1. **Serwer – 1 szt.**

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Obudowa** | * Obudowa Rack o wysokości max 1U 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, 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/ Apple 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 procesora do pracy w serwerach dwuprocesorowych. |
| **Procesor** | * Zainstalowany jeden procesor min. 16-rdzeniowy klasy x86, min. 2.0GHz, dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 265 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. |
| **RAM** | * Minimum 128GB DDR5 RDIMM 4800MT/s, |
| **Funkcjonalność pamięci RAM** | * Demand Scrubing, * Patrol Scrubing, * Permanent Fault Detection |
| **Interfejsy sieciowe/FC/SAS** | * Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT * Dodatkowa karta Dual Port (2x SFP+, 10Gb/s, SFP+, PCIe) * Dodatkowa karta SAS (4x mini SAS-HD, 12Gb/s, SAS, PCIe) |
| **Dyski twarde** | * Zainstalowane dwa dyski M.2 NVME o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. |
| **Wbudowane porty** | * 4 x USB z czego nie mniej niż 1x USB 3.0, * 2x VGA |
| **Video** | * Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200 |
| **Zasilacze** | * Redundantne, Hot-Plug min. 700W klasy Titanium |
| **Bezpieczeństwo** | * Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. * Możliwość wyłączenia w BIOS funkcji przycisku zasilania. * BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła * Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. * Moduł TPM 2.0 * Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera * Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem * Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). |
| **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); SNMP; IPMI2.0, SSH, Redfish;   + 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 lub zmianie konfiguracji sprzętowej.   + możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera   + możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera   oraz z możliwością rozszerzenia funkcjonalności o:   * + Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej   + Przesyłanie danych telemetrycznych w czasie rzeczywistym   + Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze   + Automatyczna rejestracja certyfikatów (ACE) |
| **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, Redfish   + 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   + Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach   + 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   + Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)   + 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, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.   + Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.   + Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile   + Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.   + Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.   + Zdalne uruchamianie diagnostyki serwera.   + Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.   + Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. |
| **Certyfikaty** | * Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 * Serwer musi posiadać deklaracja CE. * Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami. * 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 złoży dokument potwierdzający spełnianie wymogu.** * Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022. |
| **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 gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat. * 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 Producenta (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. Certyfikowany Technik 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 dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. * Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:   + Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.   + Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.   + Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.   + Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu.   + Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. * Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. * Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. |

1. **Serwer – 1 szt.**

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Obudowa** | * Obudowa Rack o wysokości max 1U 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, 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/ Apple 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 procesora do pracy w serwerach dwuprocesorowych. |
| **Procesor** | * Zainstalowany jeden procesor min. 16-rdzeniowy klasy x86, min. 2.0GHz, dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 265 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. |
| **RAM** | * Minimum 128GB DDR5 RDIMM 4800MT/s, |
| **Funkcjonalność pamięci RAM** | * Demand Scrubing, * Patrol Scrubing, * Permanent Fault Detection |
| **Interfejsy sieciowe/FC/SAS** | * Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT * Dodatkowa karta Dual Port (2x SFP+, 10Gb/s, SFP+, PCIe) |
| **Dyski twarde** | * Zainstalowane dwa dyski M.2 NVME o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. |
| **Wbudowane porty** | * 4 x USB z czego nie mniej niż 1x USB 3.0, * 2x VGA |
| **Video** | * Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200 |
| **Zasilacze** | * Redundantne, Hot-Plug min. 700W klasy Titanium |
| **Bezpieczeństwo** | * Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. * Możliwość wyłączenia w BIOS funkcji przycisku zasilania. * BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła * Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. * Moduł TPM 2.0 * Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera * Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem * Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). |
| **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); SNMP; IPMI2.0, SSH, Redfish;   + 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 lub zmianie konfiguracji sprzętowej.   + możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera   + możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera   oraz z możliwością rozszerzenia funkcjonalności o:   * + Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej   + Przesyłanie danych telemetrycznych w czasie rzeczywistym   + Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze   + Automatyczna rejestracja certyfikatów (ACE) |
| **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, Redfish   + 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   + Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach   + 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   + Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)   + 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, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.   + Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.   + Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile   + Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.   + Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.   + Zdalne uruchamianie diagnostyki serwera.   + Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.   + Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. |
| **Certyfikaty** | * Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 * Serwer musi posiadać deklaracja CE. * Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami. * 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 złoży dokument potwierdzający spełnianie wymogu.** * Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022. |
| **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 gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat. * 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 Producenta (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. Certyfikowany Technik 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 dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. * Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:   + Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.   + Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.   + Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.   + Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu.   + Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. * Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. * Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. |

1. **Zarządzalne urządzenie sieciowe z obsługą VLAN – 2 szt.**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Minimalne wymagania Zamawiającego** | |
|  | **CECHY ZARZĄDZANIA** | |
|  | Typ przełącznika | Zarządzany |
|  | Przełącznik wielowarstwowy | L2/L3 |
|  | Obsługa jakość serwisu (QoS) | Tak |
|  | Zarządzany w chmurze | Tak |
|  | Zarządzanie przez stronę www | Tak |
|  | Inspekcja ARP | Tak |
|  | Konfigurowanie ustawień lokalizacji (CLI) | Tak |
|  | Obsługa MIB | Tak |
|  | **OCHRONA** | |
|  | Funkcje DHCP | DHCP relay, DHCP server, DHCPv6 client |
|  | Lista kontrolna dostępu (ACL) | Tak |
|  | Zasady Listy Kontroli Dostępu (ACL) | 1024 |
|  | IGMP snooping | Tak |
|  | Ochrona hasłem | Tak |
|  | obsługuje SSH/SSL | Tak |
|  | Filtrowanie adresów MAC | Tak |
|  | Szyfrowanie / bezpieczeństwo | HTTPS, SSH, SSL/TLS |
|  | **PORTY I INTERFEJSY** | |
|  | Podstawowe przełączanie RJ-45 Liczba portów Ethernet | 48 |
|  | Podstawowe przełączania Ethernet RJ-45 porty typ | Gigabit Ethernet (10/100/1000) |
|  | Ilość slotów Modułu SFP+ | 4 |
|  | Liczba portów USB 2.0 | 1 |
|  | **SIEĆ** | |
|  | Standardy komunikacyjne | IEEE 802.1D, IEEE 802.1w, IEEE 802.1s, IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z, IEEE 802.3ad |
|  | Obsługa 10G | Tak |
|  | Dublowanie portów | Tak |
|  | Protokół drzewa rozpinającego | Tak |
|  | Blokowanie head-of-line (HOL) | Tak |
|  | Prędkość transferu danych przez Ethernet LAN | 10,100,1000 Mbit/s |
|  | Kontrola wzrostu natężenia ruchu | Tak |
|  | Automatyczne MDI/MDI-X | Tak |
|  | Podpora kontroli przepływu | Tak |
|  | Agregator połączenia | Tak |
|  | Obsługa sieci VLAN | Tak |
|  | Liczba VLANs | 4094 |
|  | **PRZESYŁANIE DANYCH** | |
|  | Wielkość tabeli adresów | 16000 wejścia |
|  | Zgodny z Jumbo Frames | Tak |
|  | Rozszerzenie Jumbo Frames | 9000 |
|  | **FUNKCJE MULTICAST** | |
|  | Obsługa Multicast | Tak |
|  | **PROTOKOŁY** | |
|  | Protokoły zarządzające | SNMP |
|  | **KONSTRUKCJA** | |
|  | Możliwości montowania w stelażu | Tak |
|  | Przycisk reset | Tak |
|  | Diody LED | Tak |
|  | **WYDAJNOŚĆ** | |
|  | Procesor wbudowany | Tak |
|  | Taktowanie procesora | 800 MHz |
|  | Pojemność pamięci wewnętrznej | 512 MB |
|  | Wielkość pamięci flash | 256 MB |
|  | Aktualizacje oprogramowania urządzenia | Tak |
|  | **MOC** | |
|  | Zasilacz dołączony | Tak |
|  | **WARUNKI PRACY** | |
|  | Zakres temperatur (eksploatacja) | -5 - 50 °C |
|  | Zakres temperatur (przechowywanie) | -25 - 70 °C |
|  | Zakres wilgotności względnej | 10 - 90% |
|  | Dopuszczalna wilgotność względna | 10 - 90% |

1. **Zarządzalne urządzenie sieciowe z obsługą VLAN – 2 szt.**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Minimalne wymagania Zamawiającego** | |
|  | **CECHY ZARZĄDZANIA** | |
|  | Typ przełącznika | Zarządzany |
|  | Przełącznik wielowarstwowy | L3 |
|  | Obsługa jakość serwisu (QoS) | Tak |
|  | Zarządzanie przez stronę www | Tak |
|  | Inspekcja ARP | Tak |
|  | Konfigurowanie ustawień lokalizacji (CLI) | Tak |
|  | Raport zdarzeń systemowych | Tak |
|  | **OCHRONA** | |
|  | Funkcje DHCP | DHCP relay, DHCP server, DHCP snooping, DHCPv6 client, DHCPv6 relay |
|  | Lista kontrolna dostępu (ACL) | Tak |
|  | Zasady Listy Kontroli Dostępu (ACL) | 1024 |
|  | IGMP snooping | Tak |
|  | Uwierzytelniania | Guest VLAN, Uwierzytelnianie na podstawie portów |
|  | Typ uwierzytelniania | IEEE 802.1x, RADIUS |
|  | Wiązanie adresów IP-MAC-Port | Tak |
|  | Zabezpieczenie przed wejściem w pętlę | Tak |
|  | Filtrowanie BPDU / Ochrona | Tak |
|  | Szyfrowanie / bezpieczeństwo | 802.1x RADIUS, SSH, SSH-2, SSL/TLS |
|  | **PORTY I INTERFEJSY** | |
|  | Podstawowe przełączanie RJ-45 Liczba portów Ethernet | 8 |
|  | Podstawowe przełączania Ethernet RJ-45 porty typ | 10G Ethernet (100/1000/10000) |
|  | Ilość portów 10G Ethernet (miedź) | 8 |
|  | Ilość slotów Modułu SFP+ | 8 |
|  | Port konsoli | RJ-45 |
|  | Liczba portów USB 2.0 | 1 |
|  | **SIEĆ** | |
|  | Standardy komunikacyjne | IEEE 802.1D, IEEE 802.1Q, IEEE 802.1ab, IEEE 802.1p, IEEE 802.1s, IEEE 802.1w, IEEE 802.1x, IEEE 802.3, IEEE 802.3ab, IEEE 802.3ad, IEEE 802.3an, IEEE 802.3az, IEEE 802.3u, IEEE 802.3x, IEEE 802.3z |
|  | Obsługa 10G | Tak |
|  | Technologia okablowania Copper Ethernet | 10BASE-T, 10GBASE-T, 100BASE-TX, 1000BASE-T |
|  | Obsługiwane typy kabli | Cat5e |
|  | Routing oparty na regułach | Tak |
|  | Przekierowywanie IP | Tak |
|  | Dublowanie portów | Tak |
|  | Protokół drzewa rozpinającego | Tak |
|  | Blokowanie head-of-line (HOL) | Tak |
|  | Prędkość transferu danych przez Ethernet LAN | 10,100,1000,10000 Mbit/s |
|  | Aktywne wyszukiwanie połączenia | Tak |
|  | Pomiar długości kabla | Tak |
|  | Kontrola wzrostu natężenia ruchu | Tak |
|  | Automatyczne MDI/MDI-X | Tak |
|  | Podpora kontroli przepływu | Tak |
|  | Agregator połączenia | Tak |
|  | Limit częstotliwości | Tak |
|  | Obsługa sieci VLAN | Tak |
|  | Funkcje wirtualnej sieci LAN | IP subnet–based VLAN, MAC address-based VLAN, Port-based VLAN, Private VLAN, Protocol-based VLAN, Stacked VLAN, Tagged VLAN, Mapowanie VLAN, Voice VLAN |
|  | Typ mapowania VLAN | Mapowanie VLAN 1:1 |
|  | Liczba VLANs | 4094 |
|  | **PRZESYŁANIE DANYCH** | |
|  | Przepustowość rutowania/przełączania | 320 Gbit/s |
|  | Prędkość przekazywania | 238,08 Mpps |
|  | Liczba kolejek | 8 |
|  | Trasa statyczna | Tak |
|  | Liczba tras statycznych | 990 |
|  | Ilość interfejsów IP | 128 |
|  | Pamięci bufora pakietów | 3 MB |
|  | Wielkość tabeli adresów | 16000 wejścia |
|  | Zgodny z Jumbo Frames | Tak |
|  | Rozszerzenie Jumbo Frames | 9000 |
|  | **FUNKCJE MULTICAST** | |
|  | Obsługa Multicast | Tak |
|  | Multicast Listener Discovery (MLD) snooping | MLD v1/2 |
|  | **PROTOKOŁY** | |
|  | Protokoły zarządzające | SNMP v1/2c/3, Telnet, HTTP/HTTPS, SSH, RADIUS, BOOTP, SNTP |
|  | Protokół wybierania drogi | RIP-2 |
|  | Protokół rejestracji GARP VLAN (GVRP) | Tak |
|  | **KONSTRUKCJA** | |
|  | Możliwości montowania w stelażu | Tak |
|  | Przycisk reset | Tak |
|  | Diody LED | Tak |
|  | Produkt stackowalny | Tak |
|  | Układ | 1U |
|  | Wsparcie wentylatorów nadmiarowych | Tak |
|  | Liczba wentylatorów | 3 |
|  | Certyfikaty | UL (UL 60950), CSA (CSA 22.2), FCC 15 (CFR 47) A |
|  | **WYDAJNOŚĆ** | |
|  | Fizyczne układanie (w szt.) | 4 |
|  | Procesor wbudowany | Tak |
|  | Taktowanie procesora | 800 MHz |
|  | Pojemność pamięci wewnętrznej | 512 MB |
|  | Wielkość pamięci flash | 256 MB |
|  | Aktualizacje oprogramowania urządzenia | Tak |
|  | Poziom hałasu | 39,1 dB |
|  | MTBF (Średni okres międzyawaryjny) | 798504 h |
|  | **MOC** | |
|  | Zasilacz dołączony | Tak |
|  | Obsługa zasilania zapasowego (RPS) | Nie |
|  | Ilość jednostek zasilania | 1 |
|  | Napięcie wejściowe AC | 100 - 240 V |
|  | Częstotliwość wejściowa AC | 50 - 60 Hz |
|  | **WARUNKI PRACY** | |
|  | Zakres temperatur (eksploatacja) | -5 - 50 °C |
|  | Zakres temperatur (przechowywanie) | -25 - 70 °C |
|  | Zakres wilgotności względnej | 10 - 90% |
|  | Dopuszczalna wilgotność względna | 10 - 90% |
|  | Emisja ciepła | 196,88 BTU/h |

1. **Licencje oprogramowania serwerowego – 2 szt.**

Wymagane minimalne parametry

Oprogramowanie Windows Server 2022 Standard (licencja na 16 rdzeni procesora, wersja OEM) lub równoważne.

Opis równoważności dla systemu Windows Server 2022 Standard:

1. System operacyjny musi być przeznaczony do zastosowań serwerowych w Środowiskach fizycznych lub o minimalnej wirtualizacji.
2. System operacyjny musi być najnowszą wersją rodziny systemów operacyjnych danego producenta.
3. Licencja na system operacyjny musi uwzględniać prawo do bezpłatnej instalacji udostępnianych przez producenta poprawek krytycznych i opcjonalnych do zakupionej wersji oprogramowania co najmniej przez 5 lat.
4. Licencja na system operacyjny musi umożliwiać uruchomienie kontrolera domeny będącego w pełni zgodnym z domeną wdrożoną u Zamawiającego domeną Active Directory pracującą w oparciu o system Windows Server 2016 musi także być dostarczona możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server
5. Licencja na system operacyjny musi być bez ograniczeń czasowych.
6. Licencja na system operacyjny musi uprawniać do uruchamiania systemu operacyjnego w środowisku fizycznym i min. 2 środowiskach wirtualnych za pomocą wbudowanych mechanizmów wirtualizacji, bez konieczności zakupu dodatkowych licencji.
7. Zaimplementowanie w systemie operacyjnym środowiska wirtualizacyjnego musi umożliwiać dodawanie i usuwanie pamięci wirtualnej oraz wirtualnych kart sieciowych podczas pracy maszyny wirtualnej.
8. System operacyjny musi posiadać graficzny interfejs użytkownika.
9. System operacyjny musi być w pełni kompatybilny z usługą Active Directory w zakresie:
10. zarządzania użytkownikami,
11. zarządzania certyfikatami dla użytkowników wraz ze wsparciem możliwości logowania do domeny kartą mikroprocesorową,
12. możliwości przydzielania praw dostępu do zasobów sieciowych,
13. instalacji zdalnej oprogramowania z pakietów msi,
14. definiowanie polityk bezpieczeństwa dla użytkowników, grup oraz stacji roboczych z systemami MS Windows: 7,8,8.1, 10,11.
15. System operacyjny musi wspierać pracę domenową wraz z automatyczną synchronizacją dla dodatkowych serwerów.
16. System operacyjny musi wspierać zarządzanie przez dostępne narzędzia administracji serwera dla systemu Windows 10 (RSAT) oraz Windows Admin Center.
17. System operacyjny musi posiadać obsługę zdalnego pulpitu poprzez protokół RDP.
18. System operacyjny musi umożliwiać ustawianie relacji zaufania pomiędzy domenami.
19. Wszystkie narzędzia i usługi systemu operacyjnego powinny być rozwiązaniem jednego producenta.
20. System operacyjny musi posiadać obsługę pamięci USB jako monitora klastra
21. System operacyjny musi pozwalać na stopniowe uaktualnienia systemu operacyjnego klastra
22. System operacyjny musi posiadać obsługę deduplikacji na potrzeby systemu plików ReFS.
23. System operacyjny musi posiadać obsługę optymalizacji transportu w tle pod kątem opóźnień.
24. System operacyjny musi posiadać wbudowaną zaporę internetową (firewall) dla ochrony połączeń internetowych; zapora musi być zintegrowana z systemem konsoli do zarządzania ustawieniami zapory i regułami ip v4 i v6;
25. System operacyjny musi posiadać możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny;
26. System operacyjny musi posiadać możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;
27. System operacyjny musi posiadać obsługa PowerShelI 5.1,
28. System operacyjny musi posiadać obsługa certyfikatów w Active Directory
29. Wszystkie wymienione powyżej parametry, role, funkcje, itp. systemu operacyjnego objęte muszą być dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).
30. **Licencje systemu operacyjnego – 2 sztuki.**

Licencje systemu operacyjnego Microsoft Windows Server 2022 Datacenter 16-core lub oprogramowania równoważnego nie mogą posiadać ograniczeń czasowych, muszą pochodzić z oficjalnego kanału dystrybucji. Licencje nie mogą być dedykowane tylko do jednego producenta sprzętu serwerowego.

RÓWNOWAŻNOŚĆ:

1. Warunki równoważności dla licencji systemu Microsoft Windows Server 2022 Datacenter.

W przypadku zaoferowania przez Wykonawcę licencji systemu równoważnego do systemu Microsoft Windows Server 2022 Datacenter, Zamawiający wymaga dostarczenia licencji dla 2 serwerów oraz instalacji i migracji obecnego środowiska. Zamawiający wymaga, aby produkt równoważny spełniał niżej wymienione wymagania:

1. Współpraca z procesorami o architekturze x86 – 64bit.
2. Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.
3. Możliwość budowania klastrów składających się z 64 węzłów.
4. Pojedyncza licencja musi obsłużyć serwer fizyczny wyposażony w 16 rdzeni.
5. Praca w roli klienta domeny Microsoft Active Directory.
6. Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie funkcjonalności Microsoft Windows Server 2016.
7. Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu.
8. Możliwość uruchomienia roli klienta i serwera czasu (NTP).
9. Możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
10. Możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
11. Możliwość uruchomienia roli serwera stron WWW.
12. W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera.
13. W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego.
14. Wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).
15. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
16. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
17. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
18. pozwalają na zmianę rozmiaru w czasie pracy systemu,
19. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
20. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
21. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
22. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość
23. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
24. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET
25. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
26. Możliwość wykorzystania standardu http/2.
27. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
28. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
29. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
30. Mechanizmy logowania w oparciu o: a) login i hasło,
31. karty z certyfikatami (smartcard),
32. wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).
33. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla:
34. określonych grup użytkowników,
35. zastosowanej klasyfikacji danych,
36. centralnych polityk dostępu w sieci,
37. centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
38. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
39. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
40. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
41. Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji   
    w dokumentach (Digital Rights Management).
42. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
43. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
44. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.
45. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:

* podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
* ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
* odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,
* bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.,

1. zdalna dystrybucja oprogramowania na stacje robocze,
2. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników,
3. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:

* Dystrybucję certyfikatów poprzez http,
* Konsolidację CA dla wielu lasów domeny,
* Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
* Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.

1. szyfrowanie plików i folderów,
2. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),
3. szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi,
4. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,
5. serwis udostępniania stron WWW,
6. wsparcie dla protokołu IP w wersji 6 (IPv6),
7. wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
8. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie uruchomienie nieograniczonej liczby aktywnych środowisk wirtualnych systemów operacyjnych (liczba ograniczona parametrami fizycznymi serwera),
9. możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
10. możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover   
    z jednoczesnym zachowaniem pozostałej funkcjonalności.
11. mechanizmy wirtualizacji mające wsparcie dla:

* dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
* obsługi ramek typu jumbo frames dla maszyn wirtualnych.
* obsługi 4-KB sektorów dysków,
* nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,
* możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.

1. możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.
2. wsparcie dla rozwiązania Kubernetes.
3. możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz   
   z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
4. wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
5. mechanizmy deduplikacji i kompresji na wolumenach.
6. mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
7. mechanizm konfiguracji połączenia VPN do platformy Azure.
8. wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.
9. mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów.
10. możliwość instalacji i poprawnej pracy Systemu Bazodanowego (Microsoft SQL Server Standard).

1. **Licencje dostępowe na użytkownika – 50 szt.**

 Definicja i Wymagania:

 1. Ogólne Wymagania Licencji:

* Licencja dostępowa na użytkownika typu CAL User CSP jest wymagana dla systemu operacyjnego Windows Server 2022, zawarta w niniejszym zamówieniu. Licencja taka, lub jej równoważna, jest niezbędna w przypadku stosowania oprogramowania wymagającego takiego typu autoryzacji dostępu.

2. Opis Równoważności Funkcjonalności:

* Wymagane oprogramowanie równoważne musi zapewniać użytkownikowi możliwość pełnego i nieograniczonego dostępu do wszystkich funkcjonalności serwera Microsoft Windows Server 2022, w szczególności z wdrożoną rolą Active Directory. Równoważne oprogramowanie powinno oferować identyczny zakres usług i możliwości, co oryginalne rozwiązanie od Microsoft.
* Licencja musi umożliwiać każdemu przypisanemu użytkownikowi dostęp do systemu serwerowego z dowolnego urządzenia, bez ograniczeń co do liczby używanych urządzeń. Jest to niezbędne, aby wspierać elastyczność pracy oraz model pracy zdalnej i hybrydowej.
* Nabywana licencja powinna zapewniać użytkownikom możliwość korzystania z systemu z wielu urządzeń. Taka funkcjonalność jest kluczowa dla użytkowników, którzy na co dzień korzystają z różnych urządzeń, takich jak komputery stacjonarne, laptopy, tablety czy smartfony.
* Osoby posiadające licencję muszą mieć zapewniony dostęp do wszystkich zasobów serwera, do których mają uprawnienia. Obejmuje to dostęp do aplikacji, danych, usług drukowania, plików i innych zasobów przewidzianych dla nich przez administratora systemu.
* Licencja powinna pozwalać na swobodną zmianę przydzielonego urządzenia przez użytkownika, bez utraty możliwości korzystania z niej na nowym urządzeniu. Jest to istotne dla zapewnienia ciągłości pracy w przypadku zmiany sprzętu przez użytkownika.
* Licencje muszą być skalowalne i elastyczne, aby umożliwić szybkie dostosowanie do zmian w strukturze zatrudnienia.
* Nabywane licencje muszą wspierać korzystanie z zasobów serwera przez użytkowników w połączeniach zdalnych. Jest to kluczowe dla organizacji, które stosują model pracy zdalnej, umożliwiając pracownikom efektywny dostęp do zasobów firmowych z dowolnej lokalizacji.

1. **Oprogramowanie antywirusowe**

Oprogramowanie antywirusowe na okres do **06.05.2026 r.** dla 60 urządzeń.

Minimalne wymagania:

Administracja zdalna w chmurze

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

Ochrona stacji roboczych

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

* tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
* tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
* tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
* tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
* tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

1. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z:

Zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.

1. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
2. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
3. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
4. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
5. Rozwiązanie musi posiadać ochronę antyspamową dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail.
6. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:

* tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
* tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
* tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
* tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.

1. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
2. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
3. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
4. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
5. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
6. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
7. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

Ochrona serwera

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7 i 8, CentOS 7 i 8, Ubuntu Server 16.04 LTS i nowsze, Debian 9, Debian 10, SUSE Linux Enterprise Server (SLES) 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux oraz Amazon Linux.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

Dodatkowe wymagania dla ochrony serwerów Windows:

1. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
2. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
3. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
4. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
5. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
6. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
7. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych*.*
8. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
9. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

Dodatkowe wymagania dla ochrony serwerów Linux:

1. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
2. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
3. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
4. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

Szyfrowanie

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit.
2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

Ochrona urządzeń mobilnych opartych o system Android

1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.
5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
6. usunięcie zawartości urządzenia,
7. przywrócenie urządzenie do ustawień fabrycznych,
8. zablokowania urządzenia,
9. uruchomienie sygnału dźwiękowego,
10. lokalizację GPS.
12. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
13. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
14. nazwę aplikacji,
15. nazwę pakietu,
16. kategorię sklepu Google Play,
17. uprawnienia aplikacji,
18. pochodzenie aplikacji z nieznanego źródła.

Ochrona serwera pocztowego MS Exchange

1. Rozwiązanie musi wspierać instalację na systemach Microsoft Windows Server 2008 R2 i nowszych.
2. Rozwiązanie musi zapewniać wsparcie dla systemów poczty Microsoft Exchange 2007/2010/2013/2016/2019.
3. Rozwiązanie musi zapewniać wsparcie dla ról Mailbox, Edge, Hub.
4. Rozwiązanie musi skanować pocztę przychodzącą i wychodzącą na serwerze MS Exchange.
5. Rozwiązanie musi zapewnić skanowanie bezpośrednio w bazach danych Exchange przy pomocy VSAPI.
6. Rozwiązanie musi mieć możliwość tworzenia różnych reguł blokowania wiadomości w tym co najmniej po zdefiniowanym nadawcy, odbiorcy, temacie wiadomości, typie załącznika, rozmiarze załącznika, rozmiarze wiadomości, nagłówku wiadomości, na podstawie uzyskanego wyniku skanowania antyspamowego i antywirusowego, godzinie odbioru, obecności załącznika chronionego hasłem lub uszkodzonego archiwum.
7. Rozwiązanie musi posiadać wbudowany w oprogramowanie filtr antyspamowy odpowiedzialny za filtrowanie niechcianej poczty.
8. System antyspamowy ma być wyposażony przynajmniej w możliwość sprawdzania list RBL, DNSBL oraz mechanizm reputacji poczty.
9. Administrator musi mieć możliwość dodania własnych adresów list RBL oraz DSBL, z których będzie korzystać aplikacja.
10. Rozwiązanie ma posiadać mechanizm greylisting (szara lista).
11. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.

Sandbox w chmurze

1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.
3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
7. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów.
8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo.
12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:
13. Czysty,
14. Podejrzany,
15. Bardzo podejrzany,
16. Szkodliwy.
17. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
18. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
19. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

Ochrona usługi Microsoft 365

1. Rozwiązanie musi obejmować ochroną usługi Microsoft, takie jak Exchange Online, Onedrive, Sharepoint oraz aplikację Teams.
2. Rozwiązanie musi posiadać możliwość dodania kilku tenantów usługi Micosoft 365.
3. Administrator musi mieć możliwość wskazania, które konto użytkownika będzie objęte ochroną.
4. Rozwiązanie musi być zarządzane za pomocą dowolnej przeglądarki internetowej z dowolnego miejsca w sieci.
5. Rozwiązanie musi być dostępny w języku polskim.
6. Konsola rozwiązania musi posiadać możliwość raportowania co najmniej:
7. użytkowników, otrzymujących najwięcej spamu,
8. użytkowników, otrzymujących najwięcej wiadomości typu „phishing”,
9. użytkowników, otrzymujących największą ilość szkodliwego oprogramowania,
10. kont użytkowników, które mogę być podejrzane.
11. Konsola rozwiązania musi posiadać funkcjonalność logowania zdarzeń z podziałem na dzienniki dla Exchange Online i Onedrive.
12. Dzienniki Exchange Online muszą posiadać funkcjonalność informowania co najmniej:
13. jaka ilość wiadomości została przeskanowania,
14. wynik skanowania poszczególnej wiadomości,
15. czynność podjęta przez rozwiązanie.
16. Dzienniki Onedrive muszą posiadać funkcjonalność informowania co najmniej o:
17. zagrożeniach, które zostały wykryte,
18. na jakim koncie zostały wykryte,
19. jakie zagrożenie zostało wykryte,
20. podjętą czynność.
21. Rozwiązanie musi posiadać funkcjonalność kwarantanny, do której będą przenoszone zainfekowane obiekty z usługi Exchange Online oraz Onedrive.
22. Musi istnieć możliwość pobrania plików z kwarantanny w formie oryginalnego pliku i pliku zabezpieczonego hasłem.
23. Administrator musi posiadać możliwość przypisania konfiguracji, do dodanych do rozwiązania tenantów lub do poszczególnych grup i użytkowników.
24. Administrator musi posiadać możliwość konfiguracji rozwiązania w oparciu o co najmniej:
25. wykorzystania do analizy mechanizmów chmurowych, tego samego producenta,
26. wprowadzenia białych i czarnych list adresów ochrony Exchange’a Online,
27. dodania znacznika do tematu wiadomości zakwalifikowanej jako SPAM i phishing.
28. Rozwiązanie musi zapewniać funkcję ochrony przed zagrożeniami 0-day.
29. Funkcja ochrony przed zagrożeniami 0-day musi wykorzystywać do działania chmurę producenta.
30. Funkcja ochrony przed zagrożeniami 0-day musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
31. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
32. Rozwiązanie musi posiadać możliwość przesyłania powiadomień e-mail z funkcją wyboru preferowanego języka.

Moduł XDR

1. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
2. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
3. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
4. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
5. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”.
6. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.
7. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
8. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.
9. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.
10. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.
11. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.
12. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
13. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
14. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.
15. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.
16. Konsola administracyjna musi mieć możliwość tagowania obiektów.
17. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.

Moduł zarządzania podatnościami i aktualizacjami

1. Rozwiązanie musi mieć możliwości wykrywania podatności w systemach operacyjnych (co najmniej Windows 10, Windows 11) oraz aplikacjach zainstalowanych na zarządzanych stacjach.

2. Baza wykrywanych podatności musi zawierać minimum 35000 CVE.

3. Rozwiązanie nie może wymagać instalacji dodatkowej konsoli, ani innych dodatkowych

komponentów na stacjach końcowych.

4. Automatyczne wykrywanie podatności musi wykonywać się zgodnie z harmonogramem, nie częściej niż raz dziennie.

5. Moduł wykrywania podatności musi umożliwiać wyświetlanie szczegółów danej podatności zawierające minimum:

- nazwę aplikacji lub systemu operacyjnego

- punktacje CVSS

- opis wykrytej podatności

- wartość ryzyka oceniona przez wewnętrzne mechanizmy producenta

6. Moduł wykrywania podatności musi wykrywać podatności w minimum 700 aplikacjach.

7. Moduł zarządzania aktualizacjami musi umożliwiać wykonanie automatycznej aktualizacji dla minimum 150 popularnych aplikacji.

8. Moduł zarządzania aktualizacjami musi umożliwiać stworzenie białej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje będą aplikowane tylko i wyłącznie dla wskazanych aplikacji w białej liście. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.

9. Moduł zarządzania aktualizacjami musi umożliwiać stworzenie czarnej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje oprogramowania będą realizowane dla wszystkich - ponad 150 aplikacji, oprócz aplikacji wskazanych na czarnej liście. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.

10. Zarządzanie aktualizacjami aplikacji musi umożliwiać ręczne wdrażanie poprawek na wybranych stacjach.

11. Moduł zarządzania aktualizacjami oraz wykrywania podatności musi być zintegrowany

bezpośrednio z programem antywirusowym tego samego producenta zainstalowanym na

zarządzanym komputerze.

12. Stacja robocza posiadająca włączony moduł wykrywania podatności oraz zarządzania

aktualizacjami musi być w odpowiedni sposób oznaczona w konsoli centralnego zarządzania.

13. Administrator konsoli musi mieć możliwość włączenia modułu wykrywania podatności i

zarządzania aktualizacjami przy pomocy menu kontekstowego dostępnego w konsoli centralnego zarządzania.

14. Moduł wykrywania podatności ma umożliwiać wyłączenie powiadomień dla wybranej podatności.

1. **Serwer do wykonywania kopii zapasowych – 1 sztuka.**

|  |  |
| --- | --- |
| Komponent | Minimalne wymagania |
| **Obudowa i pojemność** | Wysokość maksymalnie 1U do instalacji w szafie Rack.  Co najmniej 9 slotów przeznaczonych na zestaw taśm. |
| **Połączenie** | Co najmniej 1 port SAS o przepustowości co najmniej 6Gb/s w standardzie umożliwiającym podłączenie serwerów. |
| **Napęd** | Wyposażony w co najmniej 1 sztukę napędu SAS LTO8.  W komplecie:   * kabel SAS umożliwiający podłączenie biblioteki do serwera o dł. min. 2m * 10x taśma LTO8 WORM * Oznaczenia dla taśm LTO8, numery: 1-200 * Oznaczenia dla taśm LTO8 WORM, numery: 1-200 * 1 taśmy czyszczące |
| **Gwarancja** | 5 lat gwarancji producenta  Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.  Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.  Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy.  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.  Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia.  Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych.  Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.  Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. |

1. **Macierz dyskowa – 1 szt.**

|  |  |
| --- | --- |
| **Element konfiguracji/cecha/funkcjonalność** | **Wymagania minimalne** |
| Typ obudowy | Macierz musi być przystosowana do montażu w szafie rack 19”,   o wysokość maksymalnie 2U oraz umożliwiać montaż min. 12 dysków 3.5” |
| Przestrzeń dyskowa | Zainstalowane:  6x dysk HDD SAS o pojemności min. 1.2TB, Hot-Plug  6x dysk HDD NLSAS o pojemności min. 4TB, Hot-Plug |
| Możliwość rozbudowy | Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 264 dysków twardych. |
| Obsługa dysków | Macierz musi mieć możliwość obsługiwania dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS 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 RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping).  Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID.  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.  Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem. |
| Interfejsy | Macierz musi posiadać, co najmniej 8 portów iSCSI 25Gb (4 porty na kontroler), |
| Kable/wkładki | 4x kabel DAC 25GbE SFP28-SFP28 min. 5m |
| 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.  Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych. |
| 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. |
| Migracja danych w obrębie macierzy | Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia. |
| Zdalna replikacja danych | Macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy.  Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z urządzeniem. |
| 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 posiadać certyfikat sprawności 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. |
| Standardy bezpieczeństwa | Urządzenie musi spełniać następujące standardy bezpieczeństwa: EN 62368-1 (European Union), IEC 60950-1 (International) |
| Inne | Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym  producenta. Na żądanie Zamawiającego, Wykonawca musi  przedstawić oświadczenie producenta oferowanego serwera,  potwierdzające pochodzenie urządzenia z oficjalnego kanału  dystrybucyjnego producenta.  Wymagane są dokumenty poświadczające, że sprzęt jest  produkowany zgodnie z normami ISO 9001 oraz ISO 14001.  Deklaracja zgodności CE. |
| Warunki gwarancji | 3 lata gwarancji producenta  Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.  Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.  Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych.  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.  Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia.  Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii.  Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych.  Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.  Możliwość rozszerzenia gwarancji przez producenta do 7 lat.  Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.  Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. |

1. **Serwer NAS – 1 szt.**

|  |  |
| --- | --- |
| Minimalne wymagania Zamawiającego | |
| Typ urządzenia | Serwer NAS |
| Obudowa | Rack |
| Procesor | Czterordzeniowy procesor o taktowaniu 2,2 GHz osiągający w teście PassMark  co najmniej 4580 punktów |
| Sprzętowy mechanizm szyfrowania | Tak (AES-NI) |
| Pamięć RAM | min. 4 GB pamięci ECC SODIMM z możliwością rozszerzenia do min. 32 GB |
| Możliwości rozbudowy | Sprzęt powinien być wyposażony w min. 8 kieszeni na dyski twarde typu hot-swap z możliwością rozszerzenia do 12 dysków łącznie przy użyciu dodatkowej jednostki rozszerzającej podłączanej do jednostki głównej za pomocą portu eSATA |
| Porty zewnętrzne | Minimum:   * 2 porty USB 3.2.1 * 1 eSATA (jako gniazdo rozszerzenia) |
| Porty sieciowe | Minimum:   * 4 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego) * Możliwość podłączenia dodatkowych kart sieciowych 10G poprzez gniazdo rozszerzeń PCIe x8 |
| Funkcja Wake on LAN/WAN | Tak |
| Gniazdo rozszerzeń PCIe 3.0 | Min. 1x 4-liniowe gniazdo x8 |
| Wentylator obudowy | Min. 2 wentylatory 80 mm x 80 mm |
| Obsługiwane protokoły sieciowe | Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV |
| Obsługiwane systemy plików | Min.:   * Wewnętrzny: Btrfs, ext4 * Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT |
| Zarządzanie pamięcią masową | * Maksymalny rozmiar pojedynczego wolumenu: 108 TB * Minimalny liczba wewnętrznych wolumenów: 64 * Minimalny liczba obiektów iSCSI Target: 128 * Minimalny liczba jednostek iSCSI LUN: 256 * Obsługa klonowania/migawek jednostek iSCSI LUN |
| Obsługiwane typy macierzy RAID | Min. SHR, Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 |
| Funkcja udostępniania plików | * Minimalna liczba kont użytkowników: 2 048 * Minimalna liczba grup użytkowników: 256 * Minimalna liczba folderów współdzielonych: 512 * Minimalna liczba jednoczesnych połączeń SMB/NFS/AFP/FTP: 1000 |
| Uprawnienia | Uprawnienia aplikacji listy kontroli dostępu systemu Windows (ACL) |
| Wirtualizacja | Obsługa VMware vSphere®, Microsoft Hyper-V®, Citrix®, OpenStack® |
| Usługa katalogowa | Łączy się z serwerami Windows® AD/LDAP, umożliwiając użytkownikom domeny logowanie za pośrednictwem protokołów SMB/NFS/AFP/FTP/File Station przy użyciu istniejących poświadczeń. |
| 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 systemy klienckie | Windows® 7 i nowsze, macOS® 10.12 i nowsze |
| Obsługiwane przeglądarki | Chrome®, Firefox®, Edge®, Internet Explorer® 10 i nowsze, Safari® 10 i nowsze, Safari (iOS 10 i nowsze), Chrome (Android™ 6.0 i nowsze) na tabletach |
| 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 * Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wpierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym. |
| Konserwacja | * Konserwację urządzenia należy przeprowadzać przy użyciu dodatkowych, wygodnych w użyciu przesuwnych szyn rack |
| Gwarancja | Wykonawca udzieli gwarancji:   * 3 lata na urządzenie główne * 1 rok na dodatkowe akcesoria montażowe w postaci przesuwnych szyn rack |
| Dodatkowa karta rozszerzeń | Dwa gniazda NVMe SSD M.2  Interfejs magistrali hosta: PCIe 3.0 x8  Interfejs pamięci masowej: PCIe NVMe  Wysokość mocowania: Niskoprofilowe i o pełnej wysokości  Obsługiwane obudowy: 22110 / 2280  Gwarancja: 5 lat |
| Dodatkowe akcesoria | Przesuwny zestaw szyn rack |

1. **Dyski twarde do serwera plików NAS – 8 szt.**

|  |  |
| --- | --- |
| Minimalne wymagania: | |
| Pojemność | min. 8000 GB |
| Typ | HDD (magnetyczny) |
| Format | Format 3,5 cala |
| Interfejs | Serial ATA III |
| Pamięć cache | min. 256 MB |
| Prędkość obrotowa | 7200 obr./ min. |

1. **Dyski twarde do serwera plików NAS – 2 szt.**

|  |  |
| --- | --- |
| Minimalne wymagania: | |
| Pojemność | min. 500 GB |
| Typ | SSD |
| Format obudowy | M.2 |
| Interfejs | PCIe NVMe 3.0 x4 |
| Odczyt losowy | 420,000 IOPS |
| Zapis losowy | 380,000 IOPS |
| Prędkość odczytu | 3430 MB/s |
| Prędkość zapisu | 2600 MB/s |
| Niezawodność MTBF | do 1 750 000 godzin |
| Wytrzymałość | 1000 TBW |

1. **UTM – 1 sztuka**

**Wymagania Ogólne**

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. Dla wszystkich funkcji systemu musi być dostarczony dokument potwierdzony przez producenta lub autoryzwanego dytrybutora o gotowości świadczenia usług wsparcia w języku polskim oraz bezpłatnej obsługi procesu wymiany uszkodzonego urządzenia.

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 4 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:

* 10 portami Gigabit Ethernet RJ-45.

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 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 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 1.3 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 650 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.

**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**

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:

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 36 miesięcy.

**Gwarancja oraz wsparcie**

System jest objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, 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.
2. Zaleca się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.

**Serwisy i licencje**

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

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 – 2 licencje na 12 miesięcy.

1. **Oprogramowanie przeciwdziałające wyciekowi danych - licencja wieczysta – 60 szt.**

Oprogramowanie na licencji wieczystej z dwu letnim wsparciem na minimum 60 stanowisk.

1. Pełne wsparcie dla stacji roboczych z systemami Windows 7/Windows 8.1/Windows 10/Windows 11.
2. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2012 i nowszych.
3. Pomoc w programie (help) i dokumentacja do programu dostępna w języku angielskim.
4. Konsola administracyjna oraz komunikaty klienta muszą być w języku polskim.
5. Serwer administracyjny musi wspierać instalację w oparciu o bazę MS SQL.
6. Serwer administracyjny musi działać w architekturze serwer-klient, gdzie komunikacja serwera zarządzającego z klientem odbywa się przy pomocy agenta.
7. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.
8. Serwer administracyjny musi umożliwiać wykonanie instalacji/dezinstalacji zdalnej klienta na stacjach roboczych.
9. Reguły DLP muszą być egzekwowane również w przypadku braku połączenia między klientem, a serwerem zarządzającym.
10. W przypadku braku połączenia klienta z serwerem zarządzającym, klient musi mieć możliwość lokalnego przechowywania informacji oraz zebranych danych do czasu ponownego połączenia z serwerem administracyjnym.
11. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsol.
12. Administrator musi posiadać możliwość zarządzania bazą danych poprzez określone zadania: kopia bazy danych, kopia oraz wyczyszczenie bazy danych, wyczyszczenie bazy danych.  Administrator musi posiadać możliwość określenia wykonywania czasu związanego z wykonywaniem zadań na bazie danych. Zadania powinny być wykonywane co najmniej z interwałem: raz na tydzień, raz na dwa tygodnie, raz w miesiącu, raz na trzy miesiące.
13. Administrator musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych. Jeżeli rozmiar bazy danych osiągnie skonfigurowany rozmiar, najstarsze informacje muszą być usunięte z bazy danych, w celu nie przekroczenia skonfigurowanego rozmiaru bazy.
14. Serwer administracyjny programu musi mieć możliwość automatycznego pobierania aktualizacji definicji kategoryzowania stron internetowych, aplikacji oraz rozszerzeń plików. Musi być możliwość wyłączenia automatycznego pobierania.
15. Administrator musi mieć możliwość tworzenia nowych kont administratorów w konsoli programu jak i ich usuwania oraz klonowania.
16. Administrator musi mieć możliwość przypisywania jak i odbierania uprawnień do wybranych modułów programu. Uprawnienia muszą być podzielone na:
17. Ustawienia, które określają możliwość wykonania konfiguracji na poszczególnym module,
18. Logi, które określają możliwość wyświetlenia logów poszczególnego modułu.
19. Serwer musi posiadać możliwość synchronizacji użytkowników oraz stacji roboczych z domeną

Active Directory.

1. System musi posiadać możliwość logowania zdarzeń aktywności stacji roboczej, w oparciu o co najmniej:
2. logowanie oraz wylogowanie użytkownika,
3. włączenie oraz wyłączenie stacji roboczej,
4. blokada oraz odblokowanie stacji roboczej,
5. przejście w stan bezczynności stacji roboczej.

1. Administrator musi mieć możliwość, wymuszenia synchronizacji ustawień oraz logów, pomiędzy stacją roboczą, a serwerem, w czasie rzeczywistym.
2. Serwer administracyjny musi mieć możliwość ustawienia powiadomień dla użytkownika końcowego, w przypadku złamania reguł ustawionych w modułach związanymi z ochroną DLP. W powiadomieniu administrator musi posiadać możliwość określenia własnej grafiki, kontaktowego adresu e-mail oraz odnośnika do polityki bezpieczeństwa organizacji.
3. Oprogramowanie musi posiadać możliwości audytu stacji roboczych/użytkowników w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, ruch sieciowy, wysyłane oraz odebrane wiadomości e-mail oraz wykonane czynności na plikach.
4. Administrator musi posiadać możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji oraz typów plików.
5. Administrator musi posiadać możliwość filtrowania oraz sortowania zebranych danych. Tak odfiltrowane dane, administrator może zapisać w postaci plików PDF bądź XLS.
6. Konsola musi posiadać możliwość wysyłania powiadomień, jeśli dany użytkownik przekroczy określoną dopuszczalną ilość wysyłanych maili oraz w przypadku przekroczenia dopuszczalnej ilości wysyłanych danych do sieci w danym dniu lub tygodniu.
7. Serwer musi posiadać możliwość wysłania alertów, co najmniej za pośrednictwem wiadomości email.
8. Serwer administracyjny musi posiadać możliwość konfiguracji raportów w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, drukowane dokumenty, ruch sieciowy, wysyłane wiadomości e-mail oraz wykonywane czynności na plikach.
9. Raporty muszą być generowane w oparciu o wskazane stacje robocze, użytkowników bądź grupy w określonym przedziale czasu.
10. Raporty muszą być generowane do pliku PDF i/lub XLS, po podaniu lokalizacji zapisywanego pliku lub na wskazany adres(y) e-mail.
11. Serwer administracyjny musi posiadać wbudowany serwer SMTP udostępniony przez producenta oprogramowania.
12. Serwer administracyjny musi umożliwiać kategoryzację (tagowanie) plików na poziomie systemu plików lub na poziomie metadanych pliku.
13. Serwer administracyjny musi umożliwiać wykonanie zadania kategoryzacji (tagowania) plików, które już znajdują się na stacjach roboczych i zasobach sieciowych, ale również nowych plików, które powstaną na bazie już skategoryzowanych (otagowanych) plików.
14. Serwer administracyjny musi mieć możliwość kategoryzacji (tagowania) plików wrażliwych w oparciu o:
15. aplikacje, z której zostały utworzone,
16. lokalizację,
17. adres URL,
18. format pliku,
19. zawartość pliku.
20. Administrator musi mieć możliwość wyszukiwania danych osobowych na zasobach zarówno

lokalnych jak i sieciowych.

1. Dla plików skategoryzowanych (otagowanych), musi być możliwe utworzenie następujących reguł:
2. blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików, do lokalizacji na określonych dyskach lokalnych,
3. blokowanie oraz zezwalanie na zapisywanie, przenoszenie do lokalizacji na dyskach zewnętrznych z możliwością określenia białej oraz czarnej listy tych urządzeń,
4. blokowanie oraz zezwalanie na drukowanie na określonych drukarkach,
5. blokowanie oraz zezwalanie na zapisywanie i przenoszenie do lokalizacji sieciowej,
6. blokowanie oraz zezwalanie na wysyłanie za pośrednictwem klientów pocztowych z możliwością określenia białej i czarnej listy adresów i domen,
7. blokowanie oraz zezwalanie na wysyłanie do poczty webowej,
8. blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików do chmury, zarówno za pomocą przeglądarki internetowej jak i aplikacji, w oparciu o co najmniej poniższe usługi:

* Dropbox,
* Google Drive,
* SharePoint,
* OneDrive Business,
* OneDrive Personal.

1. blokowanie oraz zezwalanie na przesyłanie za pomocą komunikatorów,
2. blokowanie oraz zezwalanie na zapisywanie i przenoszenie danych poprzez usługę pulpitu zdalnego,
3. blokowanie oraz zezwalanie na wykonywanie zrzutów ekranowych, skopiowania zawartości oraz wirtualnego drukowania,
4. uruchomienie wybranego formatu pliku przez wskazaną przez administratora aplikacje,
5. Serwer administracyjny musi umożliwiać możliwość zabezpieczenia korzystania z niezaufanych repozytoriów GIT.
6. Każda z polityk musi posiadać możliwość ustawienia jej w trybie powiadomienia dla użytkownika.
7. Serwer administracyjny musi dawać możliwość klasyfikacji pliku (tagowania) użytkownikowi na stacji roboczej. Klasyfikacja musi odbywać się poprzez integrację z menu kontekstowym.
8. Klasyfikacja użytkownika musi posiadać opcję, która uniemożliwi użytkownikowi zmianę klasyfikacji na niższą.
9. Serwer administracyjny musi umożliwiać określenie białych i czarnych list zawierających

urządzenia pamięci masowej, drukarki fizycznych i sieciowych, lokalizacji sieciowych, adresów e- mail oraz domen, urządzeń przenośnych, firewire oraz bluetooth, które mogą być wykorzystywane do określenia reguł dostępu.

1. Serwer administracyjny musi posiadać funkcjonalność globalnego zablokowania lub zezwolenia na korzystanie z określonych folderów lokalnych, sieciowych, dysków o określonych literach oraz folderów synchronizacji z usługami chmury.
2. Serwer musi posiadać funkcjonalność skonfigurowania reguł dostępu dla urządzeń podłączanych do portu USB, urządzeń przenośnych, nośników optycznych CD/DVD, urządzeń Firewire, urządzeń podczerwieni, urządzeń Bluetooth, portów COM oraz LPT.
3. Serwer administracyjny musi posiadać możliwość zaszyfrowania całej powierzchni dysku w oparciu o funkcjonalność BitLocker z użyciem hasła lub modułu TPM.
4. Serwer administracyjny musi posiadać możliwość szyfrowania dysków zewnętrznych w oparciu o funkcjonalność BitLocker. Szyfrowanie oraz autoryzacja dla zaszyfrowanych nośników wymiennych musi być w pełni niezauważalna dla użytkownika.
5. Serwer administracyjny musi posiadać możliwość wyświetlenia i eksportu klucza odzyskiwania do zaszyfrowanych dysków oraz dysków wymiennych.
6. Serwer administracyjny musi posiadać możliwość wyszukiwania i ochrony plików w oparciu o ich zawartość, co najmniej o:
7. numery kart kredytowych,
8. numer PESEL,
9. numer polskiego dowodu osobistego,
10. polski numer paszportu,
11. wyrażenia regularne,
12. określone ciągi znaków,
13. numer IBAN.
14. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.
15. Weryfikacja zawartości pliku w czasie rzeczywistym musi posiadać funkcjonalność OCR (Optical Character Recognition).
16. System musi posiadać możliwość importu własnych słowników do wyszukiwania danych.
17. W przypadku incydentu bezpieczeństwa, system musi wykonać duplikat pliku lub wiadomości e- mail, w którym znajdują się dane wrażliwe (tzw. funkcjonalność „Shadow-copy”).
18. Serwer administracyjny musi posiadać możliwość wyznaczenia progu ilości wystąpień danych wrażliwych, od jakich zostanie uruchomione zadanie klasyfikacji (tagowania).
19. Serwer administracyjny musi posiadać możliwość integracji klasyfikacji danych, z modułem DLP dostępnym na rozwiązaniu FortiGate.
20. Serwer administracyjny musi umożliwiać eksport logów do rozwiązania FortiSIEM.
21. Serwer administracyjny musi umożliwiać eksport identyfikatorów oznaczonych plików do rozwiązania FortiMail, które będzie w stanie kontrolować przesyłanie tak oznaczonych plików.
22. Serwer administracyjny musi umożliwiać integrację z Office365. Integracja musi pozwalać na:
23. audyt i logowanie wiadomości e-mail,
24. audyt i logowanie operacji na plikach,
25. wprowadzanie polityk zabezpieczeń do wiadomości e-mail.
26. System musi umożliwiać integrację z narzędziami analitycznymi tj. Power BI, Tabeau).
27. Serwer administracyjny musi posiadać konsolę dostępną z poziomu przeglądarki internetowej, służącą do raportowania i zarządzania stacjami roboczymi i urządzeniami mobilnymi.
28. Konsola musi wyświetlać informacje na temat bezpieczeństwa danych, produktywności pracowników oraz utylizacji sprzętu które są podzielone na:
29. Bezpieczeństwo danych:

* Przegląd informacji o incydentach bezpieczeństwa.
* Przegląd danych przychodzących.
* Przegląd danych wychodzących.
* Przegląd informacji z Office365 które dotyczą m.in. pobierania, współdzielenia oraz lokalnego dostępu do plików.
* Podłączane/odłączane urządzenia przenośne.

1. Produktywność:

* Przegląd informacji na temat produktywności użytkowników.
* Aktywność użytkowników podczas przeglądania stron WWW oraz korzystania z aplikacji.
* Trendy.

1. Eksploatacja sprzętu:

* Przegląd informacji na temat eksploatacji sprzętu komputerowego.
* Eksploatacja sprzętu komputerowego, najbardziej nieaktywne komputery.
* Eksploatacja drukarek.
* Eksploatacji sieci.

1. Konsola webowa musi posiadać możliwość konfiguracji/zmiany domyślnego serwera SMTP.
2. Konsola webowa musi umożliwiać weryfikację wersji zainstalowanego oprogramowania klienta wraz z możliwością aktualizacji do nowej wersji lub dezaktywacji tego oprogramowania.
3. Konsola webowa musi umożliwiać wygenerowanie raportu w postaci pliku DOCX, który zawiera informacje:

* plików przenoszonych na nośniki USB i inne urządzenia przenośne,
* plików przesłanych za pomocą wiadomości e-mail,
* plików przesłanych za pomocą poczty webowej,
* plików przesłanych do Internetu,
* plików wysłanych za pomocą komunikatorów,
* plików przesłanych na dyski chmurowe,
* analiza sposobu korzystania z aplikacji,
* analiza korzystania z Internetu,
* analiza wykorzystania porali do poszukiwania pracy.

1. **UPS – 6 szt.**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa elementu, parametru lub cechy** | **Opis wymagań** |
|  | Moc pozorna | 650 VA |
|  | Moc rzeczywista | 400 W |
|  | Układ zaawansowanej ochrony przeciwprzepięciowej (ASR) | Tak |
|  | Czas przełączenia na baterię | 5 ms |
|  | Liczba, typ gniazd wyj. z podtrzymaniem zasilania i ochroną przepięciową | 3 x FR |
|  | Liczba, typ gniazd wyj. z ochroną przepięciową | 1 x FR |
|  | Funkcja EcoControl | 1 gniazdo sterowane EcoControl (automatyczna dezaktywacja nieczynnych urządzeń peryferyjnych) |
|  | Typ gniazda wejściowego | IEC320 C14 (10A) |
|  | Czas podtrzymania dla obciążenia 70% | 5 min |
|  | Czas podtrzymania przy obciążeniu 50% | 9 min |
|  | Napięcie znamionowe wejściowego | 230 V |
|  | Tolerancja napięcia wejściowego | 184 V – 264 V (regulacja 161 V – 284 V) |
|  | Częstotliwość znamionowa | 50/60 Hz auto-selekcja |
|  | Tolerancja częstotliwości | 46 – 70 Hz |
|  | Napięcie znamionowe wyjściowe | 230 V (domyślnie), 220/240 V |
|  | Zakres zmian napięcia wyjściowego | +6/-10% napięcia nominalnego |
|  | Baterie wymieniane przez użytkownika | Tak |
|  | Baterie wewnętrzne o pojemności | 1 x 7Ah 12V |
|  | Porty komunikacji | USB, HID |
|  | Ochrona linii danych | Tel., Fax, Modem, Internet i Ethernet |
|  | Ochrona przepięciowa | Tak (zgodnie z  IEC 61643-1) 525 J |
|  | Panel sterowania diodowy | min. 2 diody LED   •  stan ostrzegawczy/awaria   •  stan przeciążenia na gniazdach z podtrzymaniem bateryjnym |
|  | Alarmy dźwiękowe | •  awaria UPSa |
| •  przeciążenie UPSa |
| •  niski stan naładowania baterii |
|  | Przyciski | •  Przycisk podświetlany ON/OFF LED załączania/ wyłączenia gniazd wyjściowych z podtrzymaniem bateryjnym |
|  | Kolor | Czarny |
|  | Typ obudowy | Uniwersalna Tower/Rack (możliwość instalacji pionowej, poziomej oraz w szafie Rack 19") |
|  | Wyposażenie standardowe | •  kabel USB |
| •  oprogramowanie na CD |
| •  1 x kabel zasilający zakończony wtykiem FR (PL) |
| •  instrukcja obsługi w języku polskim |
|  | Dołączone oprogramowanie | Do bezpiecznego zamykania systemów operacyjnych przy wyczerpaniu baterii kompatybilne z: Windows 7 / Vista/XP, Mac X OS, Linux |
|  | Maksymalna szerokość | 81 mm |
|  | Maksymalna wysokość | 263 mm |
|  | Maksymalna głębokość | 235 mm |
|  | Maksymalny ciężar | 3,6 kg |
|  | Cechy | Brak wentylatora, cicha praca, konstrukcja energooszczędna |
|  | Zimny start | Tak |
|  | Uruchomienie z baterii | Tak |
|  | Ochrona przed przeładowaniem | Tak |
|  | Gwarancja producenta 24 miesiące | Tak |
|  | Certyfikat CE | Tak |

1. **UPS – 6 szt.**

|  |  |  |
| --- | --- | --- |
| Lp. | Nazwa elementu, parametru lub cechy | Opis wymagań |
| 1 | Moc pozorna | 1200 VA |
| 2 | Moc rzeczywista | 750 W |
| 3 | Układ zaawansowanej ochrony przeciwprzepięciowej (ASR) | Tak |
| 4 | Czas przełączenia na baterię | 5 ms |
| 5 | Liczba, typ gniazd wyj. z podtrzymaniem zasilania i ochroną przepięciową | 4 x Schuko (FR) |
| 6 | Liczba, typ gniazd wyj. z ochroną przepięciową | 4 x Schuko (FR) |
|  | Funkcja EcoControl | 1 gniazdo sterowane EcoControl (automatyczna dezaktywacja nieczynnych urządzeń peryferyjnych) |
| 7 | Typ gniazda wejściowego | Sznur sieciowy z wtykiem Euroshuko |
| 8 | Czas podtrzymania dla obciążenia 70% | 6 min |
| 9 | Czas podtrzymania przy obciążeniu 50% | 11 min |
| 10 | Napięcie znamionowe wejściowego | 230 V |
| 11 | Tolerancja napięcia wejściowego | 184 V – 264 V (regulacja 161 V – 284 V) |
| 12 | Częstotliwość znamionowa | 50/60 Hz auto-selekcja |
| 13 | Tolerancja częstotliwości | 46 – 70 Hz |
| 14 | Napięcie znamionowe wyjściowe | 230 V (domyślnie), 220/240 V |
| 15 | Zakres zmian napięcia wyjściowego | Jak ustawiony zakres napiecia wejsciowego |
| 16 | Baterie wymieniane przez użytkownika | Tak |
| 17 | Baterie wewnętrzne o pojemności | 2 x 9Ah 12V |
| 18 | Porty komunikacji | USB, HID |
| 19 | Ochrona linii danych | Tel., Fax, Modem, Internet i Ethernet |
| 20 | Ochrona przepięciowa | Tak (zgodnie z  IEC 61643-1) 525 J |
| 21 | Panel sterowania diodowy | min. 2 diody LED   •  stan ostrzegawczy/awaria   •  stan przeciążenia na gniazdach z podtrzymaniem bateryjnym |
| 22 | Alarmy dźwiękowe | •  awaria UPSa   •  przeciążenie UPSa   •  niski stan naładowania baterii |
| 23 | Przyciski | •  Przycisk podświetlany ON/OFF LED załączania/ wyłączenia gniazd wyjściowych z podtrzymaniem bateryjnym |
| 24 | Kolor | Czarny |
| 25 | Typ obudowy | Uniwersalna Tower/Rack (możliwość instalacji pionowej, poziomej oraz w szafie Rack 19") |
| 26 | Wyposażenie standardowe | •  kabel USB   •  oprogramowanie na CD   •  1 x kabel zasilający zakończony wtykiem FR (PL)   •  instrukcja obsługi w języku polskim |
| 27 | Dołączone oprogramowanie | Do bezpiecznego zamykania systemów operacyjnych przy wyczerpaniu baterii kompatybilne z: Windows 7 / Vista/XP, Mac X OS, Linux |
| 28 | Maksymalna szerokość | 81 mm |
| 29 | Maksymalna wysokość | 305 mm |
| 30 | Maksymalna głębokość | 312 mm |
| 31 | Maksymalny ciężar | 6,7 kg |
| 32 | Cechy | Brak wentylatora, cicha praca, konstrukcja energooszczędna |
| 33 | Zimny start | Tak |
| 34 | Uruchomienie z baterii | Tak |
| 35 | Ochrona przed przeładowaniem | Tak |
| 37 | Gwarancja producenta 24 miesiące | Tak |
| 38 | Certyfikat CE | Tak |

1. **UPS – 6 szt.**

|  |  |  |
| --- | --- | --- |
| Lp. | Nazwa elementu, parametru lub cechy | Opis wymagań |
|  | Moc pozorna | 1600 VA |
|  | Moc rzeczywista | 1000 W |
|  | Układ zaawansowanej ochrony przeciwprzepięciowej (ASR) | Tak |
|  | Czas przełączenia na baterię | 5 ms |
|  | Liczba, typ gniazd wyj. z podtrzymaniem zasilania i ochroną przepięciową | 4 x Schuko (FR) |
|  | Liczba, typ gniazd wyj. z ochroną przepięciową | 4 x Schuko (FR) |
|  | Funkcja EcoControl | 1 gniazdo sterowane EcoControl (automatyczna dezaktywacja nieczynnych urządzeń peryferyjnych) |
|  | Typ gniazda wejściowego | Sznur sieciowy z wtykiem Euroshuko |
|  | Czas podtrzymania dla obciążenia 70% | 6 min |
|  | Czas podtrzymania przy obciążeniu 50% | 11 min |
|  | Napięcie znamionowe wejściowego | 230 V |
|  | Tolerancja napięcia wejściowego | 184 V – 264 V (regulacja 161 V – 284 V) |
|  | Częstotliwość znamionowa | 50/60 Hz auto-selekcja |
|  | Tolerancja częstotliwości | 46 – 70 Hz |
|  | Napięcie znamionowe wyjściowe | 230 V (domyślnie), 220/240 V |
|  | Zakres zmian napięcia wyjściowego | Jak ustawiony zakres napiecia wejsciowego |
|  | Baterie wymieniane przez użytkownika | Tak |
|  | Baterie wewnętrzne o pojemności | 2 x 9Ah 12V |
|  | Porty komunikacji | USB, HID |
|  | Ochrona linii danych | Tel., Fax, Modem, Internet i Ethernet |
|  | Ochrona przepięciowa | Tak (zgodnie z  IEC 61643-1) 525 J |
|  | Panel sterowania diodowy | min. 2 diody LED |
| •  stan ostrzegawczy/awaria |
| •  stan przeciążenia na gniazdach z podtrzymaniem bateryjnym |
|  | Alarmy dźwiękowe | •  awaria UPSa |
| •  przeciążenie UPSa |
| •  niski stan naładowania baterii |
|  | Przyciski | •  Przycisk podświetlany ON/OFF LED załączania/ wyłączenia gniazd wyjściowych z podtrzymaniem bateryjnym |
|  | Kolor | Czarny |
|  | Typ obudowy | Uniwersalna Tower/Rack (możliwość instalacji pionowej, poziomej oraz w szafie Rack 19") |
|  | Wyposażenie standardowe | •  kabel USB |
| •  oprogramowanie na CD |
| •  1 x kabel zasilający zakończony wtykiem FR (PL) |
| •  instrukcja obsługi w języku polskim |
|  | Dołączone oprogramowanie | Do bezpiecznego zamykania systemów operacyjnych przy wyczerpaniu baterii kompatybilne z: Windows 7 / Vista/XP, Mac X OS, Linux |
|  | Maksymalna szerokość | 81 mm |
|  | Maksymalna wysokość | 305 mm |
|  | Maksymalna głębokość | 312 mm |
|  | Maksymalny ciężar | 7,8 kg |
|  | Cechy | Brak wentylatora, cicha praca, konstrukcja energooszczędna |
|  | Zimny start | Tak |
|  | Uruchomienie z baterii | Tak |
|  | Ochrona przed przeładowaniem | Tak |
|  | Gwarancja producenta 24 miesiące | Tak |
|  | Certyfikat CE | Tak |

1. **UPS – 2 szt.**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa elementu, parametru lub cechy** | **Opis wymagań** |
| 1 | Moc pozorna | 3000VA |
| 2 | Moc rzeczywista | 3000W |
| 3 | Topologia (klasyfikacja IEC 62040-3) | Podwójna konwersja on-line z korekcją wejściowego współczynnika mocy systemu (PFC) |
| 4 | Sprawność przy pracy normalnej (100% obc.) | <94% |
| 5 | Sprawność w trybie podwyższonej sprawności (100% obc.) | >98% |
| 6 | Współczynnik mocy | 1 |
| 7 | Czas przełączenia na baterię | 0 ms |
| 8 | Możliwość pracy równoległej | tak |
| 9 | Liczba, typ gniazd wyjściowych | 8 gniazd IEC C13 (10A) + 2 gniazda IEC C19 (16A), w tym 2 zarządzalne grupy wraz z pomiarem zużytej energi |
| 10 | Typ gniazda wejściowego | 1 IEC C20 (16A) lub blok zacisków w wersji HotSwap MBP HW |
| 11 | Czas podtrzymania dla 100% obciążenia dla pf=1 | 3 min |
| 12 | Czas podtrzymania przy 50% obciążenia dla pf=1 | 10 min |
| 13 | Dodatkowe bateriie | Możliwość dołożenia maksymalnie 4 zewnętrznych modułow bateryjnych |
| 14 | Napięcie znamionowe | 200/208/220/230/240 V |
| 15 | Tolerancja napięci prostownika | 176V – 276 V (100-276V przy <33% obciążeniu) |
| 16 | Częstotliwość znamionowa | 50/60 Hz autodetekcja |
| 17 | Tolerancja częstotliwości | 40– 70 Hz |
| 18 | Kształt napięcia | Sinusoidalny |
| 19 | Napięcie znamionowe wyjściowe | 230 V (domyślnie) / możliwość wyboru 200/208/220/240 V |
| 20 | Zakres zmian napięcia | +/-1% napięcia nominalnego |
| 21 | Częstotliwość wyjściowa | 50/60 Hz +/-0,5% |
| 22 | Współczynnik szczytu | 3:1 |
| 23 | Dopuszczalny zakres współczynnika mocy obc. Liniowego | 0,5 indukcyjny - 0,5 pojemnościowy |
| 24 | Baterie wymieniane przez użytkownika "na gorąco" | Tak |
| 25 | Ochrona przed przeładowaniem | Tak (ograniczenie prądu ładowarki, wyłączenie ładowarki / alarm) |
| 26 | Ochrona przed głębokim rozładowaniem | Tak |
| 27 | Okresowy automatyczny test baterii | Tak |
| 28 | System zarządzania pracą baterii | System nieciągłego ładowania baterii. Do oferty dołączyć należy opis algorytmu ładowania nieciągłego baterii. W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni. Opis powinien być materiałem firmowym producenta lub musi być przez niego potwierdzony. |
| 29 | Zdolność zwarciowa | 90A |
| 30 | Możliwość uruchomienia bez napięcia w sieci | Tak |
| 31 | Baterie wewnętrzne o pojemności nie mniejszej niż | 9Ah 12V, minimum 6 szt. |
| 32 | Czas ładowania baterii do poziomu 90% | < 1,5 godz. do 90% pojemności użytkowej |
| 33 | Interfejs komunikacyjny | •  USB |
| • RS232 DB-9 żeński (HID) |
| • 1 blok mini-zacisków dla zdalnego załączania/wyłączania |
| • 1 blok mini-zacisków do zdalnego wyłączania |
| • 1 blok mini-zacisków przekaźnika wyjściowego |
| 34 | Panel sterowania z wyświetlaczem LCD | • Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPSa). Dostarcza informacji o : stanie pracy urządzenia, stanie obciążenia, pomiarach i ustawieniach.    Funkcje ustawień i odczytów: lokalne, wyjścia (napięcie wyjściowe ,  częstotliwość wyjściowa), baterii (test baterii), pomiary i dane (numer seryjny,napięcie i częstotliwość wejściowa i wyjściowa, poziom obciążenia, pozostały czas podtrzymania, wydajność, zużycie energii). |
| • Poziomy rząd przycisków sterowania |
| • Poziomy rząd wskaźników stanu : 4 LED |
| • Sygnalizator akustyczny |
| 35 | Sygnały akustyczne | • Awaria |
| • Niski stan naładowania baterii |
| • Przeciążenie |
| • Serwis |
| 36 | Przyciski sterujące i wskaźniki diodowe LED | • Przycisk Escape (anulowanie) |
| • Przyciski funkcyjne (przewijanie w górę i w dół) |
| • Przycisk Enter (potwierdzający) |
| • Przycisk ON/OFF załączenia i wyłączenia |
| • LED trybu zasilania z siec i(kolor zielony) |
| • LED trybu baterii (kolor żółty) |
| • LED usterki (kolor czerwony) |
| • LED w trybie obejścia (kolor pomarańczowy) |
| 37 | Kolor | Czarny RAL 9005 |
| 38 | Typ obudowy | Uniwersalna Tower/Rack 2U |
| 39 | Wyposażenie standardowe | UPS, instrukcja obsługi(CD), instrukcja bezpieczeństwa, instrukcja szybkiego montażu |
| 1 x kabel szeregowy RS-232, |
| 1 x kabel komunikacyjny USB |
| 1 x kable wyjściowe IEC 16A |
| 2 x kable wyjściowe IEC 10A |
| uchwyty kablowe |
| 1 x zestaw szyn montażowych 19’ |
| podstawki do montażu wieżowego |
| 40 | Dołączone oprogramowanie | Tak, monitorujące i zarządzające UPS, umożliwiające automatyczne zamykanie serwerów zasilanych z systemu i pracujących pod kontrolą systemów operacyjnych:    - Windows:     7 / 8 / 2008 / Vista / 2003 / XP   - Microsoft SCVMM 2012   - Linux:   Debian GNU Linux: Lenny,   SUSE/Novell: SLES 11, OpenSUSE 11.2,    Redhat Enterprise Linux: RHEL 5.3, 5.4, 5.5, Fedora core 12    Ubuntu: 10.04   - VMWare: vCenter / ESXi 5.1    - Citrix XEN 6.0 |
| 41 | Zgodność ze standardem Energy Star | Tak |
| 42 | Maksymalna szerokość | 440 mm |
| 43 | Maksymalna wysokość | 86,5 mm |
| 44 | Maksymalna głębokość | 605 mm |
| 45 | Maksymalny ciężar | 27,4 kg |
| 46 | Poziom hałasu w odl. 1m | <47 dBA dla pracy normalnej |
| 47 | Znaki bezpieczeństwa | CE, C-Tick, IEC/EN 62040-1, IEC/EN 62040-2: Kat. C1, IEC/EN 62040-3 |
| 48 | Gwarancja producenta | 3 lata na elektronikę, 2 lata na baterie akumulatorów |

1. **Oprogramowanie do wykonywania kopii zapasowych – 10 licencji uniwersalnych.**

Licencja musi być na bezterminowa, bez żadnych dodatkowych opłat a wsparcie na minimum 12 miesięcy.

|  |  |
| --- | --- |
| Lp. | Minimalne wymagania Zamawiającego |
| 1. 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-recovery-solutions 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. |
| 1. 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 |
| 1. 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. |
|  | Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy. |
|  | Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) |
|  | Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard. |
|  | Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS. |
|  | Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN. |
|  | Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji. |
|  | Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO. |
|  | Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik |
|  | Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding) |
|  | Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN) |
| 1. 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 |
| 1. 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. |
| 1. 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 |
| 1. 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 |
|  | System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji od 10.x do 10.4 |
| 1. 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. migawek-sierot (orphaned snapshots) |
|  | System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie |

1. **Oprogramowanie do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych – 60 licencji:**

Oprogramowanie musi spełniać następujące wymagania w zakresie zarządzania zasobami IT:

* Zarządza wszystkimi zasobami, za które odpowiada dział IT.
* Pokazuje szczegółowe informacje i ewidencję czynności wykonanych na zasobach w trakcie całego cyklu życia.
* Ma możliwość definiowania statusów i pól oraz generowanie protokołu przekazania sprzętu.
* Potrafi przypisać dokument do wielu zasobów.
* Generuje dokumenty na podstawie szablonów.
* Automatycznie numeruje dodawane zasoby i dokumenty według zdefiniowanego wzorca numeracji.
* Posiada system zarządzania aplikacjami i licencjami.
* System identyfikuje realne zużycie licencji.
* Rozlicza licencje według użytkownika, urządzenia, numeru seryjnego lub na podstawie wersji zainstalowanej aplikacji.
* Posiada historię użycia konkretnych licencji oprogramowania.
* Oprogramowanie robi audyt inwentaryzacji sprzętu i oprogramowania.
* Posiada zdalny dostęp do managera plików z możliwością usuwania plików użytkownika.
* System zbiera informacje o wpisach rejestrowych, plikach, archiwach oraz konfiguracji sprzętowej konkretnych stacji roboczych.
* Zarządza instalacjami/dezinstalacjami oprogramowania w oparciu o menadżera pakietów MSI.
* Ma możliwość archiwizacji i porównywania audytów.
* Monitoruje harmonogram zadań Windows.

Oprogramowanie musi spełniać następujące wymagania w zakresie zarządzania użytkownikami:

* Zarządza użytkownikami, bazując na grupach i politykach bezpieczeństwa.
* Przyporządkowuje dane do konkretnego użytkownika.
* Blokuje niebezpieczne domeny WWW.
* Chroni pracowników przed wiadomościami phishingowymi i atakami APT.
* Rozróżnia wykonywane czynności na poszczególnych urządzeniach.
* Posiada rejestr naruszeń blokad, który agreguje informacje o próbach dostępu do blokowanych stron.
* Posiada dedykowane alarmy dla wszystkich rodzajów incydentów zbieranych przez rejestr naruszeń blokad.
* Ma możliwość blokowania uruchamianych aplikacji.
* Może korzystać z zewnętrznych list blokowania stron takich jak listę ostrzeżeń CERT.PL
* Monitoruje wiadomości e-mail.
* Zbiera informacje o odwiedzanych stronach WWW.
* Monitoruje użycie łącza przez poszczególnych użytkowników.
* Zarządza regułami blokowania aplikacji i stron WWW.
* Ma możliwość wykrywania podejrzanych aktywności użytkowników za pomocą mechanizmu wykrywania jigglerów.

Oprogramowanie musi spełniać następujące wymagania w zakresie pomocy technicznej:

* Posiada tworzenie zgłoszeń serwisowych i zarządza nimi.
* Ma możliwość wskazania osób, które muszą zaakceptować zgłoszenie.
* Tworzy ścieżki akceptacji na podstawie kategorii przypisanej do zgłoszenia.
* Posiada możliwość stworzenia listy aplikacji bezpiecznych do samodzielnej instalacji przez użytkownika.
* Może przetwarzać zgłoszenia w trybie anonimowym.
* Posiada rozbudowany system raportów.
* Ma bazę zgłoszeń z rozbudowaną wyszukiwarką.
* Posiada wewnętrzny komunikator z możliwością przesyłania plików oraz przydzielania uprawnień.
* Oprogramowanie posiada zdalny dostęp do komputerów z możliwością blokowania myszy/klawiatury.
* Ma równoczesny zdalny dostęp kilku administratorów do jednego agenta.
* Posiada integrację bazy użytkowników z Active Directory.
* Zarządza kontami lokalnych użytkowników Windows.

Oprogramowanie musi spełniać następujące wymagania w zakresie kontroli dostępu do danych:

* Automatycznie nadaje użytkownikom domyślną politykę monitorowania i bezpieczeństwa.
* Monitoruje operacje na plikach z zasobów sieciowych udostępnianych przez urządzenia.
* Zabezpiecza sieć przed wirusami instalującymi się automatycznie z pendrive’ów lub dysków zewnętrznych.
* Posiada integrację z Windows Defender, Windows Firewall i Windows Bitlocker.
* Alarmy o podłączonym urządzeniu obcym.
* Możliwość zdalnego szyfrowania dysków.
* Zbiera informacje o urządzeniach podłączonych do danego komputera.
* Posiada bazę wszystkich urządzeń podłączonych do komputerów w sieci.
* Posiada historię połączeń i operacji na urządzeniach przenośnych.
* Zarządza prawami dostępu.
* Ustawia reguły dla całej sieci.

Oprogramowanie musi spełniać następujące wymagania w zakresie zarządzania czasem:

* Posiada statystyki czasu spędzonego przed komputerem.
* Ma możliwość tworzenia grup złożonych z dowolnych pracowników w firmie.
* Posiada listę aplikacji używanych przez poszczególnych pracowników .
* Dodawanie dostępu do odpowiednich aplikacji dla danych grup pracowników.
* Możliwość oznaczania stron internetowych i aplikacji jako produktywne, neutralne lub nieproduktywne.
* Posiada listę kontaktów w danej organizacji.
* Podgląd zrzutu ekrany wybranego użytkownika dostępny dla menadżerów i administratorów.

1. **Wdrożeniowe oprogramowania przeciwdziałającego wyciekowi danych (DLP)**

Usługi wdrożeniowe oprogramowania przeciwdziałającego wyciekowi danych (DLP), którego głównym celem jest zabezpieczenie przed utratą lub nieautoryzowanym dostępem do informacji poufnych. Oprogramowanie to ma zostać zainstalowane na serwerze działającym pod kontrolą systemu Windows Server co najmniej w wersji 2016 oraz powinno być obsługiwane za pomocą dwóch konsol: aplikacyjnej i webowej, w celu ułatwienia zarządzania systemem.

1. Wykonawca przeprowadzi analizę wymagań Zamawiającego, zaczynając od zebrania wymagań od różnych zespołów w organizacji, aby określić, jakie funkcje i moduły oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych będą najbardziej przydatne.
2. Wykonawca przeprowadzi planowanie wdrożenia w oparciu o przeprowadzoną analizę, uwzględniając harmonogram, zasoby, zadania.
3. Wykonawca przygotuje środowisko wirtualne, upewniając się, że wszystkie wymagania stawiane przez oprogramowanie zostały spełnione, włączając w to odpowiednie zasoby, konfigurację systemu operacyjnego oraz konfigurację sieciową niezbędną do prawidłowego działania oprogramowania.
4. Wykonawca wykona konfigurację baz danych niezbędnych do wdrożenia oprogramowania, włączając to prawidłowe połączenie pomiędzy oprogramowaniem a bazą danych.
5. Wykonawca zainstaluje oprogramowanie przeciwdziałającego wyciekowi danych.
6. Wykonawca wykona integrację z istniejącymi systemami w środowisku Zamawiającego, w tym z kontrolerem domeny oraz przygotuje konta usługi oprogramowania, włączając w to konfigurację uprawnień dla konta usługi. Wykonawca przeprowadzi testy wykonanej integracji w celu upewnienia się, że informacje są poprawnie synchronizowane między oprogramowaniem a istniejącymi systemami w środowisku Zamawiającego, w tym z kontrolerem domeny oraz czy synchronizacja użytkowników, grup i innych obiektów z kontrolera domeny do oprogramowania działa w sposób prawidłowy. Wykonawca będzie monitorował i utrzymywał integrację między oprogramowaniem przez cały okres trwania wdrożenia.
7. Wykonawca uruchomieni i skonfiguruje konsolę zarządzającą, wprowadzi klucz dostępowy i usunie dane demonstracyjne.
8. Wykonawca przeprowadzi instruktaż w zakresie prawidłowej instalacji agentów niezbędnych do prawidłowego działania oprogramowania, uwzględniając utworzenie odpowiednich grup i polityk wdrożeniowych dla agentów. Po zakończonej instalacji agentów, Wykonawca przeprowadzi testy poprawności instalacji i komunikacji agentów z serwerem oprogramowania.
9. Wykonawca przeprowadzi testy instalacji w celu upewnienia się, że instalacja oprogramowania przebiegła bez problemów i wszystkie komponenty zostały poprawnie zainstalowane na serwerze oraz urządzeniach końcowych.
10. Wykonawca wykona konfigurację kategorii danych i danych wrażliwych oraz zdefiniuje wykrywanie kategorii:

* Numery kart kredytowych
* Numery IBAN
* Numery dowodów osobistych
* Polski numer paszportu
* Numer PESEL

1. Wykonawca skonfiguruje alerty związane z usługami oraz zabezpieczeniem DLP oraz przetestuje poprawność ich działania na danych testowych.
2. Wykonawca skonfiguruje zadania archiwizacji danych oraz usuwania starych wpisów z bazy danych.
3. Wykonawca przetestuje działanie polityk i wprowadzi ich aktualizację w przypadku wykrycia braku ich skutecznego działania.
4. Wykonawca wygeneruje z prawidłowo wdrożonego oprogramowania raport audytu bezpieczeństwa i przeprowadzi analizę aktywności użytkowników oraz przepływu informacji w organizacji.
5. Wykonawca przeprowadzi testy monitorowania i raportowania, weryfikując czy raporty generowane przez oprogramowanie zawierają poprawne i aktualne informacje.
6. Wykonawca przeprowadzi testy wydajnościowe w celu upewnienia się, że infrastruktura oprogramowania działa płynnie i efektywnie, nawet przy dużej liczbie urządzeń i użytkowników.
7. Wykonawca przeprowadzi testy przywracania awaryjnego, włączając w to procedury przywracania awaryjnego w celu upewnienia się, że w razie konieczności można szybko przywrócić działanie systemu oprogramowania sieciowych po awarii.
8. **Wdrożenie klastra serwerów**

Krok 1: Planowanie i Przygotowanie

* Określenie wymagań dotyczących infrastruktury, w tym sprzętu, sieci i przechowywania.
* Wybranie serwerów, które zostaną użyte jako węzły klastra. Upewnij się, że są one zgodne z wymaganiami wybranego oprogramowania.
* Skonfigurowanie łącza sieciowego i przestrzeni dyskowej, aby zapewnić odpowiednią przepustowość i pojemność.
* Zainstalowanie systemu operacyjnego na każdym węźle klastra.

Krok 2: Instalacja roli oprogramowania do wirtualizacji

* Instalacja odpowiedniej roli za pomocą menedżera serwerów lub PowerShell.
* Konfiguracja ustawień sieciowych i przechowywania na węzłach klastra, tak aby były zgodne z wymaganiami projektu.

Krok 3: Konfiguracja klastra

* Uruchomienie kreatora konfiguracji klastra w menedżerze serwerów na jednym z węzłów.
* Dodanie pozostałych węzłów klastra do konfiguracji.
* Konfiguracja ustawień klastra, takie jak nazwa klastra, adresy IP i konfiguracja przechowywania współdzielonego.

Krok 4: Konfiguracja wysokiej dostępności klastra

* Włączenie funkcji wysokiej dostępności dla maszyn wirtualnych na klastrze.
* Konfiguracja ustawień zapasowych dla klastra, aby zapewnić ochronę przed awariami węzłów.

Krok 5: Tworzenie i Zarządzanie Maszynami Wirtualnymi

* Utworzenie nowych maszyn wirtualnych na klastrze z wykorzystaniem oprogramowania do wirtualizacji.
* Konfiguracja ustawień maszyn wirtualnych, takich jak liczba procesorów, ilość pamięci i przypisywanie zasobów sieciowych.
* Zarządzanie maszynami wirtualnymi, monitorowanie ich wydajności i wykonywanie niezbędnych operacji konserwacyjnych jest kluczowe w zapewnieniu prawidłowo funkcjonującego środowiska wirtualnego uruchomionego w klastrze.

Krok 6: Testowanie i Monitorowanie

* Testowanie działania klastra, w tym jego zdolność do migracji wirtualnej i przywracania po awariach.
* Konfiguracja narzędzi monitorujących, w celu śledzenia wydajności i dostępności klastra oraz maszyn wirtualnych.
* Regularnie przeglądanie logów i raportów, w celu szybkiego reagowania na ewentualne problemy.

1. **Wdrożenie kontrolera domeny (AD):**

Etap 1: Analiza Wstępna i Planowanie Wdrożenia

1.1. Analiza Stanu Obecnego:

* Ocena istniejącej infrastruktury IT, w tym systemów operacyjnych, sieci, aplikacji i baz danych.
* Identyfikacja istniejących rozwiązań zarządzania tożsamościami i bezpieczeństwem oraz ich ewentualnych ograniczeń.

1.2. Wymagania Organizacyjne i Techniczne:

* Konsultacje z interesariuszami w celu zrozumienia potrzeb biznesowych i oczekiwań dotyczących infrastruktury IT.
* Identyfikacja wymagań dotyczących zarządzania tożsamościami użytkowników, zasobami sieciowymi i politykami bezpieczeństwa.

1.3. Opracowanie Planu Wdrożenia:

* Sporządzenie szczegółowego planu projektowego uwzględniającego harmonogram, zadania, zasoby i odpowiedzialności.
* Określenie struktury domen, schematu nazewnictwa i strategii replikacji dla środowiska Active Directory.

Etap 2: Instalacja i Konfiguracja Środowiska Active Directory

2.1. Instalacja Roli AD DS:

* Konfiguracja serwera Windows Server jako kontrolera domeny, włączając rolę Active Directory Domain Services.

2.2. Konfiguracja DNS:

* Ustawienie serwera DNS zgodnie z wymaganiami Active Directory.
* Konfiguracja strefy forward i reverse DNS dla domeny.

2.3. Tworzenie Dominy lub Integracja:

* Utworzenie nowej domeny Active Directory lub integracja z istniejącymi domenami w środowisku.

2.4. Konfiguracja Zasad Replikacji:

* Określenie i skonfigurowanie zasad replikacji między kontrolerami domeny w różnych lokalizacjach.

Etap 3: Strukturyzacja i Organizacja Domeny

3.1. Projektowanie Struktury Organizacyjnej:

* Tworzenie jednostek organizacyjnych (OU) odpowiadających strukturze organizacyjnej firmy.
* Utworzenie kont użytkowników, grup i zasobów oraz ich odpowiednie uporządkowanie w hierarchii.

3.2. Konfiguracja Polityk Grupowych (GPO):

* Ustanowienie zasad dostępu, konfiguracji użytkowników i komputerów za pomocą GPO.
* Implementacja polityk bezpieczeństwa dotyczących haseł, dostępu i innych ustawień

Etap 4: Zabezpieczenie Active Directory

4.1. Wdrożenie Zaawansowanych Mechanizmów Zabezpieczeń:

* Konfiguracja zasad kont haseł, polityk blokowania kont, kontroli dostępu.
* Implementacja szyfrowania komunikacji i audytu zdarzeń w AD.

4.2. Konfiguracja Środków Obronnych:

* Wdrożenie mechanizmów zabezpieczeń przed atakami, w tym monitorowanie logów, wykrywanie zagrożeń i zapobieganie atakom.

Etap 5: Walidacja i Optymalizacja Konfiguracji

5.1. Testowanie Funkcjonalności i Bezpieczeństwa:

* Przeprowadzenie testów weryfikujących działanie i bezpieczeństwo środowiska AD.
* Identyfikacja i rozwiązywanie ewentualnych problemów lub luk w zabezpieczeniach.

5.2. Optymalizacja Wydajności:

* Optymalizacja konfiguracji AD w celu zapewnienia efektywności i wydajności działania.
* Integracja z istniejącymi systemami i aplikacjami w celu zapewnienia spójności działań.

Etap 6: Dokumentacja Techniczna

6.1. Sporządzenie Dokumentacji:

* Przygotowanie szczegółowej dokumentacji technicznej, zawierającej opisy konfiguracji, ustawień polityk, procedur bezpieczeństwa i architektury systemu.
* Dokumentacja będzie służyć jako punkt odniesienia dla administratorów IT i personelu technicznego.

Cel Końcowy Usługi

Finalizacja usługi zapewni pełne wdrożenie systemu Active Directory, skonfigurowane zgodnie z najlepszymi praktykami branżowymi, gotowe do efektywnego zarządzania środowiskiem IT. System będzie przygotowany do zapewnienia wysokiego poziomu bezpieczeństwa, stabilności operacyjnej i skalowalności, odpowiadając na bieżące oraz przyszłe potrzeby organizacji.

1. **Wdrożenie oprogramowania do wykonywania kopii zapasowych:**

1: Planowanie i Przygotowanie

* Określenie wymagań dotyczących backupu i replikacji, w tym ilość danych do przechowywania, czas przywracania, dostępność i inne czynniki.
* Weryfikacja posiadania odpowiedniej ilości przestrzeni dyskowej i zasobów sieciowych do przechowywania kopii zapasowych.
* Pobranie niezbędnego oprogramowania do wykonywania kopii zapasowych i przeczytanie jego dokumentacji.

2: Instalacja i Konfiguracja

* Uruchomienie instalatora wybranego oprogramowania do wykonywania kopii zapasowych na wybranym serwerze.
* Postępuj zgodnie z kreatorami instalacji, akceptując licencję, wybierając komponenty do zainstalowania i konfigurując ustawienia.
* Konfiguracja połączenia ze swoim środowiskiem wirtualizacji

3: Konfiguracja Backupu

* Konfiguracja planów backupu, określając harmonogramy, miejsca przechowywania i inne parametry.
* Wybranie, które maszyny wirtualne lub inne zasoby będą chronione za pomocą kopii zapasowych.
* Ustawienie retencji danych i polityki przechowywania, aby dostosować je do wymagań firmy.

4: Konfiguracja Replikacji (opcjonalnie)

* Konfiguracje odpowiedniego zadania replikacji, określając maszyny wirtualne źródłowe i docelowe, harmonogramy i inne parametry.
* Weryfikacja dostępności docelowego środowiska na przyjęcie replikowanych maszyn wirtualnych.

5: Testowanie i Wdrażanie

* Przetestowanie planów backupu i replikacji, aby upewnić się, że są one zgodne z oczekiwaniami i spełniają wymagania czasu przywracania.
* Wdrożenie skonfigurowanych i przetestowanych planów na produkcji, monitorując ich wydajność i skuteczność.

6: Monitorowanie i Administracja

* Regularne monitorowanie wykonywanych kopii zapasowych i replikacji, w celu weryfikacji ich poprawności i zgodności z planem.
* Weryfikacja raportów i dzienników zdarzeń oprogramowania do wykonywania kopii zapasowych, aby szybko reagować na jakiekolwiek problemy.

1. **Wdrożenie oprogramowania do monitorowania infrastruktury IT**

Przedmiotem zamówienia jest wdrożenie Oprogramowania do monitorowania infrastruktury IT, obejmującego szereg działań konfiguracyjnych i operacyjnych w celu dostosowania funkcjonalności oprogramowania do specyficznych potrzeb i wymagań organizacji zamawiającej.

1. Instalacja Oprogramowania:

   - Początkowa instalacja oprogramowania na dedykowanej maszynie zgodnie z wymaganiami producenta.

   - Konfiguracja bezpiecznego dostępu dla Administratorów.

2. Konfiguracja Systemu:

   - Ustawienie parametrów przechowywania danych.

   - Konfiguracja i uruchomienie automatycznych kopii zapasowych danych.

   - Wdrożenie polityki monitorowania oraz konfiguracja i instalacja Agenta na stacjach roboczych.

3. Monitorowanie Sieci:

   - Skanowanie sieci i klasyfikacja urządzeń.

   - Rekonfiguracja urządzeń sieciowych w zakresie komunikacji dla monitorowania.

4. Polityki Alarmów i Inwentaryzacji:

   - Konfiguracja polityk alarmów oraz inwentaryzacji sprzętu.

5. Konfiguracja Zasobów:

   - Ustawienie alarmowania dla określonych zasobów.

   - Zdefiniowanie zasad monitorowania, blokowania i widoczności agenta.

6. Zarządzanie Użytkownikami:

   - Definiowanie grup klasyfikacji aplikacji i stron.

   - Omówienie możliwości wykluczeń dla blokad domen i procesów.

7. DataGuard i HelpDesk:

   - Konfiguracja polityk monitorowania katalogów lokalnych użytkownika.

   - Definiowanie reguł dostępu dla nośników i zasady działania metryk SLA.

8. AdminCenter:

   - Prezentacja interfejsu, konfiguracja pulpitów i widżetów.

   - Omówienie możliwości udostępniania pulpitów innym administratorom.

Wymagania Sprzętowe:

Wymagania techniczne i infrastrukturalne do przygotowania przez Klienta obejmują:

- Maszyna pod Serwer: Zgodność z wymaganiami określonymi w dokumentacji producenta dostępnej online.

- Konfiguracja Sieciowa: Zapewnienie ruchu sieciowego dla serwera, w tym otwarcie portów (4436 dla komunikacji z agentami, 8080 dla HelpDesk SmartTime AdminCenter).

- Oprogramowanie Dodatkowe: Instalacja aktualizacji Windows na serwerze i stacjach roboczych, konfiguracja wykluczeń w oprogramowaniu antywirusowym.

- Kopie Zapasowe: Określenie miejsca składowania kopii zapasowych i częstotliwości ich wykonywania.

1. **Dostawa i wdrożenie oprogramowania typu SIEM:**

Zamawiający na potrzeby wdrożenia udostępni infrastrukturę na serwerach zwirtualizowanych,     
wg. specyfikacji uzgodnionych z Wykonawcą. Czynności związane z wdrożeniem systemu będącego przedmiotem umowy będzie wykonywał Wykonawca. Instalacja systemu przez Wykonawcę odbywać się będzie z wykorzystaniem środków komunikacji elektronicznej.

1. Funkcjonalności systemu.

* Monitorowanie występujących zdarzeń (logów) w trybie ciągłym.
* Zbieranie zdarzeń z serwerów wirtualnych, fizycznych, Active Directory, przełączników oraz innego rodzaju urządzeń, które są oraz zostaną podłączone do infrastruktury zamawiającego.
* Agregacja oraz korelacja logów.
* Wykrywanie ataków typu brute force na różne usługi.
* Wykrywanie i przeciwdziałanie złośliwemu oprogramowaniu.
* Analiza logów w oparciu o wbudowane reguły bezpieczeństwa.
* Konfiguracja oprogramowania do przechowywania logów z kluczowych zasobów przez okres 24 miesięcy zgodnie z rozporządzeniem KRI §21 pkt. 4 „Informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata.”
* Panel do wyszukiwania zdarzeń.

1. Wdrożenie systemu.

* Wykonawca będzie odpowiedzialny za instalację i konfigurację oraz optymalizację środowiska systemu w infrastrukturze Zamawiającego oraz opiekę serwisową i wsparcie techniczne przez okres 30 dni.

1. Wykonawca przeprowadzi instruktaż stanowiskowy dla Administratorów (zarządzających systemem), co najmniej w n/w zakresie:

* Przedstawienie architektury systemu.
* Omówienie procedur obsługi administracyjnej systemu;
* omówienie możliwości funkcjonalnych, zakresu dostępnych funkcji oraz ograniczeń systemu;
* przekazanie informacji na temat konfiguracji i zarządzania systemem;
* instruktaż stanowiskowy musi obejmować część teoretyczną i praktyczną.

1. **Wdrożenie XDR**

Krok 1: Instalacja i konfiguracja

* Pobranie oprogramowania: Należy pobrać najnowszą wersję oprogramowania XDR od wybranego dostawcy. Proces ten wymaga zalogowania się na platformie dostawcy i wybrania wersji kompatybilnej z infrastrukturą IT organizacji.
* Instalacja agentów: Agent XDR musi być zainstalowany na każdym urządzeniu, które ma być monitorowane. Może to obejmować serwery, stacje robocze i urządzenia mobilne. Instalacja może być realizowana manualnie lub automatycznie, za pomocą narzędzi do zdalnego zarządzania oprogramowaniem.
* Konfiguracja agentów: Po zainstalowaniu agentów, należy je odpowiednio skonfigurować, aby zapewnić ich komunikację z centralnym serwerem XDR. Wymaga to ustawienia parametrów takich jak adresy serwera, polityki przesyłania danych i interwały synchronizacji.
* Integracja z innymi systemami: XDR powinno być zintegrowane z istniejącymi systemami zabezpieczeń, takimi jak SIEM, systemy zarządzania identyfikatorami i dostępem (IAM) oraz inne narzędzia zabezpieczeń, aby zwiększyć efektywność wykrywania i reakcji na incydenty.

Krok 2: Testowanie i optymalizacja

* Testowanie funkcjonalności: Po konfiguracji, system XDR powinien być dokładnie przetestowany, aby upewnić się, że wszystkie komponenty funkcjonują prawidłowo. Testy powinny obejmować weryfikację zdolności do zbierania danych, przetwarzania zdarzeń i generowania alertów.
* Optymalizacja konfiguracji: Na podstawie wyników testów, konfiguracja systemu XDR może wymagać dostosowania. Należy zrewidować i zoptymalizować reguły i algorytmy wykrywania, aby lepiej dostosować je do specyficznych zagrożeń i środowiska operacyjnego organizacji.

1. **Szkolenia z wdrożonych rozwiązań**

Szkolenia będą trwały co najmniej 8 dni roboczych po 8 godzin każdy. Szkolenie jest dla 2 uczestników i każde z nich musi się zakończyć otrzymaniem certyfikatu potwierdzającego udział w szkoleniu.

* **Szkolenie z klastra serwerów**

1. Podstawy architektury i konfiguracji klastra serwerowego:

* Wprowadzenie do architektury klastra, omówienie komponentów i typów konfiguracji.
* Instalacja i konfiguracja węzłów klastra oraz ich integracja z siecią organizacji.
* Zasady tworzenia klastrów wysokiej dostępności (HA) oraz konfiguracja równoważenia obciążenia.

1. Zarządzanie zasobami i skalowalność:

* Konfiguracja zasobów w klastrze oraz dynamiczne przydzielanie pamięci i mocy obliczeniowej.
* Procedury skalowania klastra przez dodawanie i usuwanie węzłów oraz monitorowanie wydajności.
* Narzędzia do zarządzania zasobami i optymalizacji operacji IT.

1. Zapewnienie wysokiej dostępności i mechanizmy awaryjne:

* Konfiguracja mechanizmów failover oraz przywracania usług w przypadku awarii węzłów.
* Ćwiczenia z automatycznego przełączania obciążenia i zarządzania redundancją.
* Analiza rzeczywistych przypadków awarii oraz symulacje scenariuszy awaryjnych.

1. Bezpieczeństwo i polityki kopii zapasowych:

* Tworzenie polityk zabezpieczających przed zagrożeniami wewnętrznymi i zewnętrznymi.
* Konfiguracja automatycznych kopii zapasowych i planów przywracania danych.
* Praktyczne ćwiczenia z tworzenia kopii zapasowych w środowisku klastrowym.
* **Szkolenie z oprogramowania XDR**

1. Podstawy instalacji i konfiguracji systemu ochrony antywirusowej:

* Omówienie architektury systemu ochrony oraz jego komponentów.
* Praktyczne wskazówki dotyczące instalacji na różnych platformach (np. Windows, Linux, Android).
* Wstępna konfiguracja, w tym integracja z siecią firmową, ustawienia dostępu oraz tworzenie kont administracyjnych.
* Konfiguracja skanowania w czasie rzeczywistym, ochrona plików, sieci oraz zabezpieczenia poczty e-mail.
* Zarządzanie funkcjami dodatkowego zabezpieczenia, takimi jak blokowanie nieautoryzowanych urządzeń USB, funkcje anti-theft i ochrona danych w urządzeniach przenośnych.

1. Zaawansowana konfiguracja polityk bezpieczeństwa i zarządzanie politykami użytkowników:

* Tworzenie spersonalizowanych polityk bezpieczeństwa dostosowanych do struktury i potrzeb organizacji.
* Konfiguracja polityk dla różnych grup użytkowników, segmentów sieci i urządzeń końcowych.
* Monitorowanie zgodności z politykami bezpieczeństwa oraz reagowanie na odchylenia od standardów.
* Praktyczne scenariusze ograniczenia dostępu do wybranych zasobów oraz ochrony przed złośliwym oprogramowaniem w określonych środowiskach.

1. Monitorowanie zagrożeń i reagowanie na incydenty bezpieczeństwa:

* Omówienie metod wykrywania i analizy incydentów w systemie ochrony antywirusowej.
* Przegląd najczęstszych zagrożeń, takich jak phishing, ransomware, spyware, ataki typu brute-force oraz ataki na urządzenia IoT.
* Konfiguracja alertów i powiadomień o zagrożeniach, w tym sygnalizacje w czasie rzeczywistym i raporty okresowe.
* Ćwiczenia z zakresu identyfikacji zagrożeń i odpowiedniego reagowania – usuwanie, izolowanie zagrożonych zasobów oraz wdrażanie działań naprawczych.
* Analiza przypadku rzeczywistych incydentów oraz omówienie przykładów skutecznej reakcji na cyberataki.

1. Zaawansowana analiza dzienników i raportów bezpieczeństwa:

* Omówienie struktury i rodzaju logów generowanych przez system.
* Praktyczne ćwiczenia w zakresie analizowania dzienników zdarzeń oraz identyfikacji potencjalnych zagrożeń.
* Tworzenie raportów cyklicznych i generowanie podsumowań dla kadry zarządzającej, aby uzyskać wgląd w stan bezpieczeństwa.
* Rekomendacje dotyczące optymalizacji procesów raportowania, w tym filtrowanie fałszywych alarmów i skupienie się na realnych zagrożeniach.

1. Zarządzanie aktualizacjami, licencjami i zgodnością systemu:

* Omówienie procesu aktualizacji oprogramowania, znaczenie aktualizacji i zarządzanie cyklem życia oprogramowania.
* Zarządzanie licencjami – optymalizacja liczby użytkowników, przypisywanie kluczy licencyjnych oraz odnowienie licencji.
* Konfiguracja automatycznych aktualizacji oraz ręczna instalacja krytycznych poprawek bezpieczeństwa.
* Testowanie i walidacja systemu po aktualizacjach w celu minimalizacji wpływu na środowisko produkcyjne.

1. Warsztaty praktyczne i symulacja incydentów:

* Ćwiczenia z reakcji na incydenty w oprogramowaniu.
* Warsztaty z identyfikacji i analizy zagrożeń w celu szybkiego reagowania i minimalizacji ryzyka.
* Ćwiczenia z tworzenia polityk bezpieczeństwa, dostosowanych do specyfiki organizacji i poziomu zagrożeń.
* **Szkolenie z oprogramowania do monitorowania infrastruktury IT**

1. Wprowadzenie do oprogramowania oraz jego podstawowa konfiguracja:

* Omówienie architektury systemu oraz komponentów umożliwiających pełne monitorowanie sieci i urządzeń.
* Praktyczna konfiguracja oprogramowania, integracja z systemem organizacji oraz zarządzanie licencjami.
* Wstępna konfiguracja użytkowników oraz przydzielanie uprawnień zgodnie z rolami w organizacji.
* Przegląd funkcji zarządzania urządzeniami końcowymi oraz możliwości automatyzacji zadań administracyjnych.

1. Monitorowanie i zarządzanie zasobami sieciowymi oraz urządzeniami końcowymi:

* Wykrywanie urządzeń w sieci, klasyfikacja zasobów i monitorowanie ich statusu.
* Konfiguracja monitorowania zasobów w czasie rzeczywistym, w tym serwerów, komputerów, urządzeń mobilnych i IoT.
* Analiza dostępności zasobów, prognozowanie wykorzystania oraz identyfikacja potencjalnych problemów wydajnościowych.
* Zarządzanie inwentaryzacją sprzętu i oprogramowania – ewidencja licencji, aktualizacji i statusu urządzeń.

1. Zarządzanie użytkownikami oraz monitorowanie ich aktywności:

* Konfiguracja kontroli dostępu i uprawnień dla użytkowników zgodnie z zasadami bezpieczeństwa.
* Monitorowanie aktywności użytkowników, analiza sesji i śledzenie nieautoryzowanych działań.
* Wdrażanie polityk dostępu do danych oraz kontrolowanie zgodności działań użytkowników z polityką bezpieczeństwa.
* Raportowanie aktywności użytkowników w systemie oraz identyfikacja potencjalnych naruszeń bezpieczeństwa.

1. Analiza i reagowanie na incydenty bezpieczeństwa oraz zagrożenia:

* Identyfikacja zagrożeń w infrastrukturze IT – analizowanie zdarzeń oraz wykrywanie anomalii.
* Tworzenie polityk bezpieczeństwa w systemie, w tym ochrony przed atakami wewnętrznymi i zewnętrznymi.
* Konfiguracja powiadomień i alertów o krytycznych zdarzeniach oraz zarządzanie priorytetami zdarzeń.
* Automatyczne blokowanie podejrzanych działań, wdrażanie reakcji na incydenty oraz procedur przywracania systemów do działania.

1. Raportowanie i audyt zgodności systemu z normami bezpieczeństwa:

* Generowanie raportów dotyczących stanu infrastruktury IT.
* Konfiguracja cyklicznych raportów dla administracji IT i zarządu w celu monitorowania efektywności polityk bezpieczeństwa.
* Tworzenie podsumowań audytów systemowych oraz analiza zgodności z wymogami bezpieczeństwa i wydajności infrastruktury.
* Praktyczne ćwiczenia z wykorzystania narzędzi audytowych oraz interpretacja wyników audytów bezpieczeństwa i zasobów IT.

1. Zarządzanie aktualizacjami, licencjami i wdrażaniem poprawek bezpieczeństwa:

* Wdrażanie i zarządzanie aktualizacjami w systemach operacyjnych oraz oprogramowaniu na urządzeniach końcowych.
* Monitorowanie zgodności aktualizacji oraz zarządzanie licencjami poszczególnych modułów oprogramowania.
* Automatyzacja procesów wdrażania poprawek krytycznych w celu minimalizacji ryzyka podatności.
* Kontrola polityk aktualizacji zgodnie z harmonogramem organizacji i wymogami bezpieczeństwa.

1. Analiza wydajności i zarządzanie dostępnością sieci oraz aplikacji:

* Praktyczne ćwiczenia z monitorowania wydajności sieci – analiza ruchu, obciążenia oraz zasobów serwerów.
* Zarządzanie dostępnością aplikacji biznesowych i minimalizowanie przestojów za pomocą funkcji monitorowania SLA.
* Wykorzystanie raportów wydajnościowych do optymalizacji zasobów oraz diagnozowania wąskich gardeł.
* Planowanie zadań i prognozowanie wydajności zasobów na podstawie zebranych danych historycznych.
* **Szkolenie z kontrolera domeny Active Directory**

Szkolenie z zakresu Active Directory (AD):

Inicjatywa szkoleniowa dedykowana Active Directory ma za zadanie zapewnić uczestnikom wszechstronne przygotowanie do efektywnego zarządzania oraz ochrony infrastruktury Active Directory, stanowiąc fundament dla bezpiecznego i zrównoważonego zarządzania tożsamościami   
i dostępami w sieciowych ekosystemach organizacyjnych. Program szkoleniowy został skonstruowany tak, aby objąć spektrum zagadnień, począwszy od elementarnych, aż po zaawansowane moduły.

1. Ekspozycja na Architekturę Active Directory: Wstępna faza szkolenia skupia się na dogłębnym zarysie roli i kardynalnego znaczenia infrastruktury Active Directory w procesach zarządzania identyfikowalnością użytkowników oraz moderacji dostępu. Uczestnicy zostaną wprowadzeni w kompleksową architekturę AD, eksplorując jej kluczowe usługi i funkcjonalności, w tym mechanizmy uwierzytelniania, autoryzacji oraz efektywne zarządzanie zasobami.
2. Podstawy Konfiguracji i Administracji Obiektami w AD: Moduł ten kładzie nacisk na praktyczne aspekty tworzenia, konfiguracji i zarządzania obiektami takimi jak użytkownicy, grupy i komputery, działającymi w obrębie środowiska AD. Uczestnicy zdobędą umiejętności w zakresie procedur dodawania, usuwania i modyfikacji obiektów, korzystając z dedykowanych narzędzi administracyjnych.
3. Wprowadzenie do Mechanizmów Polityk Grupowych: Szczegółowe omówienie i analiza roli polityk grup (Group Policy) w kontekście zarządzania konfiguracją i bezpieczeństwem infrastruktury AD. Szkolenie obejmuje metodyki tworzenia, aplikacji i administrowania politykami grupowymi, ukazując ich wpływ na regulacje i konfiguracje zarówno klientów, jak i serwerów w domenie.
4. Implementacja Zasad Bezpieczeństwa w AD: Dyskusja na temat strategii i metodologii wzmocnienia zabezpieczeń infrastruktury AD, obejmująca zarządzanie uprawnieniami, monitorowanie aktywności w logach oraz konfigurację polityk bezpieczeństwa. Szkolenie podkreśla praktyczne podejście do identyfikacji, reagowania oraz efektywnego rozwiązywania incydentów bezpieczeństwa.
5. Strategie Ochrony AD Przed Atakami: Analiza potencjalnych zagrożeń dla infrastruktury AD oraz zapewnienie szkolenia z procedur szybkiego reagowania i odtwarzania funkcjonalności systemu w przypadku wystąpienia ataków lub innych awarii. Ten segment szkolenia jest poświęcony rozwijaniu kompetencji w zakresie przeciwdziałania zagrożeniom, przywracania systemu do stanu operacyjnego oraz zapewnienia ciągłości działania krytycznych usług.

* **Szkolenie z zakresu wirtualizacji:**

Inicjatywa ta jest skoncentrowana na intensyfikacji świadomości oraz ekspansji umiejętności technicznych związanych z aspektami bezpieczeństwa operacyjnego w środowiskach wirtualizowanych. Program szkoleniowy został zaprojektowany tak, aby oferować kompendium wiedzy obejmujące kluczowe segmenty:

1. Fundamenty Technologii Wirtualizacji: Wstępna część szkolenia dedykowana jest dogłębnemu zrozumieniu essencji technologii wirtualizacji, przybliżając uczestnikom szeroki wachlarz platform wirtualizacyjnych, w tym, lecz nie ograniczając się do, Vmware oraz Hyper-V. Uczestnicy zostaną zaznajomieni z kluczowymi funkcjami, możliwościami oraz praktycznymi zastosowaniami tych technologii w różnorodnych kontekstach biznesowych, uwydatniając ich strategiczne znaczenie dla nowoczesnych przedsiębiorstw.
2. Konstrukcja, Konfiguracja i Administrowanie Maszynami Wirtualnymi: Ten moduł szkolenia skupia się na przekazaniu praktycznych wskazówek dotyczących procesów kreowania, konfiguracji oraz zarządzania wirtualnymi maszynami. Szczególny nacisk kładziony jest na procedury instalacji systemów operacyjnych, alokacji zasobów oraz konfiguracji komunikacji sieciowej, z zamiarem maksymalizacji efektywności i wydajności wirtualnych środowisk operacyjnych.
3. Metodologie Ochrony Infrastruktury Wirtualizowanej: Zaawansowany segment szkolenia poświęcony jest szczegółowej analizie i implementacji technik zabezpieczających infrastrukturę wirtualizowaną. Uczestnicy zgłębią metody i narzędzia umożliwiające izolację maszyn wirtualnych, zabezpieczanie hypervisorów oraz zarządzanie sieciami wirtualnymi, z naciskiem na kluczowe procedury monitorowania zagrożeń, konfigurację zasad zapór sieciowych oraz techniki segmentacji sieci wirtualnych. Omówione zostaną również zaawansowane strategie ochrony przed złośliwym oprogramowaniem i atakami sieciowymi, mające na celu zwiększenie odporności i bezpieczeństwa całego ekosystemu wirtualnego.

* **Szkolenie z zakresu kopii zapasowych (backup):**

Inicjatywa szkoleniowa skoncentrowana na bezpieczeństwie kopii zapasowych kieruje się ku dogłębnemu zrozumieniu i praktycznej maestrii w zakresie kreowania oraz administracji bezpiecznymi mechanizmami backupu danych, akcentując na kluczowych komponentach:

1. Fundamenty Backupu i Jego Znaczenie w Kontekście Bezpieczeństwa IT: Inauguracyjny moduł kursu dokonuje eksplikacji kluczowych pojęć i terminologii związanej z procesem tworzenia kopii zapasowych, podkreślając ich nieodzowną rolę w kompleksowej strategii bezpieczeństwa technologii informacyjnych oraz w zapewnieniu nieprzerwanej operacyjności korporacyjnych ekosystemów. Uczestnicy zdobywają perspektywę na istotę backupów jako niezbędnej linii obrony przed incydentami, które mogą zagrozić ciągłości działania organizacji.
2. Dogłębna Analiza Typologii Kopii Zapasowych: Kurs prowadzi przez szczegółowe wyjaśnienie różnorodności form backupów – od pełnych, przez przyrostowe, aż po różnicowe – oferując równocześnie pragmatyczne wytyczne dotyczące ich efektywnego planowania, konfiguracji i implementacji. Omówienie to jest kluczowe dla zrozumienia optymalnych metod zarządzania cyklem życia danych oraz dla maksymalizacji efektywności procesów backupu.
3. Implementacja Nowoczesnych Rozwiązań Backupowych: Ten segment szkolenia koncentruje się na adaptacji oraz wykorzystaniu zaawansowanych technologii i oprogramowania backupowego, włączając w to systemy lokalne oraz oparte na chmurze, techniki deduplikacji danych, mechanizmy kompresji oraz szyfrowania. Przedstawione zostają najnowsze narzędzia i metodologie, które umożliwiają zwiększenie efektywności i bezpieczeństwa procesów archiwizacji danych.
4. Weryfikacja Efektywności Backupu i Strategii Odtwarzania: Kurs zawiera kompleksowe instrukcje dotyczące testowania efektywności tworzonych kopii zapasowych oraz procedur przywracania danych, z naciskiem na strategie prewencji i reagowania na kryzysy takie jak ataki ransomware. Uczestnicy uzyskują wiedzę na temat kluczowych praktyk i procedur testowych, które zapewniają gotowość na scenariusze awaryjne.
5. Procedury i Strategie Odzyskiwania Danych po Awarii: Finalny moduł edukacyjny zagłębia się   
   w omówienie metodyk i praktycznych wytycznych szybkiego odzyskiwania funkcjonalności systemów po wystąpieniu incydentów. Szczególna uwaga poświęcona jest skutecznym strategiom odzyskiwania danych, które są fundamentem dla minimalizacji czasu przestoju i optymalizacji procesu odbudowy po awarii.

Cel szkolenia:

Podstawowym zamierzeniem niniejszego kursu szkoleniowego jest dostarczenie uczestnikom kompleksowego zestawu wiedzy teoretycznej oraz praktycznych kompetencji, które są krytyczne dla skutecznego administrowania i nadzorowania bezpieczeństwem infrastruktury technologicznej informacyjnej. Szczególny nacisk kładziony jest na głębokie zrozumienie i zarządzanie systemem Active Directory, ekosystemami wirtualizacji oraz złożonymi strategiami implementacji systemów kopii zapasowych. Celem tego szkolenia jest nie tylko przekroczenie granic czysto teoretycznego przekazu wiedzy, ale przede wszystkim rozwinięcie praktycznych umiejętności aplikacyjnych, które umożliwią uczestnikom efektywne zabezpieczanie wartościowych zasobów informatycznych przed rosnącą gamą zagrożeń cyfrowych oraz zagwarantowanie nieprzerwanej operacyjności systemów informatycznych.

Poprzez syntezę teoretycznych fundamentów z realnymi aplikacjami praktycznymi, program ma na celu wyekwipowanie uczestników w niezbędne narzędzia do identyfikacji, adekwatnej reakcji oraz neutralizacji potencjalnych zagrożeń bezpieczeństwa cyfrowego. Ponadto, kurs stawia za cel wdrożenie uczestników w głębinę najlepszych praktyk i standardów branżowych, które stanowią o kształcie profesjonalnej codziennej praktyki. Skupienie się na tych elementach ma kluczowe znaczenie dla kształtowania w uczestnikach umiejętności nie tylko reaktywnych, ale przede wszystkim proaktywnych w kontekście zarządzania ryzykiem i ochrony infrastruktury IT. W rezultacie, program szkoleniowy ma na celu przygotowanie adeptów do pełnienia roli bastionu w obronie przed zagrożeniami, promując jednocześnie kulturę bezpieczeństwa informacyjnego, która jest fundamentem dla zrównoważonego rozwoju i innowacyjności w przestrzeni technologicznej organizacji.

* **Szkolenie z systemu monitorowania, wykrywania i reagowania na zagrożenia bezpieczeństwem w czasie rzeczywistym (SIEM)**

Przedmiotem zamówienia jest przeprowadzenie kompleksowego szkolenia z zakresu obsługi i zarządzania systemem Security Information and Event Management (SIEM). Celem szkolenia jest zapewnienie uczestnikom wiedzy i umiejętności niezbędnych do efektywnego monitorowania, wykrywania oraz reagowania na zagrożenia bezpieczeństwa w czasie rzeczywistym.

Szkolenie będzie obejmować następujące zagadnienia:

1. Wprowadzenie do systemów SIEM oraz ich roli w zapewnianiu bezpieczeństwa informacji.

2. Omówienie możliwości systemów SIEM, w tym analiza logów, wykrywanie intruzów, reagowanie na zagrożenia oraz integracja z innymi narzędziami bezpieczeństwa.

3. Praktyczne aspekty zbierania, agregowania, indeksowania i analizowania danych bezpieczeństwa, w celu identyfikacji włamań, zagrożeń oraz anomalii behawioralnych.

4. Zarządzanie podatnościami: metody identyfikacji słabości systemów i aplikacji, oraz techniki korelowania ich z aktualnymi bazami danych dotyczącymi podatności.

5. Ocena konfiguracji systemu i aplikacji zgodnie z najlepszymi praktykami i standardami, w tym analiza zgodności z regulacjami takimi jak RODO/GDPR, PCI DSS, NIST.

6. Reagowanie na incydenty: strategie i procedury tworzenia reguł alarmowych oraz zarządzanie reakcją na wykryte zagrożenia.

7. Przykłady zastosowania i najlepsze praktyki w wykorzystaniu systemów SIEM w różnych środowiskach, w tym w infrastrukturze chmurowej i w systemach kontenerowych.

Szkolenie ma na celu przygotowanie uczestników do samodzielnego zarządzania systemem SIEM, zrozumienia zasad ich działania oraz umiejętności konfiguracji i adaptacji systemu do specyficznych potrzeb organizacji. Uczestnicy nauczą się, jak efektywnie monitorować i analizować bezpieczeństwo w swoich systemach, identyfikować i reagować na zagrożenia, a także jak stosować najlepsze praktyki w celu zwiększenia ogólnego poziomu bezpieczeństwa informacji.

* **Szkolenie z UTM**

Celem zamówienia jest przeprowadzenie szkolenia z zakresu podstawowej konfiguracji urządzeń UTM dla pracowników technicznych. Szkolenie ma na celu umożliwić uczestnikom zdobycie praktycznych umiejętności w zakresie konfiguracji, zarządzania oraz monitorowania urządzeń UTM, co przyczyni się do zwiększenia bezpieczeństwa sieciowego w organizacji.

Opis techniczny szkolenia:

Szkolenie obejmuje następujące moduły:

1. Przygotowanie do konfiguracji - uczestnicy nauczą się jak połączyć się z urządzeniem UTM oraz jak korzystać z interfejsu webowego do zarządzania urządzeniem.

2. Konfiguracja interfejsów sieciowych - nauka konfiguracji interfejsów Ethernet i VLAN, ustawień IP, maski podsieci itp.

3. Tworzenie reguł zapory sieciowej - praktyczne ćwiczenia z tworzenia reguł kontrolujących ruch między interfejsami oraz wchodzący i wychodzący ruch sieciowy.

4. Konfiguracja VPN - instrukcje dotyczące ustawień VPN, w tym typów tuneli, uwierzytelniania i szyfrowania.

5. Monitorowanie i diagnostyka - przekazanie wiedzy na temat monitorowania urządzenia oraz technik diagnostycznych.

6. Aktualizacja oprogramowania - procedury aktualizacji oprogramowania urządzenia.

7. Zabezpieczenie dostępu - metody silnego uwierzytelniania i zapewnienie bezpieczeństwa dostępu do konfiguracji.

8. Tworzenie kopii zapasowych - nauka regularnego tworzenia i zarządzania kopiami zapasowymi.

9. Konsultacja dokumentacji i wsparcia technicznego - jak efektywnie korzystać z dostępnych zasobów wsparcia.

10. Monitoring bezpieczeństwa - konfiguracja systemów monitorujących bezpieczeństwo.

Zakres prac:

- Organizacja i przeprowadzenie serii warsztatów szkoleniowych.

- Dostarczenie materiałów szkoleniowych.

- Praktyczne ćwiczenia z użyciem urządzeń UTM.

Oczekiwane korzyści:

Uczestnicy szkolenia zdobędą umiejętności niezbędne do efektywnego i bezpiecznego zarządzania urządzeniami UTM, co zwiększy ogólną efektywność zarządzania infrastrukturą sieciową i poprawi poziom bezpieczeństwa IT w organizacji.