Załącznik nr 1 do OPZ

Wymagane minimalne parametry techniczne

1. Serwer rakowy – 1 szt.

Wymagania minimalne przedstawia poniższa tabela:

Lp.	Nazwa	Wymagane minimalne parametry techniczne
1.	Obudowa	1. Maksymalnie 2U RACK 19 cali (wraz z szynami montażowymi oraz ramieniem do prowadzenia kabli, umożliwiającymi serwisowanie serwera w szafie rack bez wyłączania urządzenia). 2. Obudowa serwera musi umożliwiać instalację min. 8 dysków 3,5”, typu Hot Swap, SAS/SATA. 3. Szyny montażowe muszą być kompatybilne z szafą serwerową Zamawiającego Dell Netshelter SX 42U.
2.	Płyta główna	Płyta główna z możliwością zainstalowania min. dwóch procesorów klasy serwerowej. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
3.	Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
4.	Procesor	Zainstalowane min. dwa procesory ośmiordzeniowe klasy x86 – 64 bity, dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 169 punktów w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. Do oferty należy załączyć wydruk ze strony potwierdzający osiągnięty wynik dla oferowanego modelu serwera.
5.	Pamięć operacyjna	1. Min. 128 GB RDIMM DDR4 5600MT/s. 2. Płyta główna musi posiadać min. 16 slotów do instalacji pamięci i umożliwiać obsługę do minimum 1TB RDIMM pamięci. 3. Obsługa zabezpieczeń i funkcjonalności, min: Demand Scrubbing, Patrol Scrubbing, Permanent Fault Detection (PFD).
6.	Gniazda PCIe	Serwer musi posiadać minimum 4 sloty PCI-Express, w tym: 1) Minimum 3 sloty PCI-Express działające z prędkością x16. 2) Minimum 1 slot działające z prędkością x8.
7.	Interfejsy sieciowe/FC/SAS	1. Minimum 2 wbudowane interfejsy sieciowe 1 Gb Ethernet BaseT, które nie zajmują gniazd PCIe. 2. Min. wbudowane lub zainstalowane 2 interfejsy sieciowe obsługujące prędkości 10Gb Ethernet BaseT. 3. Min. 2 porty SAS obsługujące prędkości 12Gb/s wyprowadzone na zewnątrz obudowy.
8.	Dyski twarde	Zainstalowane dyski: 1) Min. 2x480GB M.2 NVMe Hot-Swap z możliwością konfiguracji RAID 1. 2) Min. 8x 4TB NearLine SAS 7.2K. Możliwość instalacji dysków SFF SAS/SATA/SSD, 2,5” lub 3,5.

9.	Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający min. 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID min.: 0, 1, 5, 6, 10, 50, 60, non-RAID (JBOD).
10.	Porty	2x USB, w tym min. 1 porty USB 3.0; 1 port VGA.
11.	Karta graficzna	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900.
12.	Chłodzenie	Zestaw wentylatorów redundantnych.
13.	Zasilacz	Minimum 2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 1100 W Titanium.
14.	System operacyjny/ dodatkowe oprogramowanie	**System musi być zainstalowany na serwerze (przez producenta lub Wykonawcę).** Zakres Przedmiotu Zamówienia obejmuje dostarczenie Oprogramowania Systemowego zwanego dalej SSO. Licencja musi uprawniać do uruchamiania SSO w środowisku fizycznym i czterech wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji. SSO musi posiadać następujące, wbudowane cechy: 1. Możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny. 3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych. 4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading). 8. Wbudowane wsparcie instalacji i pracy na wolumenach, które: 1) pozwalają na zmianę rozmiaru w czasie pracy systemu, 2) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, 3) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,

		4) umożliwiają zdefiniowanie list kontroli dostępu (ACL). 9. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 10. Wbudowane szyfrowanie dysków. 11. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET. 12. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 13. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 14. Graficzny interfejs użytkownika. 15. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe. 16. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 17. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 18. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 19. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: 1) podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, 2) usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: a. podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, b. ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, c. odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza, 3) zdalna dystrybucja oprogramowania na stacje robocze, 4) praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, 5) centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: a. dystrybucję certyfikatów poprzez http,

		b. konsolidację CA dla wielu lasów domeny, c. automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, 6) szyfrowanie plików i folderów, 7) szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), 8) możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów, 9) serwis udostępniania stron WWW, 10) wsparcie dla protokołu IP w wersji 6 (IPv6), 11) wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: a. dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, b. obsługi ramek typu jumbo frames dla maszyn wirtualnych, c. obsługi 4-KB sektorów dysków, d. nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, e. możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, f. możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model), 12) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet, 13) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath), 14) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego, 15) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, 16) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

15.	Bezpieczeństwo	1. Zatrzask górnej pokrywy oraz blokada na ramce panelu zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. 2. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. 3. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła 4. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. 5. Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera. 6. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem. 7. Możliwość integracji z RSA SecurID. 8. 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. **– załączyć do oferty dokumentację techniczną potwierdzającą spełnienie norm lub oświadczenie producenta serwera o spełnieniu normy.** 9. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). 10. Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania.
16.	Diagnostyka	Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlanie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
17.	Karta/ Moduł zarządzający	Rozwiązanie sprzętowe (tzn. Moduł), niezależne od systemów operacyjnych, zintegrowane z płytą główną lub montowane niezależnie na płycie głównej, nieograniczające w żaden sposób dostępnych wymaganych portów/slotów w zaoferowanym Serwerze, posiadające dedykowany port RJ45 i umożliwiające: 1. Zdalny dostęp do graficznego interfejsu Web karty zarządzającej. 2. Szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika. 3. Możliwość podmontowania zdalnych wirtualnych napędów. 4. Wirtualną konsolę z dostępem do myszy, klawiatury. 5. Wsparcie dla IPv6. 6. Wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH. 7. Możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz.

		8. Możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer. 9. Integracja z Active Directory. 10. Możliwość obsługi przez ośmiu administratorów jednocześnie. 11. Wsparcie dla automatycznej rejestracji DNS. 12. Wsparcie dla LLDP. 13. Wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. 14. Możliwość podłączenia lokalnego poprzez złącze RS-232. 15. Możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy. 16. Monitorowanie zużycia dysków SSD. 17. Możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi. 18. Automatyczne zgłaszanie alertów do centrum serwisowego producenta. 19. Automatyczne update firmware dla wszystkich komponentów serwera. 20. Możliwość przywrócenia poprzednich wersji firmware. 21. Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON. 22. Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych. 23. Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram. 24. Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera. 25. Serwer musi posiadać możliwość uruchomienia funkcjonalności umożliwiającej 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 lub WIFI. Karta powinna umożliwiać rozszerzenie funkcjonalności o: 1. Możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych. 2. Kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania. 3. Automatyczne odświeżanie certyfikatów SSL. 4. Możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielkoskładnikowego przy logowaniu do karty zarządzającej. 5. Możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień. 6. Możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera. 7. Możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer.

		8. Możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe. 9. Monitorowanie przepływu powietrza na bieżąco.
18.	Dodatkowe oprogramowanie do zarządzania	Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniające poniższe wymagania: 1. Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych. 2. Integracja z Active Directory. 3. Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta. 4. Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish. 5. Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram. 6. Szczegółowy opis wykrytych systemów oraz ich komponentów. 7. Możliwość eksportu raportu do CSV, HTML, XLS, PDF. 8. Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. 9. Grupowanie urządzeń w oparciu o kryteria użytkownika. 10. Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji. 11. Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach. 12. Szybki podgląd stanu środowiska. 13. Podsumowanie stanu dla każdego urządzenia. 14. Szczegółowy status urządzenia/elementu/komponentu. 15. Generowanie alertów przy zmianie stanu urządzenia. 16. Filtry raportów umożliwiające podgląd najważniejszych zdarzeń. 17. Integracja z service desk producenta dostarczonej platformy sprzętowej. 18. Możliwość przejęcia zdalnego pulpitu. 19. Możliwość podmontowania wirtualnego napędu. 20. Kreator umożliwiający dostosowanie akcji dla wybranych alertów. 21. Możliwość importu plików MIB. 22. Przesyłanie alertów „as-is” do innych konsol firm trzecich. 23. Możliwość definiowania ról administratorów. 24. Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów. 25. Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania). 26. Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta. 27. Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów.

		28. 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. 29. Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. 30. Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile. 31. Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. 32. Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. 33. Zdalne uruchamianie diagnostyki serwera. 34. Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. 35. Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
19.	Certyfikaty	1. Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001. Serwer musi posiadać deklaracja CE. 2. Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 na potwierdzenie warunku należy przedstawić certyfikat PN-EN ISO 50001 lub oświadczenie producenta o stosowaniu w fabrykach polityki zarządzania energią, która jest zgodna z obowiązującymi przepisami na terenie Unii Europejskiej. 3. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019 x64, Microsoft Windows Server 2022 x64. Na potwierdzenie powyższych warunków z tego wiersza tabeli należy przedstawić stosowne certyfikaty lub oświadczenia producenta. **Dokumenty potwierdzające należ dołączyć do oferty.**
20.	Normy Środowiskowe	1. 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 rozporządzenia nr 1272/2008WE. 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 Silver według normy wprowadzonej w 2019 roku. 2. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych – **w postaci oświadczenia producenta serwera.** Na potwierdzenie powyższych warunków z tego wiersza tabeli należy przedstawić stosowne dokumenty lub oświadczenia producenta. **Dokumenty potwierdzające należ dołączyć do oferty.**
21.	Warunki gwarancji	1. Minimum 36 miesięcy gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. 2. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych, a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy. 3. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. 4. 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. 5. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. 6. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej/internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik Wykonawcy/Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia/zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. 7. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. 8. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dostarczenia oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy

		pozostaje u Zamawiającego – **dokumenty potwierdzające należy dostarczyć Zamawiającemu w terminie 14 dni kalendarzowych od dnia podpisania umowy, jednak nie później niż 1 dzień roboczy przed rozpoczęciem fizycznych dostaw sprzętu komputerowego i oprogramowania objętego umową.** 9. Wymagane dostarczenie oświadczenia Producenta potwierdzającego, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta – **dokumenty potwierdzające należy dostarczyć Zamawiającemu w terminie 14 dni kalendarzowych od dnia podpisania umowy, jednak nie później niż 1 dzień roboczy przed rozpoczęciem fizycznych dostaw sprzętu komputerowego i oprogramowania objętego umową.** 10. Oświadczenie producenta serwera, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta – **dokumenty potwierdzające należy dostarczyć Zamawiającemu w terminie 14 dni kalendarzowych od dnia podpisania umowy, jednak nie później niż 1 dzień roboczy przed rozpoczęciem fizycznych dostaw sprzętu komputerowego i oprogramowania objętego umową.** 11. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji systemu. 12. Możliwość rozszerzenia gwarancji na koszt Zamawiającego przez producenta do 5 lat.
22	Elementy dodatkowe/montażowe	1. Szyny montażowe oraz ramie do prowadzenia kabli, umożliwiające serwisowanie serwera w szafie RACK bez wyłączania urządzenia. 2. Okablowanie: a. Dwa kable 1Gbps Ethernet kat. 6 w standardzie S/FTP, długości min. 5 m; b. Dwa kable 10 Gbps Ethernet kat. 7 w standardzie S/FTP, długości min. 5 m; c. Jeden kabel SAS 12 Gb/s, długość min. 1 m; d. Inne elementy montażowe o ile są wymagane do prawidłowego montażu i uruchomienia dostarczonego serwera, a nie zostały wymienione powyżej.
21.	Instalacja i konfiguracja	• Instalacja dostarczonego serwera we wskazanej przez Zamawiającego szafie RACK Dell Netshelter SX 42U. • Wpięcie w infrastrukturę Zamawiającego za pomocą interfejsów sieciowych/FC/SAS dostarczonego serwera wraz z ich konfiguracją. • W ramach dostawy i wdrożenia należy dostarczy stosowne okablowanie pozwalające na podłączenie serwera każdym z rodzajów interfejsów jakie wymieniono w wierszu 7 tej tabeli.

		• Instalacja i konfiguracja Oprogramowania Systemowego (SSO, system również może być preinstalowany przez Producenta) zgodnie z wymaganiami Zamawiającego. • Instalacja i konfiguracja RAID na dyskach: RAID-1 i RAID-10 zgodnie z wymaganiami Zamawiającego. • Instalacja dostarczonych modułów SAS (w razie konieczności). • Zainstalowanie/konfiguracja dostarczonego oprogramowania wirtualizacyjnego na serwerze. • Na życzenie Zamawiającego uruchomienie do czterech wirtualnych środowisk SSO o parametrach wskazanych przez Zamawiającego.
22.	Dokumentacja użytkownika	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.

2. Deduplikator – 1 szt.

Wymagania minimalne przedstawia poniższa tabela:

Lp.	Nazwa	Wymagane minimalne parametry techniczne.
1.	Urządzenie deduplikującego	Urządzenie musi być przeznaczone do deduplikacji i przechowywania kopii zapasowych i być rozwiązaniem sprzętowym.
2.	Dyski twarde/Cloud	1. Dostarczone urządzenie musi oferować przestrzeń min. 16TB netto (powierzchni użytkowej widocznej po założeniu systemu plików) bez uwzględniania mechanizmów protekcji. 2. Przestrzeń dedykowana do gromadzenia deduplikatów – wymagana skalowalność do min. 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 polityka retencyjną), bez pośrednictwa dodatkowych urządzeń (typu GATEWAY) powinny zostać przemigrowane (w postaci zdeduplikowanej) na dodatkową warstwę, wymagane wsparcie dla AWS, Microsoft Azure oraz Google GCP. Wymagana enkrypcja danych przechowywanych na warstwie typu Cloud. Wymagane dostarczenie licencji na przestrzeń min. 60TB netto dla warstwy CLOUD.
3.	Liczba portów	1. Oferowane urządzenie musi posiadać minimum: 4 porty 10Gb/s Eth BaseT. 2. Wymagana możliwość dodania do w/w konfiguracji portów: 2 porty FC 16Gb/s. 3. Wymagana możliwość obsługi poprzez porty FC protokołów VTL oraz deduplikacja na źródle.
4.	Protokoły	Oferowane urządzenie musi umożliwiać jednoczesny dostęp wszystkimi poniższymi protokołami: a) CIFS, NFS; b) zapewniającym deduplikację na źródle, wymagane wsparcie dla Veeam Backup and Replication oraz NetWorker;

		c) VTL (min. 10 jednocześnie).
5.	Licencje	Wymagane jest dostarczenie licencji, pozwalającej na jednoczesną obsługę protokołów CIFS, NFS, dedupliakacja na źródle, VTL do oferowanej pojemności urządzenia.
6.	Pozostałe parametry sprzętowego urządzenia deduplikującego	1. 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). 2. Urządzenie musi pozwalać na jednoczesną obsługę minimum 250 strumieni w tym jednocześnie: a) zapis danych minimum 150 strumieniami; b) odczyt danych minimum 50 strumieniami; c) 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. 3) 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. 4) Wszystkie zapisywane strumienie muszą podlegać globalnej deduplikacji przed zapisem na dysk (in-line) jak opisano w niniejszej specyfikacji. 5) Oferowane urządzenie musi mieć możliwość emulacji następujących bibliotek taśmowych: a) StorageTek L180; b) IBM TS 3500. 6) Oferowane urządzenie musi mieć możliwość emulacji napędów taśmowych min. LTO5 oraz LTO7. 7) 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. 8) 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. 9) 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. 10) 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. 11) 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 backu'owej, dane zapisywane poprzez interfejsy NFS CIFS bez użycia jakiejkolwiek aplikacji backup'owej również muszą być deduplikowane w sposób in-line. 12) 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). 13) Wszystkie unikalne bloki przed zapisaniem na dysk muszą być dodatkowo kompresowane.

		14) 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, wymaganie dotyczy wszystkich danych zapisanych na urządzeniu a nie wybranych grup danych objętych działaniem blokad zabezpieczających przed usunięciem/modyfikacją danych. 15) Oferowane urządzenie musi wspierać (wymagane formalne wsparcie producenta urządzenia), co najmniej następujące aplikacje: a. Veeam Backup and Replication, b. NetWorker, RMAN, c. Microsoft SQL Server Management Studio. W przypadku współpracy z każdą z poniższych aplikacji:Veeam Backup and Replication; NetWorker; RMAN (dla ORACLE); Microsoft SQL Server Management Studio (dla Microsoft SQL), urządzenie musi umożliwiać deduplikację na źródle (w przypadku Veeam B&R: na poziomie - proxy Data Mover, w przypadku NetWorker na poziomie – Client, w przypadku RMAN - serwera RMAN, w przypadku SQL – serwera SQL) 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. 16) W przypadku przyjmowania backupów z Veeam Backup and Replication, NetWorker, Oracle RMAN oraz Microsoft MSSQL (przy wykorzystaniu Microsoft SQL Server Management Studio), urządzenie musi umożliwiać deduplikację na źródle (w przypadku Veeam B&R: na poziomie - proxy Data Mover, w przypadku NetWorker na poziomie – Client, w przypadku RMAN - serwera RMAN, w przypadku SQL – serwera SQL) 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. 17) 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 oraz NetWorker. 18) Wymagana funkcjonalność Load Balancing oraz Link Failover w obrębie portów wykorzystywanych przez aplikację backupową, wymagane wsparcie tej funkcjonlaności dla Veeam Backup and Replication oraz NetWorker.

		19) Wymagane wsparcie dla backupów typu Virtual Synthetics w przypadku aplikacji Veeam Backup and Replication oraz NetWorker. 20) W przypadku deduplikacji na źródle poprzez sieć IP (LAN oraz WAN), wymagana możliwość szyfrowania komunikacji kluczem minimum 256 bitów. 21) Urządzenie musi umożliwiać zaszyfrowanie przechowywanych danych, wymagane licencje umożliwiające zaszyfrowanie i przechowywanie zaszyfrowanych danych w obrębie maksymalnej pojemności oferowanego urządzenia. 22) Urządzenie musi wspierać deduplikację na źródle poprzez sieć FC (SAN) minimum dla następujących systemów operacyjnych: Windows oraz Linux (RedHat, SuSE). 23) Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych do drugiego urządzenia takiego samego typu. Konfiguracja replikacji musi być możliwa w każdym z trybów: a. jeden do jednego; b. wiele do jednego; c. jeden do wielu; d. 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. 24) Urządzenie musi umożliwiać wydzielenie określonych portów Ethernet dedykowanych do replikacji. 25) W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami.W przypadku replikacji danych między dwoma urządzeniami oferowanego typu, wymagana możliwość kontroli przez: NetWorker oraz Microsoft SQL Server Management Studio, muszą być możliwe do uzyskania jednocześnie wszystkie następujące funkcjonalności: a. replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału serwerów pośredniczących; b. replikacji podlegają tylko te fragmenty danych (na poziomie bloków używanych do deduplikacji), które nie znajdują się na docelowym urządzeniu; c. replikacja zarządzana jest z poziomu wymaganej aplikacji; d. aplikacja posiada informację o obydwu kopiach zapasowych znajdujących się w obydwu urządzeniach bez konieczności przeprowadzania procesu inwentaryzacji. 26) 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%. 27) 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. 28) Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6 bądź równoważnej. 29) 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/odtwarzania backupów). 30) 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. 31) 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). 32) 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. 33) 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. 34) Wymagana możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia, jako niezależnego urządzenia dostępnego za pośrednictwem: a. CIFS; b. NFS; c. VTL; d. deduplikacja na źródle. 35) 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): a. Możliwość zdjęcia blokady przed upływem ważności danych (wymagane oficjalne wsparcie przez NetWorker). b. 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 przez 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). 36) Urządzenie musi mieć możliwość przechowywania danych niezmienialnych: Video, Grafika, nagrania dźwiękowe, pliki pdf, na udziałach CIFS/NFS. 37) 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). 38) Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia. 39) Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu). 40) 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). 41) Wymagana możliwość zdefiniowania harmonogramu wg. którego wykonywany jest proces usuwania przeterminowanych danych (czyszczenia), realizowany równolegle z procesami backup/restore/replication. 42) 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). 43) Urządzenie musi umożliwiać systemowo (wbudowana funkcjonalność) - realizację procesu pierwszego czyszczenia dopiero po przekroczeniu 75% zajętości oferowanej przestrzeni. 44) Urządzenie musi mieć możliwość zarządzania poprzez: a. Interfejs graficzny dostępny z przeglądarki internetowej b. Poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell). 45) Oprogramowanie do zarządzania musi rezydować na oferowanym na urządzeniu deduplikacyjnym. 46) 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. 47) 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.
7.	Gwarancja	Oferowane urządzenie powinno być objęte 36 miesięcznym wsparciem producenta działającym w trybie zgłaszania awarii: 24x7 oraz reakcją NBD, uszkodzone nośniki dyskowe pozostają u Zamawiającego bez ponoszenia dodatkowych kosztów.
8.	Instalacja i konfiguracja	1. Instalacja dostarczonego deduplikatora we wskazanej przez Zamawiającego szafie rack Dell Netshelter SX 42U. 2. Wpięcie w infrastrukturę Zamawiającego wraz z ich konfiguracją. 3. W ramach dostawy i wdrożenia należy dostarczy stosowne okablowanie pozwalające na podłączenie deduplikatora do sieci Zamawiającego. Długość min. 3 m. 4. Konfiguracja startowa deduplikatora zgodnie z wymaganiami Zamawiającego.
9.	Elementy montażowe	Szyny umożliwiające montaż urządzenia w posiadanej szafie serwerowej Dell Netshelter SX 42U przez Zamawiającego.

3. Wsparcie dla Systemu Bezpieczeństwa – 1 szt.

Zamawiający posiada urządzenie Hillstone NIPS S1560. W ramach niniejszej pozycji Zamawiający oczekuje dostawy przedłużenia subskrypcji na okres 24 m-cy, liczony od dnia dostawy, lub dostawy równoważnego systemu bezpieczeństwa ze wsparciem producenta na okres 24 m-cy, **spełniającego poniższe wymagania:**

Lp.	Nazwa	Wymagane minimalne parametry techniczne
1.	Wymagania Ogólne	1. System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. 2. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. 3. System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. 4. System wspiera protokoły IPv4 oraz IPv6 w zakresie: a. Firewall. b. Ochrony w warstwie aplikacji. c. Protokołów routingu dynamicznego.
2.	Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
3.	Interfejsy, Dysk, Zasilanie	1. System realizujący funkcję Firewall musi dysponować co najmniej poniższą liczbą i rodzajem interfejsów: 1) 10 portami 1 Gigabit Ethernet RJ-45. 2) 8 portami 5/2.5/1 Gigabit Ethernet RJ-45. 3) 4 gniazdami SFP 1 Gbps. 4) 8 gniazdami SFP+ 10 Gbps.

		2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. System Firewall musi pozwalać skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System jest wyposażony w dwa zasilacze AC.
4.	Parametry wydajnościowe	1. W zakresie Firewall'a obsługa nie mniej niż 10 mln. jednoczesnych połączeń oraz 350 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 36 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 12 Gbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 32 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 7 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 6 Gbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 4 Gbps.
5.	Funkcje Systemu Bezpieczeństwa	W ramach systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.

		13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
6.	Polityki Firewall	1. Polityka Firewall musi uwzględniać: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi realizować translację adresów NAT: źródłowego i docelowego, translację PAT oraz: 1) Translację jeden do jeden oraz jeden do wielu. 2) Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. 5. Polityka firewall musi umożliwiać filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 7. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. 1) Amazon Web Services (AWS). 2) Microsoft Azure. 3) Cisco ACI. 4) Google Cloud Platform (GCP). 5) OpenStack. 6) VMware NSX. 7) Kubernetes.
7.	Połączenia VPN	1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: 1) Wsparcie dla IKE v1 oraz v2. 2) Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). 3) Obsługa protokołu Diffie-Hellman grup 19, 20. 4) Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. 5) Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. 6) Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. 7) Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. 8) Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.

		9) Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. 10) Możliwość monitorowania wybranego tunelu IPSec site-to-site, w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. 11) Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. 12) Mechanizm „Split tunneling" dla połączeń Client-to-Site. 2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: 1) Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0. 2) Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta. 3) Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
8.	Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie musi zapewniać obsługę: 1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
9.	Funkcje SD-WAN	1. System musi umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
10.	Zarządzanie pasmem	1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System musi dawać możliwość określania pasma dla poszczególnych aplikacji.

		3. System musi pozwalać zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
13.	Ochrona przed malware	1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy musi zapewniać skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. System musi umożliwiać skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości. 4. System musi umożliwiać blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 7. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze. 8. System musi zapewniać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
14.	Ochrona przed atakami	1. Ochrona IPS musi opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System musi chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków musi zawierać minimum 17000 wpisów i musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.

		6. Rozwiązanie musi posiadać mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 7. Rozwiązanie musi posiadać możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. 8. Rozwiązanie musi posiadać funkcjonalność wykrywania i blokowania komunikacji C&C do sieci botnet. 9. Rozwiązanie musi posiadać możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
15.	Kontrola aplikacji	1. Funkcja Kontroli Aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji musi zawierać minimum 5000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) muszą być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur musi zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. 6. Rozwiązanie musi posiadać możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 7. System musi dawać możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
16.	Kontrola WWW	1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 60 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra WWW muszą być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem np.: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW musi umożliwiać statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW musi dawać możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.

		7. Rozwiązanie musi posiadać funkcje Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
17.	Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: 1) Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. 2) Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. 3) Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. System musi dawać możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. 3. System musi umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. 4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
18.	Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Rozwiązanie musi posiadać możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System musi dawać możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

		8. Rozwiązanie musi posiadać możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). 9. Rozwiązanie musi posiadać możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
19.	Logowanie	1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania element systemu pełniący funkcję Firewall musi zapewniać przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 4. Rozwiązanie musi posiadać możliwość włączenia logowania per reguła w polityce firewall. 5. System musi zapewniać możliwość logowania do serwera SYSLOG. 6. Przesyłanie SYSLOG do zewnętrznych systemów musi być możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
20.	Testy wydajnościowe oraz funkcjonalne	Wszystkie funkcje i parametry wydajnościowe systemu muszą móc być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.
21.	Serwisy i licencje	1. Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów często wymagane są dodatkowe licencje, dla tego w takim przypadku trzeba zapewnić je **na okres min. 24 miesięcy** od daty dostawy dla wymienionych modułów: 1) Kontrola Aplikacji; 2) IPS; 3) Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android); 4) Analiza typu Sandbox cloud; 5) Antyspam; 6) Web Filtering; 7) bazy reputacyjne adresów IP/domen. 2. Ponadto należy zapewnić logowanie i raportowanie w oparciu o usługę realizowaną w chmurze, z czasem retencji logów minimum 12 miesięcy, **na okres min. 24 miesięcy od daty dostawy.**
22.	Gwarancja oraz wsparcie	1. System musi być objęty serwisem gwarancyjnym producenta przez okres **min. 24 miesięcy** od daty dostarczenia, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement).

		2. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
23.	Wdrożenie/Instalacja i konfiguracja	W przypadku zaoferowania rozwiązania alternatywnego (inne niż Hillstone) Zamawiający wymaga: 1. Przeprowadzenia przez Wykonawcę audytu istniejących urządzeń UTM u Zamawiającego pod kątem dobrych praktyk i poprawności pracy. 2. Opracowania przez Wykonawcę na podstawie wyników audytu, w konsultacji z Zamawiającym projektu technicznego wdrożenia, obejmującego między innymi: 1) Instalację dostarczonego urządzenia UTM we wskazanej przez Zamawiającego szafie RACK oraz wpięcia w infrastrukturę sieciową Zamawiającego. 2) Przeniesienie istniejących konfiguracji na nowe urządzenie/a z uwzględnieniem audytu, dobrych praktyk i poprawności pracy. 3) W przypadku dodatkowych modułów, które nie mają odzwierciedlenia w dotychczas stosowanych urządzeniach Zamawiającego, należy wykonać konfigurację startową tych modułów z zachowaniem dobrych praktyk i poprawności pracy oraz w porozumieniu z Zamawiającym. 4) Wykonać konfigurację zarządzania (SSH, HTTPS, SNMP). 5) Opracować scenariusze testów akceptacyjnych. 3. Wdrożenia urządzenia/urządzeń UTM zgodnie z opracowanym projektem technicznym. 4. Realizacji testów akceptacyjnych. 5. Wymagane jest posiadanie, co najmniej dwóch osób wyznaczonych do realizacji zamówienia z aktualnym certyfikatem producenta oferowanego rozwiązania. W tym celu wykonawca musi posiadać, co najmniej dwóch inżynierów (wyznaczonych do realizacji prac związanych z wdrożeniem) posiadających aktualny certyfikat inżynierski producenta w zakresie konfiguracji, instalacji i monitorowania oferowanych zapór sieciowych. **Na wezwanie Zamawiającego Wykonawca jest zobowiązany przedstawić przed rozpoczęciem prac wymagane dokumenty.**
24.	Elementy montażowe	Wykonawca w ramach wdrożenia jest zobowiązany dostarczyć niezależnie od tego czy producent oferuje w zestawie z urządzeniem następujące elementy montażowe: 1) Szyny lub uchwyty umożliwiające montaż urządzenia w szafie typu RACK. 2) Okablowanie w ilości optymalnej, pozwalającej na wpięcie urządzenia/urządzeń w infrastrukturę sieciową Zamawiającego z uwzględnieniem interfejsów wymienionych w wierszu 3 tej tabeli oraz projektem technicznym wdrożenia, o którym mowa w wierszu 23 tej tabeli.

4. Program Antywirusowy – 300 szt.

W ramach niniejszej pozycji Zamawiający wymaga podniesienia wersji posiadanego oprogramowania ESET PROTECT Entry ON-PREM (ilości stanowisk: 300, ważne licencje do 17.12.2024 r) do wersji ESET PROTECT Enterprise, przedłużenia licencji o kolejne 24 m-ce wraz z zachowaniem liczby stanowisk tj. 300 szt., lub dostawa równoważnego systemu antywirusowego dla 300 stanowisk z okresem ważności min. do 17.12.2026 r.

Warunki dla oprogramowania równoważnego:

Dostawa oprogramowania antywirusowego zapewniającego ochronę 300 stanowisk ze wsparciem umożliwiającym aktualizację oprogramowania oraz sygnatur antywirusowych do minimum 17.12.2026 r. Oprogramowanie w ramach dostawy musi zostać wdrożone przez Wykonawcę w infrastrukturze Zamawiającego **w terminie do 18.12.2024 r.**

Pozostałe warunki równoważności przedstawia poniższa tabela:

Lp.	Nazwa	Wymagane minimalne parametry techniczne.
1.	Administracja zdalna w chmurze	1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego. 2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW. 3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL. 4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. 5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. 6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM. 7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak. 9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta. 10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. 11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. 12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo,

		comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.
2.	Ochrona stacji roboczych	1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). 2. Rozwiązanie musi wspierać architekturę ARM64. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. 5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. 9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku. 10. Rozwiązanie musi integrować się z Intel Threat Detection Technology. 11. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 13. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 14. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 15. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia. 16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:

		1) tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, 2) tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, 3) tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, 4) tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, 5) tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach. 17. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. 18. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. 19. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. 20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook. 23. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów: 1) tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące, 2) tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie, 3) tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora, 4) tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu. 24. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki. 25. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.

		26. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki. 27. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych. 28. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii. 29. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. 30. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
3.	Ochrona serwera	1. Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux. 2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS. 5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji. 7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. 8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. **Dodatkowe wymagania dla ochrony serwerów Windows:** 1. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. 2. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS). 3. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. 4. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

		5. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 6. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 7. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 8. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. 9. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu. **Dodatkowe wymagania dla ochrony serwerów Linux:** 1. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. 2. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. 3. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon. 4. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.
4.	Szyfrowanie	1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10 i Microsoft Windows 11. 2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault). 3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia. 4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
5.	Ochrona urządzeń mobilnych opartych o system Android	1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. 2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne. 3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).

		4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM. 5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi: 1) usunięcie zawartości urządzenia, 2) przywrócenie urządzenie do ustawień fabrycznych, 3) zablokowania urządzenia, 4) uruchomienie sygnału dźwiękowego, 5) lokalizację GPS. 6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. 7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: 1) nazwę aplikacji, 2) nazwę pakietu, 3) kategorię sklepu Google Play, 4) uprawnienia aplikacji, 5) pochodzenie aplikacji z nieznanego źródła.
6.	Sandbox w chmurze	1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. 2. Rozwiązanie musi wykorzystywać do działania chmurę producenta. 3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi. 4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta. 5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek. 6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania. 7. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów. 8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy. 9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione. 10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych. 11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo. 12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem: 1) Czysty; 2) Podejrzany; 3) Bardzo podejrzany;

		4) Szkodliwy. 13. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum. 14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki. 15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.
7.	Moduł XDR	1. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW. 2. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta. 3. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL. 4. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa. 5. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”. 6. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia. 7. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika. 8. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta. 9. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej. 10. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku. 11. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania. 12. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny. 13. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.

		14. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych. 15. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej podzespołów zarządzanego komputera, w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe oraz wylistowanie zainstalowanego oprogramowania firm trzecich. 16. Konsola administracyjna musi mieć możliwość tagowania obiektów. 17. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń PowerShell.
8.	Wdrożenie	1. Należy dostarczyć klucz produktu oraz najnowszą wersję oprogramowania na pendrive lub przesłać link na wskazany adres e-mail przez Zamawiającego, umożliwiający pobranie oprogramowania w zakupionej wersji ze strony producenta. Preferowana wersja interfejsu oprogramowania to język polski. 2. Należy dostarczyć instrukcję lub link do niej w języku polskim. Instrukcja musi tłumaczyć przynajmniej: proces instalacji oprogramowania na stacjach roboczych i serwerach, proces rejestracji stacji roboczych i serwerów w konsoli centralnej, instrukcję użytkowania konsoli centralnej, proces konfiguracji i użytkowania wszystkich modułów wchodzących w skład dostarczonego oprogramowania.

5. Rozbudowa oprogramowania backupowego Veeam – 1 szt.

W ramach niniejszej pozycji Zamawiający wymaga rozbudowy posiadanych licencji oprogramowania backupowego Veeam, lub dostawę równoważnego oprogramowania backupowego.

W ramach rozbudowy obecnego systemu backupowego należy wykonać poniższe czynności:

1) Wykonać dostawę niezbędnych licencji Veeam umożliwiających:
   a) upgrade posiadanych przez Zamawiającego licencji wieczystych Veeam Data Platform Foundation Universal (30 instancji) do wersji wieczystej Veeam Data Platform Advanced;
   b) rozszerzenie ulepszonych licencji wieczystych Veeam Data Platform Advanced o dodatkowe 10 instancji (do poziomu 40 instancji).
2) Dostarczenie nowych licencji Veeam Data Platform Premium w ilości minimum 10 instancji w formie subskrypcji na okres 12 m-cy.
3) Zamawiający wymaga aby wszystkie dostarczane licencje posiadały wsparcie producenta oraz prawa do aktualizacji nie krótsze niż do dnia 6.12.2025.

Warunki dla oprogramowania równoważnego z punktu 5, podpunkt 1-3, przedstawia poniższa tabela:

Lp.	Nazwa	Wymagane minimalne parametry techniczne.
1.	Wymagania ogólne	1. Dostarczone rozwiązanie musi być dostarczone **w formie licencji wieczystej.** 2. Dostarczone oprogramowanie musi umożliwiać wykonywanie kopii zapasowych z minimum 40 maszyn wirtualnych pracujących w środowisku wirtualizacyjnym (składającym się z trzech serwerów wirtualizacyjnych) lub 40 serwerów fizycznych, każdy z własną instancją systemu operacyjnego. 3. Dostarczone oprogramowanie musi być objęte wsparciem technicznym producenta przez okres minimum 12 m-cy. 4. Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie: - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5, 5. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej. 6. Oprogramowanie musi współpracować z infrastrukturą Nutanix w wersji 6.5.x - 6.7.x, Red Hat Virtualization 4.4 SP1, Oracle Linux Virtualization 4.5.4, lub nowszy oraz Proxmox VE 8.2, lub nowszy. 7. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure, Microsoft Azure Data Lake, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
2.	Całkowite koszty posiadania	1. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej. 2. Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania, których niewymagana jest osobna baza danych z metadanymi deduplikowanych bloków 3. Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji. 4. Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.

		5. Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli. 6. Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier. 7. Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu. 8. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania. 9. Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time). 10. Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu. 11. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API. 12. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji. 13. Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji. 14. Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania. 15. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych. 16. Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej. 17. Oprogramowanie musi wymagać autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np skasowanie backupu, dodanie kolejnego administratora). 18. Oprogramowanie musi posiadać integracje z systemami zarządzania kluczami szyfrującymi (KMS). 19. Oprogramowanie musi posiadać integracje z systemami typu SIEM. 20. Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji.

3.	Wymagania RPO (Recovery Point Objective)	1. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej. 2. Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych. 3. Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak, aby nieprzekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastoru. 4. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware. 5. Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware. 6. Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592). 7. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) 8. Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard. – Dodatkowo Zamawiający żąda wsparcia dla oferowanego deduplikatora oferowanego w pozycji 2. 9. Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS, jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS. 10. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN. 11. Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych, jako źródła replikacji. 12. Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO. 13. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik.

		14. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn, jako źródła do dalszej replikacji (replica seeding). 15. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN).
4.	Wymagania RTO (Recovery Time Objective)	1. Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych. 2. Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna). 3. Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami. 4. Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre. 5. Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze skompresowanego **pliku** i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne. 6. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków. 7. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform. 8. Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików. 9. Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V. 10. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell. 11. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM. 12. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.

		13. Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł. 14. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego. 15. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur. 16. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji. 17. Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux. 18. Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux. 19. Oprogramowanie musi wspierać granularne odtwarzanie baz danych MongoDB. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux. 20. Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji. 21. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN. 22. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle. 23. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI. 24. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2. 25. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN.
5.	Ograniczenie ryzyka	1. Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).

		2. Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach. 3. Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem. 4. Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32. 5. Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware. 6. Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania. 7. Oprogramowanie, bazując na wyuczonym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków. 8. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego. 9. Oprogramowanie musi mieć możliwość integracji z innymi systemami bezpieczeństwa - minimum Splunk, Palo Alto Networks XSOAR.
6.	Środowiska fizyczne	1. Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego. 2. Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych. 3. Rozwiązanie musi wspierać, co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE, Rocky Linux, AlmaLinux. 4. Rozwiązanie musi wspierać system operacyjny macOS. 5. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix. 6. Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą). 7. Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster 8. Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów. 9. Rozwiązanie musi wspierać backup podłączonych dysków USB.

		10. Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym. 11. Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury). 12. Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone. 13. Rozwiązanie musi wspierać kontrolę pasma sieciowego. 14. Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych. 15. Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN. 16. Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft. 17. Rozwiązanie musi wspierać technologię BitLocker. 18. Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania. 19. Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych. 20. Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych. 21. Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle I PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu. 22. Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform. 23. Rozwiązanie musi wspierać szyfrowanie. 24. Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache), gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne. 25. Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego. 26. Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej. 27. Rozwiązanie musi wspierać tworzenie wielu zadań backupowych.

7.	Monitoring	1. System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich. 2. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie. 3. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. 4. System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter. 5. System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn. 6. System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel. 7. System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk. 8. System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora. 9. System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów. 10. System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard). 11. System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna. 12. System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego. 13. System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta. 14. System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych. 15. System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu. 16. System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy Vmware

		17. System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji od 10.x do 10.6.
8.	Raportowanie	1. System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie. 2. System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. 3. System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów. 4. System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V. 5. System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF. 6. System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc. 7. System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach. 8. System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów 9. System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych 10. System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych. 11. System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury. 12. System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta.. 13. System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych. 14. System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’. 15. System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy Vmware.

		16. System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots). 17. System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie.
9.	Tworzenie planów odzyskiwania i ich automatyzacja	Dodatkowo Zamawiający wymaga, by dostarczone oprogramowanie równoważne umożliwiało stworzenie planów odzyskiwania i ich automatyzacji dla minimum 10 maszyn wirtualnych pracujących w środowisku wirtualizacyjnym (składającym się z trzech serwerów wirtualizacyjnych) lub 10 serwerów fizycznych, każdy z własną instancją systemu operacyjnego. **Oprogramowanie musi spełniać poniższe warunki:** 1. Rozwiązanie musi wspierać platformy oparte o VMware vSphere 6.0, 6.5, 6.7, 7.0, 8.0. 2. Rozwiązanie musi pozwalać na integrację z posiadanym Veeam Backup&Replication 12. 3. Rozwiązanie musi pozwalać na instalację komponentów na platformie Microsoft Windows Server 2012 -2022. 4. Rozwiązanie musi zapewniać zautomatyzowane przełączanie środowisk datacenter zgodnie z przygotowanym wcześniej planem odzyskiwania i migracji maszyn wirtualnych. 5. Rozwiązanie musi wykorzystywać do tego celu kopie zapasowe i repliki wykonane za pomocą Veeam Backup&Replication. 6. Rozwiązanie musi zapewniać zautomatyzowane testy potwierdzające odzyskiwalność oraz niezawodność planów odzyskiwania i migracji maszyn wirtualnych oraz zgodność z zaplanowanym SLA. 7. Rozwiązanie musi wykorzystywać do powyższych testów, mechanizmy izolacji środowiska (DataLabs) dostępne w Veeam Backup&Replication. 8. Rozwiązanie musi tworzyć dokumentację w sposób dynamiczny na podstawie stworzonych planów odzyskiwania i migracji maszyn. 9. Otrzymywane plany odzyskiwania muszą być dostępne w formacie Adobe PDF. 10. Rozwiązanie musi posiadać możliwość definiowania grup odbiorców powiadomień mailowych dla następujących wydarzeń: a. Aktualizacja planu odtwarzania; b. Raport wykonania planu odtwarzania; c. Raport wykonania testowego odtworzenia. 11. Rozwiązanie musi umożliwiać automatyczne dostosowywanie i aktualizowanie takiej dokumentacji według cyklicznego harmonogramu. 12. Rozwiązanie musi posiadać przynajmniej następujące predefiniowane kroki weryfikujące poprawność działających aplikacji po przełączeniu lub odtworzeniu w centrum zapasowym: a. Ping VM Network b. Check VM Heartbeat c. Generate Event d. Send Email e. Shutdown Source VM f. Start Service g. Verify DNS Port

		h. Verify Domain Controller Port i. Verify Exchange Mailbox j. Verify Exchange MAPI Connectivity k. Verify Exchange Services l. Verify Global Catalog Port m. Verify Mail Server Port n. Verify SharePoint URL o. Verify SQL Database p. Verify SQL Port q. Verify Web Server Port r. Verify Web Site (IIS) s. VM Power Actions t. Custom Script 13. Rozwiązanie musi posiadać pulpit informacyjny (dashboard) podsumowujący działanie awaryjnych planów odzyskiwania i testów. 14. Rozwiązanie musi zapewniać funkcjonalność delegacji uprawnień dla wybranych grup użytkowników. 15. Rozwiązanie musi pozwalać na tworzenie planów odzyskiwania użytkownikom niebędącym administratorami systemu. 16. Rozwiązanie musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter i pozwalać na dynamiczne grupowanie maszyn wirtualnych dodawanych do planów odzyskiwania. 17. Rozwiązanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API.
10.	Wdrożenie/instalacja/konfiguracja	1. Niezależnie od rodzaju oprogramowania (czy będzie to rozbudowa obecnego, czy dostawa równoważnego), należy je zainstalować je na serwerze z punktu 1 tej specyfikacji technicznej. Oprogramowanie musi być zainstalowane na maszynie wirtualnej. 2. Konfigurując nowy system kopii zapasowych Zamawiającego należy pamięta, by do jego budowy wykorzystać obecnie używaną bibliotekę taśmową oraz dostarczony deduplikator z punktu 2 tej specyfikacji technicznej. Należy wykonać niezbędne prace instalacyjne, przyłączeniowe, konfiguracyjne, które pozwolą na współpracę wymienionych wyżej urządzeń z dostarczonym oprogramowaniem. 3. Przed przystąpieniem do konfiguracji i modernizacji systemu kopii Zamawiającego, należy przygotować plan modernizacji i go przedstawić do akceptacji. 4. Należy przenieść lub odwzorować całą obecną konfigurację sytemu backupu jaką posiada Zamawiający, wraz z wszystkimi harmonogramami wykonywania kopi zapasowych oraz kopiowaniem backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592) na bibliotekę taśmową Zamawiającego. 5. Należy rozszerzyć konfigurację sytemu kopii zapasowych (dostarczonego oprogramowania) poprzez wykorzystanie dodatkowych 10 licencji, o wskazane przez Zamawiającego zasoby, które dotychczas nie były objęte systemem backupu.

		6. Należy przygotować plany odzyskiwania i ich automatyzację dla minimum 10 maszyn wirtualnych, pracujących w środowisku wirtualizacyjnym (składającym się z trzech serwerów wirtualizacyjnych) lub 10 serwerów fizycznych, każdy z własną instancją systemu operacyjnego. 7. Konfiguracja oprogramowania musi obejmować tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Cloud oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Docelową chmurę Zamawiający wskaże na etapie realizacji wdrożenia. 8. Istotnym elementem konfiguracji systemu będzie skonfigurowanie przez Wykonawcę niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu oraz wszelki innych mechanizmów o ile takie posiadać będzie dostarczone oprogramowanie, których zadaniem jest ochrona przed ransomware. 9. Po zakończeniu wdrożenia należy przekazać Zamawiającemu kopię pliku konfiguracyjnego oprogramowania, który pozwoli w razie awarii oprogramowania i konieczności jego ponownej instalacji na szybkie przywrócenie całej konfiguracji systemu kopii.
11.	Szkolenie	1. Po zakończeniu wdrożenia nowego oprogramowania i modernizacji systemu kopii Zamawiającego, należy przeszkolić wskazane osoby w jego eksploatacji. 2. Szkolenie musi liczyć co najmniej 12 godz. i być podzielone na minimum dwie części oraz odbywać się w dogodnych dla obydwu stron terminach ustalonych z Zamawiającym. 3. Szkolenie musi się odbyć w siedzibie Zamawiającego na zmodernizowanym systemie kopii i uwzględniać wszystkie niezbędne czynności pozwalające na jego codzienną eksploatację.