**Załącznik nr 1**

OPIS PRZEDMIOTU ZAMÓWIENIA

## Rozszerzenie i podniesienie poziomu funkcjonalnego platformy do zarządzania kopiami zapasowymi wraz ze zwiększeniem licencji do 6 rdzeni.

|  |
| --- |
| ***Obecnie posiadana wersja:***  License: **Veeam Data Platform — Essentials Edition** |
|  |
| Quantity: **4 Sockets** |
| Support Expiration Date: **August 10, 2026** |

***Wersja wymagana:***

**Veeam Data Platform Foudation Enterprise,** licencja na **6 corów**, okres licencjonowania na cały okres trwałości projektu tj. na 36 miesięcy.

Wymagania stawiane zaproponowanemu rozwiązaniu:

|  |
| --- |
| **Wymagania ogólne** |
| 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 Peer Insights: i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5, |
| Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019, 2022 i 2025. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej |
| Oprogramowanie musi współpracować z infrastrukturą Nutanix w wersji 6.5.x - 7.0, Red Hat Virtualization 4.4 SP1, Oracle Linux Virtualization 4.5.4 lub nowszy oraz Proxmox VE 8.2 lub nowszy. |
| 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. |
| **Całkowite koszty posiadania** |
| Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej |
| Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków |
| 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 |
| 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. |
| Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla conajmniej trzech pamięci masowych to takiej puli. |
| Oprogramowanie musi pozwalać na przechowywanie kopii bezpieczeństwa w chmurze producenta. |
| 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. |
| Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu. |
| Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania |
| 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) |
| Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu |
| Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API |
| Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji |
| 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 |
| Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania |
| Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych. |
| Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej |
| Oprogramowanie musi wymagać autoryzacji dwuch administratorów backupu do wykonania krytycznych operacji (np skasowanie backupu, dodanie kolejnego administratora) |
| Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji. |
| **Wymagania RPO** |
| Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej |
| Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych. |
| Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna conajmniej dla platformy VMware i Hyper-V |
| 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. |
| Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware. |
| Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592). |
| Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) |
| Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard. |
| 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. |
| Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN. |
| 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. |
| 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. |
| Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik |
| Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding) |
| Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN) |
| **Wymagania RTO** |
| 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. |
| 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) |
| 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 |
| Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre |
| Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne. |
| Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków |
| Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform. |
| 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 |
| 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. |
| Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell |
| Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM |
| Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej. |
| 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. |
| Oprogramowanie musi pozwalać na backup i odtwarzanie usługi Entra ID. W szczególności użytkowników, grupy, role, jednostki administracyjne, entrprise applications. |
| 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. |
| 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. |
| 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. |
| 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. |
| 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. |
| Oprogramowanie musi wspierać granularne odtwarzanie baz danych MongoDB. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux. |
| Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji |
| Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN |
| Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle |
| Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI |
| Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2 |
| Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN |
| **Ograniczenie ryzyka** |
| 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) |
| Dla VMware’a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych |
| 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 |
| 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. |
| Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware |
| Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania |
| Oprogramowanie, bazując na wyuczonynym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków |
| Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego. |
| **Środowiska fizyczne** |
| Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego |
| Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych |
| Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE, Rocky Linux, AlmaLinux |
| Rozwiązanie musi wspierać system operacyjny macOS |
| Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix |
| Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą) |
| Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster |
| 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 |
| Rozwiązanie musi wspierać backup podłączonych dysków USB |
| Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym |
| 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) |
| Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone |
| Rozwiązanie musi wspierać kontrolę pasma sieciowego |
| Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych |
| Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN |
| Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft |
| Rozwiązanie musi wspierać technologię BitLocker |
| Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania |
| 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 |
| Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych |
| Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle I PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu. |
| 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 |
| Rozwiązanie musi wspierać szyfrowanie |
| Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne |
| Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego |
| Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej |
| Rozwiązanie musi wspierać tworzenie wielu zadań backupowych |

## Wznowienie licencji na już posiadane oprogramowanie do wirtualizacji.

Posiadana licencja na: **VMware vSphere 8 Essentials Plus Kit for 3 hosts (Max 2 processors per host)**

**Licencja ma być na okres 24 miesięcy.**

**Szczegóły posiadanych licencji:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Service** | **Covered Item** | **Qty** | **End Date** |
| Basic Support/Subscription for VMware vSphere 8 Essentials Plus Kit for 3 hosts (Max 2 processors per host) for 1 year | VMware vSphere 8 Essentials Plus for 1 processor | 6 | 10-AUG-2026 |
| Basic Support/Subscription for VMware vSphere 8 Essentials Plus Kit for 3 hosts (Max 2 processors per host) for 1 year | VMware vSphere 8 Essentials Plus Kit for 3 hosts (Max 2 processors per host) | 1 | 10-AUG-2026 |
| Basic Support/Subscription for VMware vSphere 8 Essentials Plus Kit for 3 hosts (Max 2 processors per host) for 1 year | VMware vCenter Server 8 Essentials for vSphere 8 | 1 | 10-AUG-2026 |

Zamawiający dopuszcza zaofertowanie wyższej wersji niż obecnie posiadana

Obecne licencje obowiązują do: **10.08.2026**

**Specyfikacja techniczna minimalna**

1. Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych.
2. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
3. Pojedynczy fizyczny procesor wymaga przypisania do niego licencji w ilości zgodnej z liczbą fizycznych rdzeni, jednak nie mniejszej niż 16 licencji na rdzenie.
4. Licencja na konsolę do zarządzania środowiskiem wirtualnym musi być zawarta w licencji na oferowany wirtualizator. Ilość licencji na konsolę zarządzającą do rozwiązania determinuje sumaryczna ilość posiadanych licencji na rdzenie fizycznych procesorów.
5. Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości 62 TB.
6. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia 24 TB pamięci operacyjnej RAM.
7. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych.
8. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe.
9. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 20 portów USB.
10. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 4 GB pamięci graficznej.
11. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
12. Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
13. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows 7/8/10/11, Windows Server, Amazon Linux 2, macOS, OS X, Asianux, Ubuntu, CentOS, NeoKylin, Debian, FreeBSD, Oracle Linux, RHEL, SUSE, Photon OS.
14. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
15. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
16. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.
17. System musi posiadać funkcjonalność wirtualnego przełącznika sieciowego umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów.
18. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.
19. Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN).
20. Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade). Wsparcie techniczne musi być świadczone bezpośrednio przez producenta oprogramowania. Licencjonowanie nie może odbywać się w trybie OEM.
21. Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, w szczególności Microsoft Active Directory, Open LDAP.
22. Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej.
23. Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych pomiędzy różnymi systemami pamięci masowych.
24. Rozwiązanie musi zawierać funkcjonalność pozwalającą na ominięcie testów inicjalizacyjnych sprzętu fizycznego w celu szybkiego startu wirtualizatora.
25. Rozwiązanie musi zawierać możliwość zabezpieczania maszyn wirtualnych przez rozwiązania antywirusowe firm trzecich bez konieczności instalacji agenta wewnątrz maszyny wirtualnej.
26. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy, bez jakiegokolwiek przestoju i bez utraty danych, pomiędzy serwerami fizycznymi, niezależnie od dostępności współdzielonej przestrzeni dyskowej,
27. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy, bez jakiegokolwiek przestoju i bez utraty danych, pomiędzy zasobami dyskowymi, niezależnie od dostępności współdzielonej przestrzeni dyskowej,
28. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy, bez jakiegokolwiek przestoju i bez utraty danych, jednocześnie między serwerami fizycznymi oraz zasobami dyskowymi, niezależnie od dostępności współdzielonej przestrzeni dyskowej.
29. Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA), aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym. Rozwiązanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci.
30. Rozwiązanie musi zapewniać wsparcie dla wirtualizacji zagnieżdżonej, w szczególności w zakresie możliwości zastosowania wszystkich funkcjonalności w tym Hyper-V systemu Windows Server na maszynie wirtualnej.
31. Rozwiązanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej.
32. Oprogramowanie do wirtualizacji musi zapewniać mechanizm takiego zabezpieczenia wybranych przez administratora wirtualnych maszyn, aby w przypadku awarii lub niedostępności serwera fizycznego maszyny, które na nim pracowały, były bezprzerwowo dostępne na innym serwerze z zainstalowanym oprogramowaniem wirtualizacyjnym. Mechanizm ten umożliwia zabezpieczenie maszyn wirtualnych wyposażonych w minimum 2 wirtualne procesory / 8 wirtualnych procesorów.
33. Rozwiązanie musi umożliwiać automatyczne równoważenie obciążenia CPU/MEM serwerów fizycznych pracujących jako platforma dla infrastruktury wirtualnej.
34. Rozwiązanie musi mieć możliwość oszczędzania energii elektrycznej poprzez automatyczne wyłączenie wskazanych serwerów fizycznych w przypadku braku obciążenia generowanego przez wirtualne maszyny i automatycznego ich włączenia w sytuacji wzrostu obciążenia.
35. Rozwiązanie musi mieć możliwość automatycznego równoważenia obciążenia fizycznych zasobów dyskowych poprzez przenoszenie zwirtualizowanych dysków pracujących maszyn wirtualnych pomiędzy fizycznymi zasobami dyskowymi.
36. Oprogramowanie do wirtualizacji musi zapewniać mechanizm pozwalający tworzyć profil (szablon konfiguracji) wybranego serwera a następnie instalować ten profil/konfigurację na innych serwerach lub sprawdzać zgodność konfiguracji pomiędzy zdefiniowanym wcześniej profilem a wskazanym serwerem fizycznym.
37. Rozwiązanie musi mieć możliwość uruchamiania fizycznych serwerów wchodzących w skład infrastruktury z obrazu udostępnionego poprzez protokół PXE.
38. Rozwiązanie musi umożliwiać szyfrowanie danych oraz dysków wirtualnych maszyn.
39. Rozwiązanie natywnie wspiera technologię Nvidia vGPU.
40. Rozwiązanie musi umożliwiać utworzenie jednorodnego, wirtualnego przełącznika sieciowego, rozproszonego na wszystkie serwery fizyczne platformy wirtualizacyjnej.
41. Rozwiązanie musi wspierać technologię, która umożliwia offloading funkcji sieciowych i bezpieczeństwa z hosta wirtualizacyjnego na specjalizowaną kartę DPU.

## Wznowienie licencji UTM.

1. Przedmiotem zamówienia jest wznowienie licencji na urządzenia:

* **FortiGate 100F - FG100FTK22005509**
* **FortiGate 100F - FG100FTK22005546**
* **FortiGate 40F - FGT40FTK22099WYW**

używane w infrastrukturze Zamawiającego.

1. Wznowienie licencji obejmuje następujące moduły zabezpieczeń, zapewniające pełną ochronę urządzeń do końca trwania projektu, tj. 36 miesięcy:

* Kontrola Aplikacji,
* IPS,
* Antywirus z aktualizacjami sygnatur obejmującymi ochronę urządzeń mobilnych, co najmniej dla systemu operacyjnego Android
* Analiza typu sandbox realizowana w chmurze,
* Antyspam,
* Web Filtering,
* Bazy refutacyjne adresów IP i domen

Licencje muszą zapewniać nieprzerwaną aktualizację baz sygnatur i definicji zagrożeń dla wszystkich w/w funkcji przez cały okres obowiązywania licencji.

Okres obowiązywania obecnych licencji: 2026-01-31

## Wznowienie licencji systemu bezpieczeństwa poczty elektronicznej.

1. Przedmiotem zamówienia jest wznowienie licencji na:

* **FortiMail 200F - FE200FT921000699 (1 szt.),**

używane w infrastrukturze Zamawiającego.

1. Wznowienie licencji obejmuje następujące moduły zabezpieczeń, zapewniające pełną ochronę urządzeń do końca trwania projektu, tj. 36 miesięcy:
2. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta  i serwisów przez cały okres obowiązywania licencji. Powinny one obejmować:

* kontrola Antyspam,
* Filtrowanie URL,
* kontrola antywirusowa,
* ochrona typu Virus Outbrake,
* Sandbox w chmurze,
* ochrona typu Click Protect,
* Content Disarm & Reconstruction,
* Business Email Compromise

Okres obowiązywania obecnej licencji: 2026-01-31