utraty danych (czas między ostatnim backupem a chwilą awarii) g. Najmniej wiarygodne zabezpieczanych serwery (procent nieudanych backupów) h. Lista najwolniejszych/najszybszych zabezpieczanych maszyn i. Poziom SLA (procentowa liczba udanych backupów) w odniesieniu do poziomu założonego j. Mierzenie poziomu SLA dla poszczególnych zabezpieczanych serwerów przy uwzględnieniu założonego okna backupowego i RPO (punktu do którego się odtwarzamy) k. Liczba danych backupowanych dziennie l. Liczba zadań backupowych dziennie m. Zużycie zasobów na serwerach backupowych (procesor, pamięć, karty sieciowe LAN, SAN) n. Zużycie mediów backupowych i napędów taśmowych o. Aktualna konfiguracja systemu backupowego p. Historia zmian konfiguracji systemu backupowego q. Posiadane licencje systemu backupowego r. Wykorzystanie systemu backupowego przez poszczególne działy / grupy użytkowników (chargeback per cost center)
88.	W ramach dostarczonych licencji wymagana możliwość zaindeksowania oraz przeszukiwania backupów z poziomu graficznego interface'u (GUI), wymagana również możliwość wyszukania dowolnych fraz w nazwach plików.

OPROGRAMOWANIE – wymagania dotyczące ochrony w trybie Continuous Data Protection dla środowisk VMware vSphere

89.	integracja na poziomie VMware vCenter Plug-in (ORCHESTRATION, MANAGEMENT) , vSphere Web Client GUI
90.	wsparcie dla HA, DRS, S-DRS, VMotion, S-VMotion
91.	możliwość integracji z VMware vRealize Operations Manager

92.	rozwiązanie dostarczane w postaci oprogramowania instalowanego na platformie ESXi
93.	skalowalność zapewniająca wsparcie dla 8000 VM w obrębie poj. vCenter
94.	zabepieczenie dowolnej maszyny wirtualnej wraz z aplikacjami w trybie ciągłym tzn. umożliwiającym odtworzenie do dowolnego punktu w czasie (tzw. PIT – Point In Time), wymagane wsparcie dla VMware ESXi 7.x
95.	możliwość tworzenia tzw. CONSISTENCY GROUP zapewniających identyczną konsystencję dla przynależących do danej grupy maszyn wirtualnych (VM), wymagane wsparcie dla min. 250 CONSISTENCY GROUP
96.	zabezpieczenie realizowane za pośrednictwem ciągłej replikacji (a nie za pomocą SNAPSHOT'ów) na poziomie VMDK oraz RDM, niezależnie od użytego storage'u (tzw. Storage Agnostic -warunkiem jest wsparcie przez VMware), wymagane wsparcie dla połączeń: FC, FCoE, iSCSI, NAS oraz DAS
97.	wsparcie dla replikacji (bi-directional) asynchronicznej oraz synchronicznej (realizowanej na poziomie dostarczanego oprogramowania), połączonych z mechanizmem tzw. JOURNALING umożliwiającego odnotowanie wszystkich zmian zabezpieczanego środowiska
98.	odporność na krótkotrwałe problemy (przeciążenie, zaniki) związane z siecią WAN
99.	wbudowana funkcjonalność deduplikacji oraz kompresji w przypadku transmisji danych poprzez WAN
100.	wsparcie dla równoległej replikacji zabezpieczanego środowiska do różnych ośrodków docelowych (min. 3-ech), wsparcie dla replikacji równoległej powinno być zapewnione również na poziomie grup konsystencji (CONSISTENCY GROUP)
101.	proponowane rozwiązanie powinno umożliwiać: stworzenia DISASTER RECOVERY dla całego zabezpieczanego wirtualnego środowiska zbudowanego w oparciu o VMware • operacyjne ODTWARZANIE dowolnej maszyny VM wraz z aplikacjami • MIGRACJI danych w trybie ON-LINE na inne zasoby dyskowe
102.	równoległe wsparcie środowisk lokalnych oraz zdalnych, wymagana możliwość pracy w 3-ech trybach, tzw.: CDP (Continuous Data Protection … tryb replikacji lokalnej), CRR (Continuous Remote Replication … tryb replikacji zdalnej), CLR (Continuous Local and Remote Replication … połączenie CDP oraz CLR … tryb replikacji lokalnej oraz zdalnej) w ramach dostarczonych licencji

103.	granularność umożliwiająca pominięcie określonych plików VMDK związanych z wirtualnymi serwerami VM objętych protekcją
104.	architektura FAULT-TOLERANT, brak pojedynczego punktu awarii
105.	wyskalowanie systemu powinno gwarantować RPO (Recovery Point Objective) w przypadku codziennej pracy ciągłej na poziomie pojedynczych sekund
106.	proponowana konfiguracja systemu powinna zapewnić następującą retencję przechowywanych kopii bezpieczeństwa: - RPO=30s z ostatnich 24h, - RPO=24h z ostatniego tygodnia, - RPO=1tydzień z ostatniego miesiąca
107.	możliwość odtworzenia zabezpieczanego środowiska do dowolnego punktu w czasie
108.	możliwość trybu pracy umożliwiającego objęciem protekcją w sposób automatyczny nowo dodanych maszyn wirtualnych (VM)
109.	rozwiązanie powinno dopuszczać zmiany HW na poziomie infrastruktury zabezpieczanego środowiska bez negatywnego wpływu na działanie systemu
110.	możliwość użycia mechanizmu typu BOOKMARK dla oznaczenia konsystentnych kopii zabezpieczanych aplikacji
111.	wsparcie dla VSS, zapewnienie konsystencji aplikacji na poziomie VSS
112.	możliwość automatycznego przeprowadzania operacji typu FAILOVER/FAILBACK do dowolnego punktu w czasie dla określonych produkcyjnych serwerów wirtualnych (VM), w tym: odtworzenie, uruchomienie (z zachowaniem wymaganej sekwencji), konfigurację
113.	możliwość automatycznego przeprowadzania operacji typu FAILOVER/FAILBACK do dowolnego punktu w czasie określonych testowych maszyn wirtualnych (VM)
114.	możliwość automatycznego zainicjowania procesu REVERSE REPLICATION w przypadku procesów FAILOVER/FAILBACK
115.	możliwość przeprowadzania testów DR bez wpływu na zabezpieczane serwery produkcyjne oraz bez konieczności zmian w działaniu replikacji (np.: PAUSE, REVERSE, …)
116.	możliwość skryptowego tworzenia planów RECOVERY

Deduplikator 1 szt., oferowane urządzenie musi spełniać następujące wymagania

118.	Dostarczone urządzenie musi oferować przestrzeń min. 8TB netto (powierzchni użytkowej) bez uwzględniania mechanizmów protekcji, wymagana skalowalność do min. 170TB netto.
119.	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 polityka retencyjną), bez pośrednictwa dodatkowych urządzeń (typu GATEWAY) powinny zostać przemigrowane (w postaci zdeduplikowanej) na dodatkową warstwę, wymagane wsparcie dla dla AWS oraz Microsoft Azure. Wymagana enkrypcja danych przechowywanych na warstwie typu Cloud. Wymagane dostarczenie licencji na przestrzeń min. 64TB netto dla warstwy CLOUD.
120.	Oferowane urządzenie musi posiadać minimum: • 4 porty Eth 10Gb/s OP (wraz z 4-a wkładkami SFP) • 2 porty FC 16Gb/s (wraz z wkładkami) wymagana możliwość obsługi każdym z w/w portów protokołów CIFS, NFS, deduplikacja na źródle Wymagana możliwość rozbudowy o kolejne: • 2 porty Eth 10 Gb/s OP wymagana możliwość obsługi poprzez porty FC protokołów VTL oraz deduplikacja na źródle.
121.	Oferowane urządzenie musi umożliwiać jednoczesny dostęp wszystkimi poniższymi protokołami: • CIFS, NFS • zapewniającymi deduplikację na źródle – wymagane wsparcie dla oferowanej aplikacji backupowej • VTL (min. 10 jednocześnie)
122.	Wymagane jest dostarczenie licencji, pozwalającej na jednoczesną obsługę protokołów CIFS, NFS, VTL oraz umożliwiwiającego deduplikację na źródle wspieraną przez oferowaną aplikację backupową dla maksymalnej pojemności urządzenia
123.	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).

117.	Urządzenie musi być przeznaczone do deduplikacji i przechowywania kopii zapasowych. Urządzenie musi spełniać wymagania wyspecyfikowane w niniejszej tabeli.

124.	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.
125.	Oferowane urządzenie musi mieć możliwość emulacji następujących bibliotek taśmowych:

	• StorageTek L180 lub • IBM TS 3500
126.	Oferowane urządzenie musi mieć możliwość emulacji napędów taśmowych min. LTO5 oraz LTO7
127.	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.
128.	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.
129.	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.

130.	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.
131.	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.
132.	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)
133.	Wszystkie unikalne bloki przed zapisaniem na dysk muszą być dodatkowo kompresowane.
134.	Oferowane urządzenie musi wspierać (wymagane formalne wsparcie producenta urządzenia), co najmniej następujące aplikacje: oferowana aplikacja backup'owa, RMAN, Microsoft SQL Server Management Studio. W przypadku współpracy z każdą z poniższych aplikacji:

	• oferowana aplikacja backup'owa • 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 danych odbywa się na dowolnym serwerze posiadającym funkcjonalność: Media Agenta / klienta /serwera RMAN / serwera SQL . 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, ew. licencje wymagane do realizacji opisanej funkcjonalności są przedmiotem tego postępowania.

135.	W przypadku przyjmowania backupów z 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, ew. licencje wymagane do realizacji opisanej funkcjonalności są przedmiotem tego postępowania.
136.	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 ew. licencje wymagane do realizacji opisanej funkcjonalności są przedmiotem tego postępowania.
137.	Oferowane urządzenie powinno umożliwiać uruchamianie maszyn wirtualnych VMware bezpośrednio z danych backupowych bez konieczności odtwarzania danych – funkcjonalność ta musi być oficjalnie wspierana i zintegrowana z oferowaną aplikacją backupową.
138.	W przypadku deduplikacji na źródle poprzez sieć IP (LAN oraz WAN), wymagana możliwość szyfrowania komunikacji kluczem minimum 256 bitów.
139.	Urządzenie powinno umożliwiać zaszyfrowanie przechowywanych danych, wymagane licencje umożliwiające zaszyfrowanie i przechowywanie zaszyfrowanych danych w obrębie maksymalnej pojemności oferowanego urządzenia.
140.	Urządzenie musi wspierać deduplikację na źródle poprzez sieć FC (SAN) minimum dla następujących systemów operacyjnych: • Windows • Linux (RedHat, SuSE)
141.	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 urządznia 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 nie jest przedmiotem postępowania.
142.	Urządzenie musi umożliwiać wydzielenie określonych portów Ethernet dedykowanych do replikacji.

143.	W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami.
144.	W przypadku replikacji danych między dwoma urządzeniami oferowanego typu, wymagana możliwość kontroli przez: oferowaną aplikację backup'ową, 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, 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
145.	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%.
146.	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.
147.	Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6 bądź równoważnej.
148.	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/odtwarzania backupów).
149.	Urządzenie musi pozwalać na przechowywanie minimum 700 Snapshotów jednocześnie w obrębie oferowanej przestrzeni, przy zachowaniu globalnej deduplikacji oraz standardowego trybu pracy urządzenia – umożliwiającego wykorzystanie wszystkich dostępnych funkcjonalności.
150.	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).
151.	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.

152.	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.
153.	Wymagana możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia, jako niezależnego urządzenia dostępnego za pośrednictwem: • CIFS • NFS • VTL • deduplikacja na źródle
154.	Urządzenie powinno umożliwiać zdefiniowanie blokady skasowania danych (funkcjonalność WORM). Blokada skasowania danych musi chronić plik w zdefiniowanym czasie przed usunięciem pliku oraz 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) lub ISO Standard 15489-1 w zakresie ochrony danych Licencje na blokadę WORM muszą być dostarczone wraz z urządzeniem. W przypadku braku wymaganej funkcjonalności WORM, wymagana dostawa dodatkowej macierzy typu NAS (NFS/CIFS) o pojemności netto dwukrotnie większej od wymaganej pojemności netto deduplikatora (8TB x 2 = 16TB 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. Blokada WORM (zarówno w przypadku deduplikatora jak i macierzy NAS) musi być zintegrowana z oferowaną aplikacją backup'ową co oznacza: • możliwość uruchomienia blokady WORM dla określonych danych z poziomu oferowanej aplikacji backup'owej • możliwość określenia/wymuszenia czasu blokady z poziomu oferowanej aplikacji backup'owej • możliwość raportowania od strony oferowanej aplikacji backup'owej danych zabezpieczonych przed usunięciem wymaganą blokadą WORM

155.	Urządzenie musi mieć możliwość przechowywania danych niezmienialnych: Video

	• Grafika • Nagrania dźwiękowe • Pliki pdf na udziałach CIFS/NFS.
156.	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 powinna być realizowana w locie, czyli przed usunięciem z pamięci oryginalnych danych (otrzymanych z aplikacji backupowej), musi być realizowana w trybie ciągłym (a nie adhoc), wymagane parametry wydajnościowe urzadzenia muszą uwzględniać tę funkcjonalność. Wymagane potwierdzenie opisanej funkcjonalności w oficjalnej dokumentacji producenta oferowanego urządzenia.
157.	Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia.
158.	Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu).
159.	Wymagana możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora).
160.	Wymagana możliwość zdefiniowania harmonogramu wg. którego wykonywany jest proces usuwania przeterminowanych danych (czyszczenia), realizowany równolegle z procesami backup/restore/replication.
161.	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).
162.	Urządzenie musi umożliwiać systemowo (wbudowana funkcjonalnosc) - realizację procesu pierwszego czyszczenia dopiero po przekroczeniu 75% zajętości oferowanej przestrzeni.
163.	Urządzenie musi mieć możliwość zarządzania poprzez • Interfejs graficzny dostępny z przeglądarki internetowej • Poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell)
164.	Oprogramowanie do zarządzania musi rezydować na oferowanym na urządzeniu deduplikacyjnym.

165.	Urządzenie musi być rozwiązaniem kompletnym, appliancem 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.