**Załącznik nr 7**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

1. **Informacje ogólne. Cel zamówienia.**
2. Celem zamówienia jest zwiększenie poziomu cyberbezpieczeństwa ww. podmiotów poprzez wzmocnienie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informatycznych. Celem jest wdrożenia mechanizmów i środków zwiększających odporność na ataki z cyberprzestrzeni.
3. W wyniku podjętych działań przyczyniających się do sprawnego i bezpiecznego działania systemów informatycznych, podniesie się poziom cyberbezpieczeństwa.
4. W celu wzmocnienia odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informatycznych konieczny jest zakup sprzętu, oprogramowania i usług informatycznych w obszarze cyberbezpieczeństwa jako kompleksowego i efektywnego rozwiązania.
5. Skutkiem realizacji będzie skuteczne zabezpieczenie systemów informatycznych przed cyberprzestępczością w kontekście: ochrony danych osobowych (RODO), potencjalnej utraty danych, ujawnienia wrażliwych danych osobom nieuprawnionym albo umożliwienia atakującym zniszczenia dokumentów lub danych, co zapewni ciągłość pracy oraz zwiększy poczucie bezpieczeństwa.
6. Przedmiot zamówienia będzie realizowany w ramach projektu konkursu grantowego pn. „Cyberbezpieczny Samorząd” realizowanego z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa, Priorytet II: Zaawansowane usługi cyfrowe (dalej: konkurs „Cyberbezpieczny Samorząd”).
7. **Szczegółowy opis przedmiotu zamówienia.**
8. **Zadanie nr 1:**
9. Przedmiotem niniejszego postępowania jest
   1. Dostawa dwóch serwerów typu Rack oraz macierzy dyskowej zgodnie z **załącznikiem 1**
   2. Dostawa serwera typu Rack zgodnie z **załącznikiem 2**
   3. Dostawa urządzenia deduplikującego zgodnie z **załącznikiem 3**
   4. Instalacji środowiska wirtualnego wraz z usługą migracji obecnego środowiska na nowo dostarczane serwery zgodnie z pkt 1.1
   5. Instalacja i konfiguracja systemu backupu na dostarczanym serwerze z pkt 1.3 wraz z konfiguracją urządzenia deduplikującego z punktu 1.3 jako medium.
   6. Dostawa licencji
      1. Licencje dostępowe do serwera CAL dla 75 użytkowników 2019/2022
      2. Licencje Windows Server 2022 powalające na uruchomienie min 6 maszyn wirtualnych w ramach wdrażanego rozwiązania, pozwalające na swobodną migrację maszyn wirtualnych pomiędzy węzłami klastra lub równoważne.
      3. Licencje oprogramowania systemu backupu umożliwiające backup min. 10 maszyn wirtualnych na okres do końca czerwca 2026r. zgodnie z **załącznikiem 4**
10. Realizacja prac wdrożeniowych godnie z poniższym opisem

**Planowany zakres prac wdrożeniowych w kolejności wykonania**

W ramach prac wdrożeniowych przeprowadzone zostaną następujące czynności:

* Projekt przedwdrożeniowy:
  + Analiza przedwdrożeniowa poprzedzona audytem
  + Szczegółowa architektura wdrożenia
  + Dokumentacja projektowa
* Akceptacja Zamawiającego + naniesienie ewentualnych zmian
* Instalacja w szafie RACK dostarczonego w ramach postępowania sprzętu zgodnie z projektem przedwdrożeniowym
* Okablowanie oraz konfiguracja dostarczonego sprzętu zgodnie z projektem przedwdrożeniowym
* Przygotowanie środowiska wirtualnego zgodnie z dokumentacją projektową:
  + Instalacja systemów operacyjnych wirtualizatora, konfiguracja klastra HA.
  + Testy poprawności konfiguracji klastra HA
  + Konfiguracja zasobów macierzy dyskowej i udostępnienie zasobów dla klastra HA
  + Przygotowanie scenariusza migracji
* Migracja środowiska wirtualnego
  + Realizacja scenariusza migracji poprzez:

- Migracja wirtualnych maszyn z obecnych serwerów Zamawiającego na nowe serwery klastra HA

* + Weryfikacja poprawności migracji
  + Migracja maszyn powinna zostać wykonana w taki sposób, aby nie miało to wpływu na funkcjonowanie środowiska zamawiającego. Zamawiający przewiduje możliwość migracji poza godzinami pracy urzędu
* Wdrożenie systemu backupu:
  + Instalacja i konfiguracja oprogramowania systemu kopii zapasowej zgodnie z przygotowanym projektem
  + Konfiguracja urządzenia deduplikującego wraz z udostępnieniem zasobów medium backupowego dla systemu kopii zapasowej
  + Utworzenie polityk kopii zapasowej zgodnie z przygotowanym projektem
  + Wdrożenie polityki chroniącej zasoby medium kopii zapasowej przed przypadkowym lub celowym usunięciem danych z medium backupowego przez ustalony w projekcie okres czasu, implementacja funkcji WORM
  + Przeprowadzenie testów wykonywania kopii zapasowej oraz poprawności odtwarzania danych dla wskazanych przez zamawiającego systemów
  + Przeprowadzenie testów bezpieczeństwa poprzez próbę usunięcia danych, potwierdzających zabezpieczenie systemu kopii zapasowej przed skasowaniem lub zmodyfikowaniem. Weryfikacja poprawności implementacji funkcji WORM,
* Implementacja i uruchomienie systemu monitoringu oraz alertowania dla wdrożonego środowiska wirtualnego oraz systemu kopii zapasowej a w szczególności:
* Konfiguracja monitoringu poprawności wykonywania zadań kopii zapasowej wraz z konfiguracją alertów
* Konfiguracja monitoringu zajętości medium backupowego wraz konfiguracją alertów
* Konfiguracja monitorowania systemu backupu pod kątem analityki entropii w celu wczesnego wykrycia oprogramowania złośliwego typu Ransomware wraz z konfiguracją alertów
* Konfiguracja monitoringu zasobów środowiska wirtualnego pod kątem wydajności oraz zajętości wraz z konfiguracją alertów
* Dokumentacja powdrożeniowa zwierająca szczegółowy opis wdrażanych komponentów środowiska wraz ze schematem połączeń.
* Końcowy odbiór prac przez Zamawiającego.

Na potwierdzenie wykonania konfiguracji zostaną wykonane testy potwierdzające zgodność dostarczonych komponentów z wymaganiami Zamawiającego (Opisem Przedmiotu Zamówienia).

**Załącznik 1**

Poniżej przedstawiono parametry minimalne dla serwera:

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Obudowa** | * Obudowa Rack o wysokości max 2U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. * Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. * Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android lubApple iOS) przy użyciu jednego z protokołów BLE/ WIFI. |
| **Płyta główna** | * Płyta główna z możliwością zainstalowania do dwóch procesorów. * Obsługa procesorów 32 rdzeniowych. * Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. * Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. * Płyta główna powinna obsługiwać do 1TB pamięci RAM. |
| **Chipset** | * Dedykowany przez producenta procesor do pracy w serwerach dwuprocesorowych |
| **Procesor** | * Min. Jeden procesor min. 16-rdzeni klasy x86, min. 2 GHz, dedykowane do pracy z oferowanym serwerem umożliwiające osiągnięcie wyniku min. 270 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. |
| **RAM** | * Minimum 128GB DDR5 RDIMM 5600MT/s, |
| **Gniazda PCI** | * Min. dwa sloty PCIe |
| **Interfejsy sieciowe/FC/SAS** | * Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 4 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT (Dodatkowa, dwuportowa karta 10/25GBe SFP28 wraz z wkładkami SFP+ 10GbE Czteroportowa, karta SAS HBA 12Gb |
| **Dyski twarde** | * Zainstalowane dwa dyski M.2 NVME o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. |
| **Wbudowane porty** | * 4x USB, w tym min. 1 porty USB 3.0 * 1 x USB-C * 2x port VGA (jeden na panelu przednim) * Możliwość rozbudowy o Serial Port lub wsparcie portu do zarządzania 1Gb/s Ethernet z obsługą Serial-over-LAN. |
| **Video** | * Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024 |
| **Wentylatory** | * Redundantne, Hot-Plug |
| **Zasilacze** | * Redundantne, Hot-Plug min. 1100W klasy Titanium |
| **Bezpieczeństwo** | * Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. * Moduł TPM 2.0 * Możliwość włączania i wyłączania portów USB na obudowie * Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem |
| **Karta Zarządzania** | * Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:   + zdalny dostęp do graficznego interfejsu Web karty zarządzającej;   + zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);   + szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;   + możliwość podmontowania zdalnych wirtualnych napędów;   + wirtualną konsolę z dostępem do myszy, klawiatury;   + wsparcie dla IPv6;   + wsparcie dla WSMAN (Web Service for Management) równoważnie Refish; SNMP; IPMI2.0, SSH;   + możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;   + możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;   + integracja z Active Directory;   + możliwość obsługi przez dwóch administratorów jednocześnie;   + wsparcie dla dynamic DNS;   + wysyłanie do administratora maila z powiadomieniem o awarii konfiguracji sprzętowej. |
| **Oprogramowanie do zarządzania** | * Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:   + Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych   + integracja z Active Directory   + Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta   + Wsparcie dla protokołów SNMP, IPMI, Linux SSH,   + Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram   + Szczegółowy opis wykrytych systemów oraz ich komponentów   + Możliwość eksportu raportu do CSV, HTML, XLS, PDF   + Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.   + Grupowanie urządzeń w oparciu o kryteria użytkownika   + Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji   + Szybki podgląd stanu środowiska   + Podsumowanie stanu dla każdego urządzenia   + Szczegółowy status urządzenia/elementu/komponentu   + Generowanie alertów przy zmianie stanu urządzenia.   + Filtry raportów umożliwiające podgląd najważniejszych zdarzeń   + Integracja z service desk producenta dostarczonej platformy sprzętowej   + Możliwość przejęcia zdalnego pulpitu   + Możliwość podmontowania wirtualnego napędu   + Kreator umożliwiający dostosowanie akcji dla wybranych alertów   + Możliwość importu plików MIB   + Przesyłanie alertów „as-is” do innych konsol firm trzecich   + Możliwość definiowania ról administratorów   + Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów   + Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta   + Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów   + Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, , aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.   + Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.   + Zdalne uruchamianie diagnostyki serwera.   LUB równoważnie:  Możliwość zainstalowania oprogramowania zarządzającego i diagnostycznego wyprodukowanego przez producenta serwera umożliwiające zdalne zarządzanie wszystkimi dostarczonymi serwerami jako grupą serwerów (klastrem), posiadające interfejs graficzny dostępny z poziomu przeglądarek internetowych (HTML), pozwalające m.in. na:  • włączenie, wyłączenie, restart, podgląd logów serwerów, sprawdzenie statusu sprzętu, przejęcie pełnej konsoli graficznej serwerów.  • tworzenie szablonów instalacyjnych dla systemów operacyjnych.  • tworzenie profili serwerów ze zdefiniowanymi parametrami BIOS, procesora/-ów, pamięci, kontrolera RAID które umożliwiają szybkie wdrożenie identycznej konfiguracji na grupie serwerów.  • zdalne montowanie obrazów ISO pozwalające na uruchomienie z nich serwera.  • aktualizacja sterowników i BIOS serwerów.  • zbieranie statystyk zużycia energii dla wszystkich serwerów z możliwością graficznej prezentacji danych historycznych. |
| **Certyfikaty** | * Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 lub równoważną **Wybrany w postępowaniu** **Wykonawca przedstawi dokument potwierdzający spełnienie wymogu przed zawarciem umowy.** * Serwer musi posiadać deklaracja CE - **Wybrany w postępowaniu** **Wykonawca przedstawi dokument potwierdzający spełnienie wymogu przed zawarciem umowy.** * 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 Dyrektywy WEEE 2002/96/EC. 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](http://www.epeat.net) potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku – **Wybrany w postępowaniu** **Wykonawca przedstawi dokument potwierdzający spełnienie wymogu przed zawarciem umowy.**   LUB Równoważnie do wyżej opisanego wymogu spełnienia normy co najmniej Epeat Silver, produkt musi posiadać deklarację RoHS – **Wybrany w postępowaniu** **Wykonawca przedstawi dokument potwierdzający spełnienie wymogu przed zawarciem umowy.** |
| **Dokumentacja użytkownika** | * Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim. * Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |
| **Warunki gwarancji** | * Zamawiający wymaga zapewnienia przez wykonawcę usługi wsparcia technicznego z zakresu wdrażanej technologii na okres do końca czerwca 2026 r. * Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. * Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy (dla krytycznych zgłoszeń serwisowych) * Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. * 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. * Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. * Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. * Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, * Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu przedłożenia oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. * Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające wykonawca będzie zobowiązany złożyć na każde żądanie Zamawiającego. |

**Macierz dyskowa**

|  |  |
| --- | --- |
| **Element konfiguracji/cecha/funkcjonalność** | **Wymagania minimalne** |
| Typ obudowy | Macierz musi być przystosowana do montażu w szafie rack 19”,  o wysokość maksymalnie 2U z możliwością instalacji min. 24 dysków 2.5” |
| Przestrzeń dyskowa | Zainstalowane:  10x dysk SAS o pojemności min. 2.4TB, Hot-Plug  4x dysk SSD SAS o pojemności min. 1.6TB, Hot-Plug |
| Możliwość rozbudowy | Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 276 dysków twardych. |
| Obsługa dysków | Macierz musi mieć możliwość obsługiwania dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD i SAS i w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5” jak również 3,5”. |
| Sposób zabezpieczenia danych | Macierz musi obsługiwać mechanizmy RAID zgodne z RAID1, , RAID5, RAID6 oraz  Macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku).  Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków. |
| Tryb pracy kontrolerów macierzowych | Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów. |
| Pamięć cache | Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM.  Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi.  Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat. |
| Rozbudowa pamięci cache | Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash lub równoważnie Pamięć cache (dot. wymogu powyżej) musi umożliwiać rozbudowę do 64 GB RAM.  Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem. |
| Interfejsy | Macierz musi posiadać, co najmniej 8 portów 12Gb SAS (4 porty na kontroler), + 4 porty 10GbE iSCSI |
| Kable/wkładki | 4x kabel 12Gb HD Mini-SAS/HD Mini-SAS min. 2m |
| Zarządzanie | Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej. |
| Zarządzanie grupami dyskowymi oraz dyskami logicznymi | Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej.  Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy.  Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| Thin Provisioning | Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning.  Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP).  Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| Tiering | Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS.  Tiering musi obejmować wszystkie woluminy w danej puli dyskowej. |
| Wewnętrzne kopie migawkowe | Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii.  Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| Wewnętrzne kopie pełne | Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych.  Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| Podłączanie zewnętrznych systemów operacyjnych | Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami).  Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, Vmware, Citrix.  Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych.  Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie. |
| Redundancja | Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów.  Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory.  Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.  Zasilacze użyte w macierzy powinny spełniać wymagania dotyczące sprawności dla zasilacza minimum 80+ Gold. |
| Dodatkowe wymagania | Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych.  Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie.  Oferowany system dyskowy musi mieć możliwość kompresji i deduplikacji danych. Licencja na tą funkcjonalność musi być zawarta w cenie i musi obejmować zaoferowaną w ramach macierzy przestrzeń dyskową.  Oferowany system dyskowy musi mieć możliwość uruchomienia funkcjonalności szyfrowania danych na poziomie kontrolerów macierzowych. Jeśli na obsługę powyższej funkcjonalności wymagana jest dodatkowa licencja, nie jest ona wymagana w tym postępowaniu |
| Standardy bezpieczeństwa | Urządzenie musi spełniać następujące standardy bezpieczeństwa: EN 62368-1 (European Union), IEC 60950-1 (International) lub równoważnie macierz musi umożliwiać tworzenie wg ustalonego harmonogramu odpornych na zagrożenia cybernetyczne kopii wolumenów, których nie można zmienić ani usunąć w wyniku błędów użytkownika, złośliwych działań lub ataków oprogramowania ransomware. |
| Inne | Urządzenia muszą być zakupione w legalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z legalnego kanału dystrybucyjnego producenta.  Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001 lub równoważne.  Deklaracja zgodności CE. **Wybrany w postępowaniu** **Wykonawca przedstawi dokument potwierdzający spełnienie wymogu przed zawarciem umowy.** |
| Warunki gwarancji | Zamawiający wymaga zapewnienia przez wykonawcę usługi wsparcia technicznego z zakresu wdrażanej technologii na okres do końca czerwca 2026 r.  Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet . Możliwości zgłaszania zdarzeń serwisowych i komunikacji z serwisem producenta w języku polskim.  Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy (dla krytycznych zgłoszeń serwisowych)  Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania.  Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.  Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.  Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.  Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego  Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu przedłożenie oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.  Serwis powinien być świadczony przez producenta sprzętu lub autoryzowaną firmę serwisującą Producenta. W przypadku autoryzowanej przez producenta firmy serwisującej, taka firma musi posiadać ISO 9001:2015 oraz ISO-27001 lub równoważne na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające wykonawca złoży na każde żądanie Zamawiającego. |

**Załącznik 2**

**Serwer backupu**

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Obudowa** | * Obudowa Rack o wysokości max 2U z możliwością instalacji min. 8 dysków 2.5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. * Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, |
| **Płyta główna** | * Płyta główna z możliwością zainstalowania do dwóch procesorów. * Obsługa procesorów 32 rdzeniowych. * Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. * Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. * Płyta główna powinna obsługiwać do 1TB pamięci RAM. |
| **Chipset** | * Dedykowany przez producenta procesor do pracy w serwerach dwuprocesorowych. |
| **Procesor** | * Min. Jeden procesor 8-rdzeniowy, min. 2.6GHz, umożliwiający osiągnięcie wyniku min. 169 w teście SPECrate2017\_int\_base, dla oferowanego serwera, dostępnym na stronie www.spec.org w konfiguracji dwuprocesorowej |
| **RAM** | * Minimum 64GB DDR5 RDIMM 4800MT/s, |
| **Interfejsy sieciowe/FC/SAS** | * Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT |
| **Dyski twarde** | * Zainstalowane   + 4x dysk SAS o pojemności min. 1.2TB, 12Gb, 2,5“ Hot-Plug. * Zainstalowane dwa dyski M.2 NVMe SSDs o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1. |
| **Kontroler RAID** | * Sprzętowy kontroler dyskowy, posiadający   + Min. 8GB nieulotnej pamięci cache,   + Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.   + Wsparcie dla dysków samoszyfrujących |
| **Wbudowane porty** | * 4 x USB z czego nie mniej niż 1x USB 3.0, * 1 x VGA |
| **Video** | * Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200 |
| **Zasilacze** | * Redundantne, Hot-Plug min. 1100W klasy Titanium |
| **Bezpieczeństwo** | * Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. * Moduł TPM 2.0 * Możliwość włączania I wyłączania portów USB na obudowie * Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem |
| **Karta Zarządzania** | * Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:   + zdalny dostęp do graficznego interfejsu Web karty zarządzającej;   + zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);   + szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;   + możliwość podmontowania zdalnych wirtualnych napędów;   + wirtualną konsolę z dostępem do myszy, klawiatury;   + wsparcie dla IPv6;   + wsparcie dla WSMAN (Web Service for Management) lub równoważnie Refish; SNMP; IPMI2.0, SSH;   + możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;   + możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;   + integracja z Active Directory;   + możliwość obsługi przez dwóch administratorów jednocześnie;   + wsparcie dla dynamic DNS;   + wysyłanie do administratora maila z powiadomieniem o awarii |
| **Oprogramowanie do zarządzania** | * Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:   + Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych   + integracja z Active Directory   + Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta   + Wsparcie dla protokołów SNMP, IPMI, Linux SSH,   + Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram   + Szczegółowy opis wykrytych systemów oraz ich komponentów   + Możliwość eksportu raportu do CSV, HTML, XLS, PDF   + Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.   + Grupowanie urządzeń w oparciu o kryteria użytkownika   + Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji   + Szybki podgląd stanu środowiska   + Podsumowanie stanu dla każdego urządzenia   + Szczegółowy status urządzenia/elementu/komponentu   + Generowanie alertów przy zmianie stanu urządzenia.   + Filtry raportów umożliwiające podgląd najważniejszych zdarzeń   + Integracja z service desk producenta dostarczonej platformy sprzętowej   + Możliwość przejęcia zdalnego pulpitu   + Możliwość podmontowania wirtualnego napędu   + Kreator umożliwiający dostosowanie akcji dla wybranych alertów   + Możliwość importu plików MIB   + Przesyłanie alertów „as-is” do innych konsol firm trzecich   + Możliwość definiowania ról administratorów   + Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów   + Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta   + Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów   + Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, , aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.   + Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.   + Zdalne uruchamianie diagnostyki serwera.   LUB równoważnie:  Możliwość zainstalowania oprogramowania zarządzającego i diagnostycznego wyprodukowanego przez producenta serwera umożliwiające zdalne zarządzanie wszystkimi dostarczonymi serwerami jako grupą serwerów (klastrem), posiadające interfejs graficzny dostępny z poziomu przeglądarek internetowych (HTML), pozwalające m.in. na:  • włączenie, wyłączenie, restart, podgląd logów serwerów, sprawdzenie statusu sprzętu, przejęcie pełnej konsoli graficznej serwerów.  • tworzenie szablonów instalacyjnych dla systemów operacyjnych.  • tworzenie profili serwerów ze zdefiniowanymi parametrami BIOS, procesora/-ów, pamięci, kontrolera RAID które umożliwiają szybkie wdrożenie identycznej konfiguracji na grupie serwerów.  • zdalne montowanie obrazów ISO pozwalające na uruchomienie z nich serwera.  • aktualizacja sterowników i BIOS serwerów.  • zbieranie statystyk zużycia energii dla wszystkich serwerów z możliwością graficznej prezentacji danych historycznych. |
| **Certyfikaty** | * Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 lub równoważne - Wykonawca przedstawi dokument potwierdzający spełnienie wymogu. * Serwer musi posiadać deklaracja CE - Wykonawca przedstawi dokument potwierdzający spełnienie wymogu. * 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 Dyrektywy WEEE 2002/96/EC. 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](http://www.epeat.net) potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku – Wykonawca przedstawi dokument potwierdzający spełnienie wymogu.   LUB Równoważnie do wyżej opisanego wymogu spełnienia normy co najmniej Epeat Silver, produkt musi posiadać deklarację RoHS - Wykonawca przedstawi dokument potwierdzający spełnienie wymogu. |
| **Dokumentacja użytkownika** | * Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim. * Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |
| **Warunki gwarancji** | * Zamawiający wymaga zapewnienia przez wykonawcę usługi wsparcia technicznego z zakresu wdrażanej technologii na okres do końca czerwca 2026 r. * Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. * Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy (dla krytycznych zgłoszeń serwisowych) * Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. * 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. * Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. * Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. * Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, * Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu przedłożenie oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. * Firma serwisująca musi posiadać ISO 9001:2015 oraz na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające Wykonawca będzie zobowiązany przedłożyć na każde żądanie Zamawiającego. |

**Załącznik 3**

**Deduplikator, wymagania szczegółowe**

|  |  |
| --- | --- |
| Lp. | Parametr wymagany |
|  | Urządzenie musi być przeznaczone do deduplikacji i przechowywania kopii zapasowych. Urządzenie musi spełniać wymagania wyspecyfikowane w niniejszej tabeli. |
|  | Dostarczone urządzenie musi oferować przestrzeń min. 8TB netto (powierzchni użytkowej) bez uwzględniania mechanizmów protekcji.  Urządzenie musi posiadać dwa kontrolery pracujące w trybie active-active lub active-pasive. Awaria pojedynczego kontrolera nie może powodować braku dostępu do danych backupowych. |
|  | Dostarczone urządzenie powinno umożliwiać rozbudowę o warstwę typu CLOUD dedykowaną do długotrwałego przechowywania danych (tzw. Long Term Retention) – dane o określonej retencji (zgodnie z założoną polityka retencyjną), bez pośrednictwa dodatkowych urządzeń (typu GATEWAY) powinny zostać przemigrowane (w postaci zdeduplikowanej) na dodatkową warstwę, wymagane wsparcie dla AWS oraz Microsoft Azure. Wymagana enkrypcja danych przechowywanych na warstwie typu Cloud. Wymagane dostarczenie licencji na przestrzeń min. 60TB netto dla warstwy CLOUD. Wymagana funkcjonalność powinna wspierać aplikację Veeam Backup and Replication oraz NetWorker.  Jako równoważne Zamawiający dopuszcza możliwość konfiguracji w przyszłości drugiego identycznego urządzenia z możliwością konfiguracji migracji danych w celu 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). |
|  | Oferowane urządzenie musi posiadać minimum   * 4 porty Eth 10 Gb/s Eth BaseT lub SFP+   wymagana możliwość obsługi każdym z w/w portów protokołów CIFS, NFS, deduplikacja na źródle  oraz   * 2 porty FC 16Gb/s   wymagana obsada wszystkich portów wkładkami, wymagana możliwość obsługi poprzez porty FC protokołów deduplikacja na źródle. |
|  | Oferowane urządzenie musi umożliwiać jednoczesny dostęp wszystkimi poniższymi protokołami:   * CIFS, NFS * zapewniającym deduplikację na źródle, |
|  | Wymagane jest dostarczenie licencji, pozwalającej na jednoczesną obsługę protokołów CIFS, NFS, deduplikacja na źródle, do oferowanej pojemności urządzenia |
|  | Oferowane pojedyncze urządzenie musi osiągać zagregowaną wydajność (dla maksymalnej konfiguracji) protokołami: **NFS** co najmniej 6 TB/h (dane podawane przez producenta) oraz co najmniej 18 TB/h z wykorzystaniem **deduplikacji na źródle** (dane podawane przez producenta). |
|  | Urządzenie musi pozwalać na jednoczesną obsługę minimum 250 strumieni w tym jednocześnie:   * zapis danych minimum 150 strumieniami * odczyt danych minimum 50 strumieniami * replikacja minimum 50 strumieniami   pochodzących z różnych aplikacji oraz dowolnych protokołów (CIFS, NFS, deduplikacja na źródle) w tym samym czasie.  Wymienione wartości 250 jednoczesnych strumieni dla wszystkich protokołów (czyli jednocześnie 150 dla zapisu i jednocześnie 50 strumieni dla odczytu i jednocześnie 50 strumieni dla replikacji) musi mieścić w przedziale oficjalnie rekomendowanym i wspieranym przez producenta urządzenia.  Wszystkie zapisywane strumienie muszą podlegać globalnej deduplikacji przed zapisem na dysk (in-line) jak opisano w niniejszej specyfikacji. |
|  | 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. |
|  | Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku  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. |
|  | Oferowany produkt musi posiadać obsługę mechanizmów globalnej deduplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, VTL, deduplikacja na źródle) przechowywanych w obrębie całej zaoferowanej przestrzeni co oznacza, że przechowywany na urządzeniu fragment danych nie może być ponownie zapisany bez względu na to, jakim protokołem zostanie ponownie otrzymany. 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. |
|  | 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. |
|  | 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). |
|  | Wszystkie unikalne bloki przed zapisaniem na dysk muszą być dodatkowo kompresowane. |
|  | Oferowane urządzenie musi wspierać (co najmniej następujące aplikacje: Veeam Backup and Replication, , RMAN,  W przypadku współpracy z każdą z poniższych aplikacji:   * Veeam Backup and Replication   urządzenie musi umożliwiać deduplikację na źródle i przesłanie nowych, nie znajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN.  Deduplikacja w wyżej wymienionych przypadkach musi zapewniać, aby z zabezpieczanych serwerów do urządzenia były transmitowane poprzez sieć LAN jedynie fragmenty danych nie znajdujące się dotychczas na urządzeniu. |
|  |  |
|  | W przypadku systemów LINUX (min.: RedHat oraz SuSE) oraz Windows urządzenie powinno umożliwiać deduplikację na źródle na poziomie systemu plików. Dane kopiowane na wydzielony system plików (bez pośrednictwa aplikacji backupowej) powinny podlegać deduplikacji ew. licencje nie są przedmiotem tego postępowania. |
|  | Oferowane urządzenie powinno umożliwiać uruchamianie maszyn wirtualnych VMware bezpośrednio z danych backupowych bez konieczności odtwarzania danych, funkcjonalność ta powinna być wspierana przez Veeam Backup and Replication. |
|  | Wymagana funkcjonalność Load Balancing oraz Link Failover w obrębie portów wykorzystywanych przez aplikację backupową, wymagane wsparcie tej funkcjonlaności dla Veeam Backup and Replication. |
|  | Wymagane wsparcie dla backupów typu Virtual Synthetics w przypadku Veeam Backup and Replication. |
|  | W przypadku deduplikacji na źródle poprzez sieć IP (LAN oraz WAN), wymagana możliwość szyfrowania komunikacji kluczem minimum 256 bitów. |
|  | Urządzenie powinno umożliwiać zaszyfrowanie przechowywanych danych, wymagane licencje umożliwiające zaszyfrowanie i przechowywanie zaszyfrowanych danych w obrębie maksymalnej pojemności oferowanego urządzenia. |
|  | Urządzenie musi wspierać deduplikację na źródle poprzez sieć FC (SAN) minimum dla następujących systemów operacyjnych:   * Windows * Linux (RedHat, SuSE) |
|  | Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych do drugiego urządzenia takiego samego typu. Konfiguracja replikacji musi być możliwa w każdym z trybów:  \* jeden do jednego  \* wiele do jednego  \* jeden do wielu  \* kaskadowej (urządzenie A replikuje dane do urządzenia B, które te same dane replikuje do urządzenia C)  Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane mogą być tylko te fragmenty danych (bloki) które nie znajdują się na docelowym urządzeniu. |
|  | Urządzenie musi umożliwiać wydzielenie określonych portów Ethernet dedykowanych do replikacji. |
|  | W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami. |
|  | Wymagana możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami – oferowane urządzenie powinno być wyposażone w mechanizm umożliwiający zarządzaniem stopnia wykorzystania pasma na potrzeby replikacji. |
|  | Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6 bądź równoważnej. |
|  | Oferowane urządzenie musi umożliwiać wykonywanie SnapShot’ów, czyli umożliwiać zamrożenie obrazu danych (stanu backupów) w urządzeniu na określoną chwilę. Oferowane urządzenie musi również umożliwiać odtworzenie danych ze Snapshot’u.  Odtworzenie danych ze Snapshot’u nie może wymagać konieczności nadpisania danych produkcyjnych jak również nie może oznaczać przerwy w normalnej pracy urządzenia (przyjmowania/odtwarzania backupów). |
|  | 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. |
|  | 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). |
|  | 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. |
|  | 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. |
|  | Wymagana możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia jako niezależnego urządzenia dostępnego za pośrednictwem:   * CIFS * NFS * deduplikacja na źródle |
|  | Urządzenie musi umożliwiać zdefiniowanie blokady skasowania danych (funkcjonalność WORM). Blokada skasowania danych musi chronić plik w zdefiniowanym czasie przed usunięciem pliku, modyfikacją pliku.  Licencje na blokadę usunięcia/zmiany przechowywanych plików muszą być dostarczone wraz z urządzeniem. |
|  | Urządzenie musi mieć możliwość przechowywania danych niezmienialnych:   * Video * Grafika * Nagrania dźwiękowe * Pliki pdf na udziałach CIFS/NFS. |
|  | Urządzenie musi weryfikować wszystkie składowane dane po zapisie (nie chodzi o ew. weryfikację danych indeksowych generowanych przez urządzenie, ale o weryfikację wszystkich zabezpieczanych danych backup’owych). Każda zapisana na dyskach porcja danych musi być odczytana i porównana z danymi otrzymanymi przez urządzenie. Powyższa weryfikacja powinna być realizowana w locie, czyli przed usunięciem z pamięci oryginalnych danych (otrzymanych z aplikacji backupowej), musi być realizowana w trybie ciągłym (a nie ad-hoc), wymagane parametry wydajnościowe urządzenia muszą uwzględniać tę funkcjonalność. |
|  | Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia lub równoważnie niezwłocznie po upływie retencji z wykorzystaniem wewnętrznych mechanizmów czyszczenia |
|  | Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu). |
|  | Wymagana możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora), wymagane potwierdzenie w ogólno dostępnej dokumentacji. Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności). Równoważnie dopuszczalne jest rozwiązanie, w którym zasoby są tak zwymiarowane, że deklarowana wydajność zapisu/odczytu/ backupu/replikacji nie jest ograniczona w jakimkolwiek stopniu podczas procesów czyszczenia. |
|  | Wymagana możliwość zdefiniowania harmonogramu, wg. którego wykonywany jest proces usuwania przeterminowanych danych (czyszczenia), realizowany równolegle z procesami backup/restore/replication. Równoważnie dopuszczalne jest rozwiązanie lepsze, w którym zwalniana przestrzeń jest czyszczona niezwłocznie po jej zwolnieniu. |
|  | 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 (Równoważnie dopuszczalne jest rozwiązanie lepsze, w którym zwalniana przestrzeń jest czyszczona niezwłocznie po jej zwolnieniu. |
|  | Urządzenie musi mieć możliwość zarządzania poprzez   * Interfejs graficzny dostępny z przeglądarki internetowej * Poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell) |
|  | Oprogramowanie do zarządzania musi rezydować na oferowanym na urządzeniu deduplikacyjnym. |
|  | 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. |
|  | 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. |
|  | Oferowane urządzenie powinno być objęte wsparciem producenta obejmującego okres do końca czerwca 2026 r., działającym w trybie zgłaszania awarii: 24x7 oraz reakcji on-site w trybie NBD.  Zamawiający wymaga od podmiotu realizującego serwis lub producenta urządzenia złożenia oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. |

**Załącznik 4**

**Oprogramowanie do wykonywania kopii zapasowych**

**Ilość: 1 kpl**

|  |  |
| --- | --- |
|  | **Wymagane minimalne parametry techniczne** |
| **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: https://www.gartner.com/reviews/market/data-center-backup-and-recoverysolutions 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 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej.  Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS 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 nieograniczonej liczby pamięci masowych to takiej puli.  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. |
| **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 na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastoru.  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 lub równoważną.  Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy.  Oprogramowanie musi mieć możliwość tworzenia retencji GFS (GrandfatherFather-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 i Oracle 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 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 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 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 oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.  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 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.  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 i Oracle 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 |
| **Monitoring** | System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich.  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.  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.  System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter.  System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn.  System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel.  System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk.  System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora.  System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów.  System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard).  System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna.  System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego.  System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta.  System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.  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.  System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy Vmware |
| **Raportowanie** | 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.  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.  System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.  System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V. System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF.  System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc.  System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach.  System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów.  System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych. System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych.  System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury.  System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta.  System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.  System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’.  System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy Vmware.  System musi mieć możliwość generowania raportów dotyczących tzw. migaweksierot (orphaned snapshots).  System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie. |

**Szkolenie specjalistyczne**

Zamówienie obejmuje szkolenie z wdrażanych rozwiązań w ramach zamówienia

1. Zamawiający wymaga, aby Wykonawca zorganizował i przeprowadził szkolenie w siedzibie Zamawiającego.
2. Szkolenie ma obejmować dostarczane oprogramowania i urządzenia.
3. Warsztaty mają odbyć się w formie stacjonarnej, na terenie Polski.
4. Zamawiający wymaga, aby usługa została zrealizowana w terminie realizacji zamówienia po dostarczeniu i wdrożeniu urządzeń oraz oprogramowania. Dokładny termin zostanie ustalony zgodnie z procedurą przewidzianą we wzorcu umowy.
5. Zamawiający wymaga przeszkolenia w formie warsztatów 1 uczestnika, z tym, że ilość jest szacunkowa, co nie powinno wpływać na koszty.
6. Zamawiający wymaga, aby w trakcie warsztatów realizowane były ćwiczenia opisujące codzienną pracę administracyjną z wdrożonym rozwiązaniem, rozwiązywaniem problemów, procedurę aktualizacji rozwiązania oraz rozbudowy o dodatkowe widoki i kanały napływu danych.
7. Zamawiający wymaga, aby warsztaty zamykały się w ramach czasowych 2 dni roboczych (2x 7 godz.)
8. Zamawiający wymaga, aby warsztaty kończyły się potwierdzeniem uczestnictwa w formie certyfikatu potwierdzającego odbyte szkolenie.

**ZADADNIE NR 2**

|  |  |
| --- | --- |
| **Szczegółowy opis przedmiotu zamówienia** | |
|  | |
| Typ urządzenia | Serwer NAS |
| Obudowa | Rack |
| Procesor | Ośmiordzeniowy procesor o taktowaniu 2,1 GHz, maksymalnie 2,7 GHz z technologią Turbo Boost osiągający w teście PassMark na sierpień 2022 co najmniej 10 000 punktów - Wykonawca przedstawi dokument potwierdzający spełnienie wymogu. |
| Sprzętowy mechanizm szyfrowania | Tak (AES-NI) |
| Pamięć RAM | min. 16 GB pamięci ECC UDIMM z możliwością rozszerzenia do min. 64 GB |
| Zainstalowane dyski | **2 x SSD o parametrach:**  Pojemność min: 800 GB,  Typ: M.2, PCI Express 3.0 NVMe,  przeznaczenie: NAS,  Prędkość odczytu z nośnika min. 3100MB/s,  Prędkość zapisu nośnika min.: 1000 MB/s,  Losowy odczyt (4KB) min: 400000 IOPS,  Losowy zapis (4KB) min: 70000 IOPS,  Średni okres międzyawaryjny min. 1800000h,  Dysk musi być kompatybilny z zaoferowanym urządzeniem – lista zgodności.  **12 x dysk HDD o parametrach:**  Pojemność min. 12 TB,  szybkość min: 7200 RPM,  rozmiar bufora pamięci min.: 256 MB,  rozmiar: 3,5”,  Typ: SATA III,  Przeznaczenie: NAS,  Przepustowość interfejsu min.: 6Gb/s,  Średni czas do awarii min.: 2500000h  Dysk musi być kompatybilny z zaoferowanym urządzeniem – lista zgodności. |
| Możliwości rozbudowy | Sprzęt powinien być wyposażony w min. 12 kieszeni na dyski twarde 3,5 cala typu hot-swap z możliwością rozszerzenia do 36 dysków łącznie przy użyciu dodatkowych jednostek rozszerzających podłączanych do jednostki głównej |
| Porty zewnętrzne | Minimum:   * 2 porty USB 3.2.1 * 2 gniazda rozszerzenia |
| Porty sieciowe | Minimum:   * 2 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego) * 2 porty 10GbE RJ45 (wymogiem jest, aby dostarczane urządzenie posiadało wbudowane porty 10Gbe RJ-45 pozostawiając tym samym wolne gniazda rozszerzeń PCIe) |
| Funkcja Wake on LAN/WAN | Tak |
| Gniazdo rozszerzeń PCIe 3.0 | Min. 2x 8-liniowe gniazdo x8 lub równoważnie min. 3 (2 x Gen4 x4 +1 x Gen 4 x8) |
| Wentylator obudowy | Min. 4 wentylatory |
| Obsługiwane protokoły sieciowe | Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4,, NFS z autentykacją Kerberos, iSCSI, http, HTTPs, FTP, SNMP, LDAP, CalDAV |
| Obsługiwane systemy plików | Min.:   * Wewnętrzny: Btrfs lub ZFS, ext4 * Zewnętrzny: ext4, ext3, FAT32, NTFS, HFS+, exFAT |
| Zarządzanie pamięcią masową | * Maksymalny rozmiar pojedynczego wolumenu:   + 1 PB (wymagana pamięć 64 GB, tylko grupy RAID 6)   + 200 TB (wymagana pamięć 32 GB)   + 108 TB * Minimalny liczba wewnętrznych wolumenów: 256 * Minimalny liczba obiektów iSCSI Target: 256 * Minimalny liczba jednostek iSCSI LUN: 512 * Obsługa klonowania/migawek jednostek iSCSI LUN |
| Obsługiwane typy macierzy RAID | Podstawowy (Basic) lub Single, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, |
| Funkcja udostępniania plików | * Minimalna liczba lokalnych kont użytkowników:   4000 * Minimalna liczba lokalnych grup: 512 * Minimalna liczba folderów współdzielonych: 512 * Minimalna liczba jednoczesnych połączeń CIFS/AFP/FTP: 1024 |
| Uprawnienia | Uprawnienia aplikacji listy kontroli dostępu systemu Windows (ACL) |
| Wirtualizacja | Obsługa Vmware vSphere®, Microsoft Hyper-V®, Citrix®, |
| Usługa katalogowa | Integracja z usługami Windows® AD Logowanie użytkowników domeny przez protokoły SMB/NFS/AFP/FTP lubWWW , integracja z LDAP |
| Bezpieczeństwo | Zapora, szyfrowanie folderu współdzielonego, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne  blokowanie logowania, obsługa Let’s Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania) |
| Obsługiwane przeglądarki | Chrome®, Firefox®, Edge®, , Safari® 10 i nowsze, |
| Oprogramowanie | * Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych, aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych * Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów * Urządzenie musi umożliwiać pracę w trybie klastra wysokiej dostępności (HA) aby zapewnić nieprzerwany, natychmiastowy dostęp do zasobów bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system). Wszystkie dane z powodzeniem zapisane na serwerze aktywnym będą na bieżąco kopiowane do serwera pasywnego zapewniając replikację w czasie rzeczywistym i dostęp do danych oraz usług w przypadku uszkodzenia jednostki aktywnej dając gwarancję ciągłości pracy. Utworzenie klastra HA ma się opierać o 2 identyczne urządzenia. |
| Konserwacja | * Konserwację urządzenia należy przeprowadzać przy użyciu dodatkowych, wygodnych w użyciu przesuwnych szyn rack dostarczonych z zestawem |
| Zasilanie | * Wymogiem jest dostarczenie sprzętu wyposażonego w nadmiarowy zasilacz. |
| Gwarancja | Wykonawca udzieli gwarancji:   * na okres do końca czerwca 2026 r. na urządzenia główne   oraz na dodatkowe akcesoria montażowe w postaci przesuwnych szyn rack |

**Zadanie nr 3:**

**Szczegółowy opis przedmiotu zamówienia;**

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.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

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 7 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

* Firewall.
* Ochrony w warstwie aplikacji.
* Protokołów routingu dynamicznego.

# 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.

# Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:

* 16 portami Gigabit Ethernet RJ-45.
* 8 gniazdami SFP 1 Gbps.
* 2 gniazdami SFP+ 10 Gbps.

1. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
2. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q.
3. System jest wyposażony w zasilanie AC.

# Parametry wydajnościowe:

1. W zakresie Firewall’a obsługa nie mniej niż 1.4 mln jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 11 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 2.5 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.

# Funkcje Systemu Bezpieczeństwa:

W ramach systemu ochrony są 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).

# Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

* Translację jeden do jeden oraz jeden do wielu.
* Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

1. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
3. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
4. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
5. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.

* Amazon Web Services (AWS).
* Microsoft Azure.
* Cisco ACI.
* Google Cloud Platform (GCP).
* OpenStack.
* VMware NSX.
* Kubernetes.

# Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:

* Wsparcie dla IKE v1 oraz v2.
* Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
* Obsługa protokołu Diffie-Hellman grup 19, 20.
* Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
* Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
* Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
* Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
* Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
* Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
* Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
* Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
* Mechanizm „Split tunneling” dla połączeń Client-to-Site.

1. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:

* 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.
* Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
* 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.

# Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia 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.

# Funkcje SD-WAN

1. System umożliwia 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).

# Zarządzanie pasmem

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

# Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. System umożliwia 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 umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje 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 współpracuje 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 zapewnia 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.

# Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

# Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

# Kontrola WWW

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja 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.

# Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:

* Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
* Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
* Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

1. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
2. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

# 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 jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

# Logowanie

1. Elementy systemu bezpieczeństwa realizują 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 zapewnia 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 obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

# Testy wydajnościowe oraz funkcjonalne

1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

# Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

1. Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres do końca czerwca 2026 r..
2. **W ramach postępowania muszą zostać dostarczone również licencje do posiadanego przez Zamawiającego urządzenia FG100F o numerze seryjnym: FG100FTK21050334** upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: kontrola aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych – co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na **okres do końca czerwca 2026 r.**.

# Gwarancja oraz wsparcie

1. System jest objęty serwisem gwarancyjnym producenta przez okres do końca czerwca 2026 r., polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

# Opisy do wymagań ogólnych

1. Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

Wymagane jest oświadczenie producenta lub partnera producenta , iż produkt pochodzi z legalnego kanału sprzedaży.

**Zadanie nr 4:**

Wdrożenie musi obejmować:

1. Omówienie konsoli Managementowej
2. Przygotowanie konfiguracji Agentów oraz polityk
3. Wsparcie przy wdrożeniu Agentów Windows/Mac/Linux
4. Wsparcie przy konfiguracji pozostałych funkcjonalności.

Zamawiający informuje, że posiada obecnie system antywirusowy oparty na licencji ESET PROTECT Entry On-Prem – 65 stanowisk – identyfikator publiczny: 33D-NWS-3BD z terminem obowiązywania do 16.01.2025r.

Zamawiający docelowo oczekuje dostarczenia oprogramowania z funkcją XDR, tj. oprogramowania ESET PROTECT Enterprise lub równoważnego (zgodny z opisem wymagań równoważnych) na okres do końca czerwca 2026r. od dnia zakończenia ważności posiadanej licencji oraz rozszerzenia licencji do 75 stanowisk.

Opis równoważności Funkcjonalności Systemu XDR

1. - Agent musi obsługiwać funkcjonalności Next Generation EPP (Endpoint Protection Platform) oraz EDR (Endpoint Detection and Response) w jednym autonomicznym agencie, który do realizacji swoich funkcjonalności nie potrzebuje łączności z chmurą lub konsolą zarządzającą. Wymagane jest wsparcie dla systemów operacyjnych Windows, macOS i Linux.

2. - Rozwiązanie musi być w stanie identyfikować zaawansowane zagrożenia, takie jak ataki bez plikowe, 0-day malware czy wykorzystywanie podatności posiadanego software/hardware bez korzystania z silników reputacji lub silników detekcji opartej o sygnatury. Przez silnik reputacyjny rozumiemy identyfikację zagrożeń z wykorzystaniem następujących elementów reputacji: adresy IP, DNS, URL, skróty/hashe.

3. - Rozwiązanie musi wykorzystywać statyczne oraz dynamiczne algorytmy bazujące na sztucznej inteligencji w celu identyfikacji zagrożeń, również tych które nie są wcześniej znane.

4. - Agent musi być w pełni autonomiczny, co oznacza, że jego działanie i funkcjonalność nie może być zależna od serwera zarządzania, chmury ani ŻADNYCH zasobów zewnętrznych od agenta.  Wykrywanie i reagowanie na zaawansowane zagrożenia (0-day, bezplikowe, oparte na pamięci RAM, Exploity 0-Day, ransomware, cryptominers, lateral movement, APT) musi być możliwe w czasie rzeczywistym, nie może zależeć od stanu sieciowego stacji (agent musi realizować te same funkcjonalności w trybie online i offline) oraz nie może wymagać innego rodzaju zewnętrznych zasobów.

5. - Informacje na temat incydentów bezpieczeństwa muszą być przechowywane co najmniej przez 365 dni.

6. - Moduły EPP / EDR oferowane w rozwiązaniu muszą automatycznie reagować na pojawiające się zagrożenia, łagodząc zagrożenia w czasie zbliżonym do rzeczywistego, w autonomiczny sposób, z następującymi opcjami odpowiedzi na zagrożenie, definiowane przez politykę bezpieczeństwa:

     6.1 - Ostrzeżenie: taka notyfikacja musi być stała, nawet jeśli polityka nie jest w trybie ochrony.

     6.2 - Zabij proces: Zatrzymuje procesy. Aktywna zawartość w dokumentach, plikach wykonywalnych i procesach podrzędnych jest zatrzymywana. Agent włącza funkcję zabicia procesu dla procesów, które działają wbrew normalnemu zachowaniu stacji końcowej lub nie pasują do działań aplikacji, w której ukrywa się proces.

     6.3 - Kwarantanna: zatrzymuje procesy, szyfruje plik wykonywalny i przenosi go na ograniczoną ścieżkę. Jeśli zagrożenie jest znane, agent automatycznie je unieszkodliwia, zanim będzie można je wykonać.

      6.4 - Odłącz się od sieci: (lub kwarantanna sieciowa lub izolacja sieciowa) Agent musi komunikować się tylko z konsolą zarządzającą. Stacja końcowa nie może komunikować się z innymi elementami w sieci. Wszystkie działania na konsoli zarządzania muszą działać niezależnie od stanu izolacji sieci agenta.

     6.5 - Funkcja Naprawy (Remediate): Zatrzymuje procesy, poddaje kwarantannie pliki binarne, usuwa połączone biblioteki, usuwa pliki źródłowe i przywraca konfigurację systemu operacyjnego, aplikacji i ustawień użytkownika do stanu sprzed rozpoczęcia ataku.

      6.6 - Rollback: przywraca stan stacji końcowej do stanu z momentu utworzenia migawki VSS (Volume Shadow Copy), cofając zmiany wprowadzone przez złośliwy proces i skojarzone z nim zasoby. Agent powinien autonomicznie i w czasie zbliżonym do rzeczywistego przywrócić dane z chronionego hosta w przypadku ataku z wykorzystaniem szkodliwego oprogramowania typu ransomware.

7. - Rozwiązanie EPP / EDR musi wspierać następujące modele wdrożenia: SaaS (agent-> usługa SaaS w chmurze) lub wdrożenie lokalne (urządzenie wirtualne) lub wdrożenie hybrydowe.

8. - Rozwiązanie musi obsługiwać następujące mechanizmy wykrywania złośliwego oprogramowania:

     8.1 - Przed wykonaniem (Pre-Execution): identyfikacja złośliwego oprogramowania na podstawie plików za pośrednictwem silnika reputacji. Funkcja nie wymaga aktualizacji baz danych sygnatur oraz aktualizacji plików sygnatur do realizacji swoich zadań. Dopuszcza się, aby działanie tej funkcjonalności było zależne od chmury lub serwera zarządzającego – dlatego skanowanie całego dysku tym silnikiem powinno odbywać się TYLKO podczas początkowej instalacji i nie może być wymagane, aby zapewnić poprawne działanie wszystkich funkcji bezpieczeństwa.

     8.2 - Przed wykonaniem (Pre-Execution): rozwiązanie musi potrafić identyfikować nieznane szkodliwe oprogramowanie oparte na plikach na podstawie analizy statycznego z wykorzystaniem algorytmów uczenia maszynowego. Taka analiza musi odbywać się autonomicznie na stacji końcowej, bez zewnętrznych zależności lub zewnętrznego przetwarzania. Funkcjonalność nie może wymagać do działania uwzględnienia znanych IoC (DNS, IP, URL, HASH), a detekcja tego typu musi działać w czasie rzeczywistym podczas dostępu do systemu operacyjnego lub danego pliku.

     8.3 - W czasie wykonywania (Run-Time): agent musi identyfikować i reagować na ataki z wykorzystaniem wyrafinowanych technik hackerskich (ataki bezplikowe, podatności i malware 0-day, złośliwe skrypt, lateral movement, oprogramowanie ransomware, trojany, APT itp.) Identyfikacja tych zagrożeń nie może wymagać zewnętrznych zależności, interwencji człowieka lub analizy danych poza chronioną stacją końcową. Funkcjonalność musi być realizowana w czasie zbliżonym do rzeczywistego poprzez wykorzystanie algorytmów sztucznej inteligencji. Znane IoC (DNS, IP, URL, HASH) nie mogą być wymagane jako środek identyfikacji zagrożenia.

9. - Rozwiązanie musi zapewniać silny mechanizm „Anti-Tamper”, czyli mechanizmy ochrony przed manipulacja oprogramowaniem przez malware lub użytkownika końcowego. Taki mechanizm musi być chroniony unikalnym hasłem dla każdego komputera końcowego. Stan WŁ./WYŁ. Ochrony przed manipulacją powinien być opcją konfigurowalną w polityce bezpieczeństwa.

10. - Polityka bezpieczeństwa musi zapewniać opcję włączenia lub wyłączenia poszczególnych silników detekcyjnych lub według typu silnika (silniki przed wykonaniem i uruchomieniem). Opcja ta nie jest wymagana dla silnika reputacji.

11. - Rozwiązanie musi zawierać otwarty interfejs API który umożliwia integracje z innymi rozwiązaniami, monitorowanie środowiska oraz automatyzacje niektórych z procesów. Dokumentacja interfejsu API powinna być natywnie dostępna z poziomu konsoli zarządzania.

12. - Rozwiązanie musi obsługiwać architekturę typu Multi-Site lub Multi-Tenant, aby całkowicie odseparować utworzone w systemie instancję i zapewnić odpowiedni dostęp administracyjny do konkretnej lokacji utworzonej zgodnie z modelem Multi-Site.

13. - Rozwiązanie musi obsługiwać uwierzytelnianie SSO - SAMLv2.

14. - Rozwiązanie musi zapewniać mechanizm RBAC (Role-based Access Control) pozwalający na definiowanie granularnych uprawnień dla poszczególnych użytkowników administracyjnych zarówno do wybranych funkcji systemu jaki i dostępów do odpowiednich poziomów w architekturze Multi-Site lub Multi-Tenant.

15. - Rozwiązanie musi obsługiwać uwierzytelnianie dwuskładnikowe (2FA) w celu uzyskania dostępu administracyjnego za pomocą aplikacji Google Authenticator lub Duo.

16. - Rozwiązanie musi obsługiwać następujące formaty syslog: CEF, CEF2, RFC-5424, STIX i IOC. Rozwiązanie powinno obsługiwać certyfikaty SSL i X.509 do szyfrowania i uwierzytelniania transportu syslog.

17. - Rozwiązanie musi zapewniać możliwość wysyłania wiadomości tekstowych do użytkownika stacji końcowej, bezpośrednio z konsoli zarządzania, nawet kiedy agent pracujący na stacji, znajduje się w trybie izolacji sieci / kwarantanny sieciowej.

18. - Rozwiązanie musi umożliwiać zintegrowane z usługą Active Directory, aby możliwe było automatyczne przypisywanie agentów do grup, w celu powiązania ich z zasadami AD. Konsola zarządzania NIE powinna łączyć się z usługą Active Directory bezpośrednio za pośrednictwem programu ADFS ani żadnej innej metody uzyskiwania atrybutów usługi Device i User AD. Serwer zarządzania rozwiązaniem nie powinien mieć żadnych zależności od stanu usługi AD.

19. - Rozwiązanie musi zawierać dashboard pokazujący wszystkie komputery, oraz możliwość ich filtrowania na podstawie atrybutów takich jak: OS, typ stacji końcowej, wersja agenta, występujące podatności, atrybuty AD, informacyjne telemetryczne, adresacja IP, charakterystyki hardware, ilości CPU, adresy Mac, interfejsy, nazwa hosta, nazwa grupy, domena). Lista powinna być dostępna do przeglądania w celu inwentaryzacji hostów, stosowania akcji dla podzbioru stacji końcowych lub mapowania stacji końcowych do grup. Musi zapewniać opcję wyświetlenia szczegółów stacji, takie jak aspekty telemetrii, stan stacji, aplikacje oraz zapewniać następujące opcje działania: Odłącz/ Połącz się od sieci (kwarantanna sieciowa, Uruchom ponownie OS, Zamknij system, Wyślij wiadomość do użytkownika, Odinstaluj agenta, Wyświetl zagrożenia.

20. - Polityka ochrony stacji musi umożliwiać odpowiedź na wykryte zagrożenie w oparciu o kwalifikację zdarzenia (zagrożenie [Malicious Threat] czy podejrzane działanie [Suspicious Threat]). Odpowiedź na zagrożenie powinna umożliwiać wybranie opcje alert-only lub opcje aktywnej ochrony w oparciu o klasyfikację zagrożenia. Aktywna odpowiedź na zagrożenie, powinna być wykonywana przez autonomicznego agenta, nawet jeśli chroniona stacja nie jest podłączona do sieci.

21. - Rozwiązanie EPP / EDR musi mieć funkcjonalność lokalnego firewalla dla chronionej stacji końcowej. Ochrona firewall musi umożliwiać realizację unikalnych polityk dla każdej chronionej grupy hostów. Reguły firewalla powinny umożliwiać uwzględnienie następujących parametrów: FQDN, IP, CIDR. Funkcjonalność musi być obsługiwana dla następujących systemów operacyjnych: Windows, Linux i MacOS.

22. - Rozwiązanie EPP / EDR musi mieć funkcjonalność kontroli urządzeń, które próbują uzyskać dostęp do chronionej stacji. Kontrola urządzeń musi umożliwiać realizację unikalnych polityk dla każdej chronionej grupy hostów. Wymagana jest obsługa kontroli urządzeń dla następujących interfejsów: USB i Bluetooth.

23. - Rozwiązanie EPP / EDR musi posiadać funkcję informowania o podatnościach aplikacji zainstalowanych na chronionym hoście i dostarczać informacji z CVE związanych z wykrytą podatnością wzbogaconą danymi ze strony MITRE i NVD.

24. - Funkcjonalność przedstawiająca podatności w aplikacjach zainstalowanych na chronionym hoście musi dostarczać informacje o historii danej podatności, to jest, kiedy została wykryta, kiedy został opracowana poprawka, kiedy został przydzielony numer CVE, itp. Dodatkowo, funkcja musi przedstawiać indykatory podatności, takie jak np. czy dana podatność jest obecnie używana do wykonywania ataków, czy można ją wykorzystać zdalnie, itp.

**Zadanie nr 5:**

**ETAPY PRAC - Wdrożenie**

1. Instalacja i konfiguracja serwera (maszyna fizyczna lub VM) dla usługi
2. Instalacja i konfiguracja usługi w zakresie uzgodnionym w projekcie technicznym, w szczególności obejmująca:
   1. Przygotowanie konfiguracji agenta
   2. Dystrybucję agenta na stacje robocze
   3. Inwentaryzację sprzętu i oprogramowania stacji roboczych, w tym okresowe skanowania sieci pod kątem wykrycia nowych zasobów
   4. Zarządzanie licencjami na stacjach roboczych, w tym zliczanie realnego użycia aplikacji
   5. Zarządzanie aplikacjami na stacjach roboczych, w tym blokowanie niechcianych aplikacji, powiadamianie o wykrytych aplikacjach i podobne
   6. Zarządzanie konfiguracją stacji roboczych, poprzez masową dystrybucję pakietów zmian plikowych/zmian w rejestrze i podobnych
   7. Masową i indywidualną dystrybucję oprogramowania na stacje robocze
   8. Przejmowanie pulpitu stacji roboczych i metody interakcji z użytkownikiem podczas sesji zdalnej
   9. Zarządzanie i dystrybucję poprawek Microsoft i poprawek innych producentów na stacje robocze
   10. Funkcje raportowania i alertowania
   11. Konfiguracja zaawansowana OS i aplikacji w zakresie bezpieczeństwa (hardening).
3. Warsztat dla Zamawiającego, obejmujący tematykę praktycznej administracji wdrożonymi rozwiązaniami
4. Dokumentacja techniczna. Opracowanie dokumentacji powdrożeniowej

**Wymagania systemu zarządzania:**

* System musi umożliwiać instalację na systemie operacyjnym Windows (wersja co najmniej (2008)
* Dostęp do systemu jest zapewniony za pośrednictwem konsoli webowej bez konieczności instalacji dodatkowych komponentów
* System działa agentowo
* System ma możliwość instalacji wersji 32bit oraz 64bit.
* System obsługuje bazy danych Postgres oraz MS SQL jako instancje do przechowywania danych
* System posiada wbudowane funkcjonalności wykonywania backupu bazy danych, odtworzenia bazy danych, zmiany bazy danych
* System pozwala na podłączenie certyfikatu w formie .PFX(PKCS12)
* System posiada interfejs programowania aplikacji API pozwalający na integrację z innymi systemami
* System umożliwia połączenie z Servicedesk Plus
* System pozwala na wysyłanie powiadomień SMS w zakresie alertów dotyczących zinwentaryzowanego sprzętu
* System posiada możliwość zarządzania urządzeniami z systemami Windows (Vista i wyższe), Windows Server (2008 i wyższe) Linux (Ubuntu 10.04), Oracle Linux, Red Hat Enterprise Linux 8 i wyżej, CentOS 8, Fedora 19, mandriva 2010, Debian 7, Linux Mint 13, OpenSuse 11, Suse enterprise Linux 11), macOS (wersja 10.7 i wyższe), Android (wersja 4.0 i wyższe), IOS (wersja 4.0 i wyższe), Windows Phone (wersja 8.1 i wyższe), chromeOS (wersja 57.0 i wyższe), tvOS (wersja 7.0 i wyższe)
* System posiada funkcje Geofencing oraz Conditional Exchange Access.
* System pozwala na wysyłanie wdrożenia automatycznie inicjowanego ponownie po przesłaniu pominiętych poprawek
* System umożliwia tworzenie niestandardowych reguł produktowych bez nazwy dostawcy pod kontrolą aplikacji.
* System rozpoznaje stacje robocze w ramach Active Directory oraz Workgroup.
* System umożliwia dodawanie załączników takich jak faktury, gwarancje w dowolnym formacie
* System umożliwia instalację i deinstalację aplikacji z indywidualnymi ustawieniami dla pojedynczych stacji, określonych grup roboczych, użytkowników lub grup użytkowników.
* System umożliwia tworzenie list aplikacji, które będą mogły być instalowane przez samego użytkownika z poziomu stacji roboczej, tzw. Portal samoobsługowy.
* System posiada wbudowane funkcje zarządzania i wdrażania łat systemowych i ServicePack na stacjach roboczych oraz serwerach, w szczególności musi rozpoznawać sekwencje instalacji.
* Funkcje wdrażania łat obejmują co najmniej oprogramowanie: systemy operacyjne Windows: Vista, 7, 8, 10, 11, Windows Server 2008, 2012, 2016, 2022, Systemy MacOS (wersja 10.7 i wyższe), Microsoft Office, Google Chrome, Opera, Skype, Mozilla Firefox, Adobe Reader, Adobe Acrobat, Adobe Shockwave Player, Adobe Flash Player, Java, inne
* System posiada wbudowane narzędzia rozpoznawania podatności stacji roboczych na zagrożenia w oparciu o brakujące łaty systemowe.
* Architektura systemu umożliwia zarządzanie stacjami roboczymi w sieci LAN
* System posiada wbudowane narzędzia zarządzania zasobami IT, w szczególności rozpoznaje komponenty sprzętowe oraz oprogramowanie zainstalowane na stacjach roboczych.
* System posiada wbudowane narzędzia zdalnego dostępu (sesji) z wykorzystaniem technologii ActiveX, HTML 5, z możliwością uzyskania potwierdzenia użytkownika oraz ma możliwość włączenia opcji nagrywania tych sesji.
* System umożliwia wdrażanie polityk konfiguracji dla systemów Windows, w szczególności polityk zużycia energii, konfiguracji drukarek i przeglądarek Internet Explorer, Mozilla Firefox, Google Chrome oraz Microsoft Edge.
* System posiada wbudowane narzędzia systemowe umożliwiające zdalne uruchomianie stacji roboczych, zdalne zamykanie stacji roboczych, skanowanie, czyszczenie i defragmentację dysków
* System posiada rozbudowany system zarządzania użytkownikami z podziałem na administratora, audytora, gościa, menadżera zasobów, menadżera łat, z możliwością dodawania nowych ról z określonymi uprawnieniami.
* System posiada możliwość dodania nowego użytkownika systemu z uwierzytelnianiem lokalnym lub Active Directory wraz z obsługą SSO oraz przy wykorzystaniu autoryzacji SAML
* System posiada możliwość uruchamiania instalatora aplikacji z uprawnieniami dowolnego użytkownika.
* System posiada mechanizm dwuskładnikowej autoryzacji dla opcji odinstalowania manualnego agenta.
* System umożliwia dodawanie i rozliczanie licencji aplikacji.
* System umożliwia uruchamianie zdalnego Menedżera Systemu dla systemu operacyjnego Windows bez potrzeby uruchamiania połączenia zdalnego sesją RDP, który pozwoli na: podgląd i zamykanie uruchomionych procesów na stacji roboczej, podgląd, uruchamianie, zatrzymywanie, zmianę stanu usług na stacji roboczej, uruchamianie zdalnego wiersza poleceń, podgląd, dodawanie i modyfikację rejestru systemowego stacji roboczej, przegląd logów systemowych stacji roboczej, podgląd menedżera urządzeń, podgląd udziałów sieciowych
* System umożliwia generowanie następujących raportów:
  + Raporty Active Directory
    - Aktualnie zalogowani użytkownicy
    - Często zalogowani użytkownicy,
    - rzadko logujący się użytkownicy,
    - nieaktywni Użytkownicy
    - Historia logowania użytkownika
    - Historia logowania użytkowników na poszczególnych komputerach
  + Wykorzystania aplikacji w skali całej organizacji
  + Raporty dotyczące poprawek
    - Narażone systemy,
    - Narażone poprawki,
    - Obsługiwane poprawki,
    - Brakujące poprawki czekające na zatwierdzenie,
    - Systemy wymagające ponownego uruchomienia
  + Raporty inwentaryzacji
  + Raporty dotyczące sprzętu
    - Komputery wg systemu operacyjnego,
    - Komputery wg producenta,
    - Komputery wg pamięci
    - Komputery wg wykorzystania dysku,
    - Komputery wg wieku
    - Komputery wg typu urządzenia
    - Zmapowane dyski logiczne
  + Raporty dotyczące oprogramowania
    - Oprogramowanie według producenta
    - Ostatnio zainstalowane oprogramowanie
    - Niedozwolone oprogramowanie
    - Wykorzystanie oprogramowania przez komputer
    - Klucze produktu oprogramowania
    - Komputery z/bez określonego oprogramowania
    - Podsumowanie zasad pomiaru użytkowania oprogramowania
    - Oprogramowanie specyficzne dla użytkownika
  + Raporty dotyczące licencji
    - Zgodność licencji Licencje do odnowienia
  + Raporty dotyczące systemu
    - Użytkownicy grupy systemu
    - Komputery wg usług
  + Raporty dotyczące gwarancji
    - Gwarancja niedługo wygaśnie
    - Gwarancja wygasła
    - Niezidentyfikowane komputery
  + Raporty bezpieczeństwa
    - Szczegóły Antivirus
    - Szczegóły Bitlocker
    - Szczegóły Firewall
    - Raporty skanowania plików multimedialnych
    - Szczegóły pliku wg kategorii
    - Szczegóły pliku wg rozszerzenia
* System umożliwia planowanie raportów i przesyłanie ich w formie pliku PDF, XLSX, CSV na podany adres mailowy
* System umożliwia tworzenie niestandardowych raportów w oparciu o kryteria dostępne z systemu.
* System umożliwia tworzenie niestandardowych raportów w oparciu o wysyłanie zapytań SQL do bazy danych z poziomu konsoli zarządzającej.
* System umożliwia kopiowanie plików do folderów, kopiowanie wielu plików i kopiowanie folderów.
* System pozwala na Import komputerów z pliku np. CSV
* System posiada możliwość generowania logów a także wyświetlania listy statusów i wykonanych akcji
* System umożliwia podgląd wydajność sieci i komputera w czasie rzeczywistym podczas sesji zdalnych.
* System posiada możliwość wysyłania ogłoszenia do komputerów docelowych.
* System posiada możliwość zarządzanie funkcją BitLocker, która umożliwia wdrażanie wielu metod szyfrowania dysków w celu zabezpieczenia danych przedsiębiorstwa.
* System posiada możliwość ograniczenia, ile razy użytkownik może odroczyć zamknięcie lub ponowne uruchomienie komputera.
* System posiada możliwość zautomatyzowania zarządzania certyfikatami klientów dzięki integracji ACME Endpoint Central.
* System posiada możliwość zdalnego dostępu do programu Windows PowerShell.
* System posiada możliwość tworzenia dynamicznych grup niestandardowych do kontroli aplikacji i urządzeń.