Załącznik nr 1

OPIS PRZEDMIOTU ZAMÓWIENIA

SPIS TREŚCI

Spis treści

[1. Specjalistyczne szkolenie dla osoby odpowiedzialnej za bezpieczeństwo w obszarze IT 3](#_Toc191562602)

[2. Zakup serwera dla Urzędu Gminy w celu replikacji danych i przejęcia zadań w przypadku awarii wraz z instalacją i konfiguracją 4](#_Toc191562603)

[3. Zakup serwera NAS wraz z instalacją i konfiguracją 14](#_Toc191562604)

[4. Zakup routera z zabezpieczeniem antywirusowym wraz z instalacją i konfiguracją 23](#_Toc191562605)

[5. Zakup UPSów do serwerowni wraz z instalacją dla Urzędu Gminy oraz Gminnego Ośrodka Pomocy Społecznej w Trzebiechowie 26](#_Toc191562606)

[6. Zakup zarządzalnych urządzeń sieciowych z obsługą VLAN 31](#_Toc191562607)

[7. Zakup oprogramowania przeciwdziałającemu wyciekowi danych wraz z licencją, wdrożeniem i rocznym wsparciem 33](#_Toc191562608)

[9. Zakup oprogramowania do backupu danych wraz z instalacją, konfiguracją i wsparciem 35](#_Toc191562609)

[10. Zakup oprogramowania antywirusowego -przedłużenie licencji dla Urzędu Gminy 44](#_Toc191562610)

# Specjalistyczne szkolenie dla osoby odpowiedzialnej za bezpieczeństwo w obszarze IT

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla przeprowadzonego szkolenia** |
| **Szkolenie z antywirusa** | Wykonawca zapewni certyfikowane szkolenie (min. 2 dni) dla administratora Zamawiającego (1 osoba) z dostarczonego rozwiązania antywirusowego. Szkolenie w formie online, zorganizowane w autoryzowanym przez producenta ośrodku szkoleniowym. Szkolenie musi zawierać min. poniższe zagadnienia:   * Omówienie konsoli do zarządzania * Omówienie funkcji serwera, * Zarządzanie aktualizacją, * Polityki i dziedziczenie * Zapora osobista * Powiadomienia i raportowanie * Kontrola dostępu do stron internetowych * Kontrola dostępu do urządzeń * zarządzać urządzeniami mobilnymi   Szkolenie zostanie dostarczone w formie vouchera, z możliwością zrealizowania w wybranym przez Administratora terminie w okresie min. **12 miesięcy** |
| **Szkolenie z utworzenia usługi katalogowej w formie warsztatów** | Wykonawca zapewni certyfikowane szkolenie (min. 2 dni) dla administratora Zamawiającego (1 osoba) z dostarczonego rozwiązania klasy DLP. Szkolenie w formie online, zorganizowane w autoryzowanym przez producenta ośrodku szkoleniowym.  Szkolenie musi zawierać min. poniższe zagadnienia:   * Konfiguracji systemu * Wdrożenie rozwiązania * Konfiguracja konsoli, * Wdrożenie serwera * Kategoryzacja aplikacji oraz stron internetowych * Analiza potencjalnych wycieków danych * konfiguracja dostępów dla urządzeń i portów * Reguły: DLP, ogólne, aplikacji.   Szkolenie zostanie dostarczone w formie vouchera, z możliwością zrealizowania w wybranym przez Administratora terminie w okresie min. **12 miesięcy** |
| **ilość** | 1 komplet |

# Zakup serwera dla Urzędu Gminy w celu replikacji danych i przejęcia zadań w przypadku awarii wraz z instalacją i konfiguracją

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Obudowa** | * Obudowa Rack o wysokości max 1U z możliwością instalacji do 8 dysków 2.5" Hot-Plug * Obudowa wyposażona 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. * 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 12-rdzeniowy, min. 2.1GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 168 w teście SPECrate2017\_int\_base dostępnym na stronie www.spec.org dla dwóch procesorów. |
| **RAM** | * 128GB DDR4 RDIMM 3200MT/s, |
| **Kontroler RAID** | * Sprzętowy kontroler dyskowy, posiadający   + Min. 8GB nieulotnej pamięci cache,   + Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.   + Wsparcie dla dysków samoszyfrujących |
| **Dyski twarde** | * Zainstalowane:   + 4x dysk SAS o pojemności min. 2.4TB, Hot-Plug. * Zainstalowane dwa dyski M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1. |
| **Gniazda PCI** | * Dwa sloty PCIe LP |
| **Interfejsy sieciowe/SAS** | * Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet BaseT oraz 2 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) |
| **Wbudowane porty** | * Przednie: min. 1x VGA, min. 1x USB 2.0, min. 1x micro-USB dedykowane dla karty zarządzającej, * Tylne: min. 1x VGA, min. 2x USB w tym 1x USB 3.0, |
| **Video** | * Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900 |
| **Wentylatory** | * Redundantne |
| **Zasilacze** | * Redundantne, Hot-Plug maksymalnie 1100W klasy Titanium |
| **Elementy montażowe** | * Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych * Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych |
| **System operacyjny/dodatkowe oprogramowanie** | Zakres Przedmiotu Zamówienia obejmuje dostarczenie Oprogramowania Systemowego zwanego dalej SSO, pokrywającego licencyjnie Wszystkie core oferowanych procesorów.  Licencja musi uprawniać do uruchamiania SSO w środowisku fizycznym minimum dwóch wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji.  SSO musi posiadać następujące, wbudowane cechy:  a) możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym,  b) możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności minimum 64TB przez każdy wirtualny serwerowy system operacyjny,  c) możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych,  d) możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci,  e) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy,  f) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy,  g) automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading),  i) wbudowane wsparcie instalacji i pracy na wolumenach, które:  I. pozwalają na zmianę rozmiaru w czasie pracy systemu,  II. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,  III. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,  IV. umożliwiają zdefiniowanie list kontroli dostępu (ACL),  j) wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość,  k) wbudowane szyfrowanie dysków  l) możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET,  m) możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów,  n) wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych,  o) graficzny interfejs użytkownika,  p) zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,  r) wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play),  s) możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu,  t) dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa,  u) możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:  I. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,  II. 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:  1) podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,  2) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,  3) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,  III. zdalna dystrybucja oprogramowania na stacje robocze,  IV. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,  V. centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:  1) dystrybucję certyfikatów poprzez http,  2) konsolidację CA dla wielu lasów domeny,  3) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,  VI. szyfrowanie plików i folderów,  VII. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),  VIII.możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,  IX. serwis udostępniania stron WWW,  X. wsparcie dla protokołu IP w wersji 6 (IPv6),  XI. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie minimum 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:  1) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,  2) obsługi ramek typu jumbo frames dla maszyn wirtualnych,  3) obsługi 4-KB sektorów dysków,  4) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,  5) możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API,  6) możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model),  v) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet,  w) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath),  x) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego,  y) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty,  z) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.  Dodatkowo licencja pozwalająca na łączenie się z zasobami serwera dla 26 użytkowników. |
| **Bezpieczeństwo** | * Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. * Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. * 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 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 SSL   + 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;   + integracja z Active Directory;   + wsparcie dla automatycznej rejestracji 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   + możliwość obsługi przez sześciu użytkowników jednocześnie;   + możliwość podmontowania zdalnych wirtualnych napędów;   + wirtualną konsolę z dostępem do myszy, klawiatury;   + możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;   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. |
| **Oprogramowanie do monitorowania** | Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:   * Monitoring:   + ilość podłączonych oraz rozłączonych systemów   + stan podłączonych urządzeń   + informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów   + Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia   + informacje o statusie gwarancji dla poszczególnych urządzeń   + informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń   + informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych.   + Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych   + Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych.   + Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych.   + Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC.   + Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej.   + Monitoring parametrów serwerów z informacją o minimum:     - Obciążeniu procesora     - Zużyciu pamięci RAM     - Temperaturze procesorów     - Temperaturze powietrza wlotowego     - Zużyciu prądu     - Zmianach w fizycznej konfiguracji serwera     - Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.   + Monitoring parametrów pamięci masowych z informacją o minimum:     - Opóźnieniach     - IOPS     - Przepustowości     - Utylizacji kontrolerów     - Pojemność całkowita i dostępna     - Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów.     - Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.     - Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata     - Informacje o poziomie redukcji danych     - Informacje o statusie replikacji oraz snapshotów   + Monitoring parametrów przełączników sieciowych z informacją o minimum:     - Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny     - Stanie komponentów: zasilacze, wentylatory     - Podłączonych hostach     - Ilości i statusu portów     - Utylizacji procesora     - Utylizacji poszczególnych portów     - Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. * Aktualizacja firmware   + możliwość aktualizcji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizcji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizcji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizcji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizcji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania * Raporty   + Możliwość generowania raportów dla serwerów zawierających informację o:     - Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej     - Średnim obciążeniu: procesorów, pamięci RAM, IO,   + Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o:     - Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji   + Generowanie raportów do plików CSV i PDF * Cyberbezpieczeństwo   + Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia.   + Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń.   + Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych.   + Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. * Wspierane urządzenia   + Urządzenie Producenta dostarczane w ramach postępowania   + Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) * Wirtualny asystent   + Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; * Możliwość rozszerzenia funkcjonalności   + Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. * Inne   + Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android |
| **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. |
| **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 5 lat. * Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet. * Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. * Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon/portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. * Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. * 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 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. |
| **Wymagania wdrożeniowe** | Zamawiający w ramach dostawy wymaga dodatkowo, aby Wykonawca wykonał usługi wdrożeniowe polegające na minimum:  a) Konfiguracja serwera:   * montażu w/w sprzętu w posiadanej szafie rack przez Zamawiającego w sposób zgodny z zaleceniami producenta dostarczanych serwerów. Prowadzenie kabli nie może powodować zaburzeń w cyrkulacji gorącego powietrza wydmuchiwanego z serwerów- podłączenia serwera do wskazanej przez Zamawiającego infrastruktury sieciowej za pomocą właściwych kabli zapewniający bezawaryjną i ciągłą pracę w przypadku awarii jednej z kart sieciowych serwera * wykonać testy niezawodności środowiska serwerowego poprzez odłączanie jednej ze ścieżki/wyłączanie urządzenia oraz test redundancji zasilania.   b) Wykonawca musi przygotować niezbędną dokumentację w zakresie dokumentacji powdrożeniowej zawierającej opis konfigurowanych opcji wdrożonego środowiska serwerowego. Wymaga się, aby wdrożenie było przeprowadzone przez inżynierów (minimum 1 osoba) posiadających wiedzę na temat dostarczanego modelu serii serwerów danego producenta |
| **ilość** | 1 sztuka |

# Zakup serwera NAS wraz z instalacją i konfiguracją

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Architektura procesora** | 64 bit x86 |
| **Procesor liczba rdzeni** | Nie mniej niż 6 o taktowaniu nie niższym niż 3,8 GHz |
| **Pamięć RAM** | Nie mniej niż 16GB UDIMM DDR5 |
| **Pamieć RAM liczba slotów** | Minimum 4 sloty |
| **Pamięć RAM - możliwość rozszerzenia** | Nie mniej niż do 192 GB |
| **Pamięć Flash** | Nie mniej niż 5GB |
| **Liczba zatok na dyski twarde** | Minimum 12 |
| **Gniazda M.2** | 2 x M.2 2280 PCIe Gen 5 x2 |
| **Obsługiwane dyski twarde** | 3.5" SATA oraz 2.5" SATA / SSD SATA |
| **Pojemność dysków twardych jakie można stosować** | do 24 TB |
| **Możliwość podłączenia modułu rozszerzającego** | Tak, do 8 |
| **Porty LAN** | Minimum 2x 2,5 Gigabit Ethernet  Minimum 2 x 10GBASE-T |
| **Diody LED** | HDD 1–12, stan urządzenia, LAN |
| **Porty USB** | minimum 2 x Typ-A USB 3.2 Gen 2 |
| **Złącza PCIe** | Nie mniej niż 3 |
| **Przyciski** | Reset, Zasilanie |
| **Typ obudowy** | RACK, 2U |
| **Dopuszczalna temperatura pracy** | od 0 do 40˚C |
| **Wilgotność względna podczas pracy** | 5-95% R.H. |
| **Zasilanie** | Redundatne 550 W(x2), 100–240 V |
| **Agregacja łączy** | Tak |
| **Obsługiwane systemy plików** | Dyski wewnętrzne: ZFS Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+ |
| **Możliwość podłączenia karty WLAN na USB** | Tak |
| **Łączenie usług z interfejsem** | Tak |
| **Szyfrowanie udziałów** | Tak, min AES 256 |
| **Szyfrowanie dysków zewnętrznych** | Tak |
| **Zarządzanie dyskami** | RAID 0,1,5,50,6,60,10, Triple Parity, Triple Mirror Konfiguracja priorytetu odbudowy grup RAID RAID HotSpare i Global HotSpare SSD Trim HDD S.M.A.R.T. Skanowanie uszkodzonych bloków  Wykrywanie uszkodzenia i naprawa danych Cache odczytu z wykorzystaniem dysków SSD Cache odczytu i dziennik zapisu z wykorzystaniem dysków SSD Funkcjonalność migawek udziałów oraz LUN, wraz z możliwością ich replikacji na drugie urządzenie |
| **Wbudowana obsługa iSCSI** | Obsługa wielu jednostek LUN na Target Obsługa mapowania i maskowania LUN Obsługa SPC-3 Persistent Reservation Obsługa MPIO & MC/S  Wykonywanie migawek oraz kopii zapasowej LUN |
| **Obsługa Fiber Channel (FC SAN)** | Wsparcie opcjonalnych kart FC Mapowanie LUN |
| **Zarządzanie prawami dostępu** | Przypisanie pojemności dla użytkowników Importowanie listy użytkowników Zarządzanie kontami użytkowników  Zarządzanie grupą użytkowników  Zarządzanie uprawnieniami dla użytkowników i grup Obsługa zaawansowanych uprawnień dla podfolderów |
| **Obsługa Windows AD** | Logowanie użytkowników domenowych poprzez protokoły CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera i klienta LDAP |
| **Funkcje backup** | Oprogramowanie do tworzenia kopii bezpieczeństwa plików, opracowane przez producenta urządzenia dla systemów Windows.  Backup na zewnętrzne dyski twarde. |
| **Współpraca z zewnętrznymi dostawcami usług chmury** | Przynajmniej: Amazon S3, Amazon Glacier, Microsoft Azure, Google Cloud Storage, Dropbox, OneDrive for Business, Google Drive |
| **Darmowe aplikacje na urządzenia mobilne** | Monitoring i zarządzanie urządzeniem / Współdzielenie plików / Obsługa kamer  Dostępne na systemy iOS oraz Android |
| **Minimum obsługiwane aplikacje** | Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer pobierania (Bittorrent/HTTP/HTTPS/FTP) |
| **VPN** | VPN client / VPN server Minimum obsługa PPTP, OpenVPN |
| **Administracja systemu** | Połączenia HTTP/HTTPS Powiadamianie przez e-mail Powiadamianie przez SMS (z wykorzystaniem zewnętrznych usług) DDNS oraz zdalny dostęp w chmurze producenta SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP oraz lokalnych przez USB Monitorowanie zasobów urządzenia Monitorowanie zasobów systemu w czasie rzeczywistym Rejestr zdarzeń Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania Możliwość aktualizacji oprogramowania z powiadomieniem z serwerów producenta Ustawienia systemowe: kopia zapasowa, przywracanie, resetowanie systemu |
| **Wirtualizacja** | Możliwość uruchomienia maszyn wirtualnych z systemem Windows, Linux, Unix i Android Import maszyn wirtualnych  Klonowanie maszyn wirtualnych Migawki maszyn wirtualnych  GPU pass-through dla dodatkowych kart graficznych |
| **Zabezpieczenia** | Filtracja IP Ochrona dostępu do sieci z automatycznym blokowaniem połączeń Obsługa HTTPS FTP z SSL/TLS (Explicit) Obsługa SFTP (tylko admin) Szyfrowanie AES 256-bit Import certyfikatu SSL |
| **Możliwość instalacji dodatkowego oprogramowania** | Tak, sklep z aplikacjami producenta i aplikacjami firm zewnętrznych Możliwość instalacji z gotowych paczek oraz wbudowane narzędzia wirtualizacji umożliwiającee zarówno obsługę kontenerów Docker/LXD jak i pełnych maszyn wirtualnych |
| **Gwarancja** | 5 lat |
| **Montaż** | dedykowane szyny montażowe do szafy rack (tego samego producenta co serwer NAS |
| **DYSKI HDD - 7szt** | |
| **Kompatybilność** | Kompatybilne z oferowanym urządzeniem (lista kompatybilności) |
| **Gwarancja** | 5 lat, pozostawienie dysków u klienta w razie awarii |
| **Pojemność po sformatowaniu** | 8 TB |
| **Format obudowy** | 3,5 cala |
| **Zaawansowane formatowanie danych (AF)** | Tak |
| **Technologia zapisu** | CMR |
| **Zgodność z dyrektywą RoHS** | Tak |
| **Wbudowane kolejkowanie poleceń** | Tak |
| **Interfejs** | SATA 6 Gb/s |
| **Szybkość transmisji** | 267 MB/s |
| **Klasa wydajności** | Klasa 7200 obr./min |
| **Pamięć podręczna (MB)** | 256 |
| **Cykle ładowania/rozładowania** | 600 000 |
| **Współczynnik obciążenia w skali roku** | 550 TB/rok |
| **Nienaprawialne błędy odczytu na odczytane bity** | <1 na 10^15 |
| **MTBF** | 2 000 000 |
| **Dyski m2 - 2szt** | |
| **Kompatybilność** | Kompatybilne z oferowanym urządzeniem (lista kompatybilności) |
| **Pojemność** | 1 TB |
| **Interfejs** | PCIe Gen 3.0 8 Gb/s |
| **Form Factor** | M.2 2280-S3-M |
| **Ograniczona gwarancja** | 5-letnia |
| **Odczyt sekwencyjny** | Do 3 430 MB/s \* |
| **Zapis sekwencyjny** | Do 3 000 MB/s \* |
| **Odczyt losowy (4KB, QD32)** | Do 515 000 operacji/s \* |
| **Zapis losowy (4KB, QD32)** | Do 560 00 operacji/s \* |
| **TBW** | 2000 |
| **Specyfikacja wdrożenia** | |
| **Wymagania minimum** | * - Inicjalizacja urządzenia * - Konfiguracja puli pamięci oraz grup RAID * - Konfiguracja sieci * - Konfiguracja użytkowników i grup * - Utworzenie folderów udostępnionych * - Instalacja pakietów bezpieczeństwa * - Zaawansowana konfiguracja migawek * - Konfiguracja replikacji danych lub backupu * - Uruchomienie dowolnych, dodatkowych usług na urządzeniu * - Weryfikacja poprawności działania urządzenia |
| Ilość | 1 komplet |

# Zakup routera z zabezpieczeniem antywirusowym wraz z instalacją i konfiguracją

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Kontrola dostępu** | Kontrola dostępu oparta na źródłowym/docelowym adresie IP |
| **Filtrowanie** | • Filtrowanie grup WEB • Filtrowanie adresów URL • Bezpieczeństwo sieciowe |
| **Ochrona przed atakami ARP** | • Wysyłanie pakietów GARP\* • Skanowanie ARP\* • Wiązanie adresów IP i MAC\* |
| **Ochrona przed atakami sieciowymi** | • TCP/UDP/ICMP Flood Defense • Blokowanie skanowania TCP (Stealth FIN/Xmas/Null) • Blokowanie odbierania pakietów ping z sieci WAN |
| **Standardy i protokoły** | • IEEE 802.3, IEEE802.3u, IEEE802.3ab, IEEE802.3z, IEEE 802.3x, IEEE 802.1q • TCP/IP, DHCP, ICMP, NAT, PPPoE, NTP, HTTP, HTTPS, DNS, IPSec, PPTP, L2TP, OpenVPN, SNMP, WireGuard VPN |
| **Porty** | Minimum:  • 2 Porty 10GE SFP+ (1 WAN, 1 WAN/LAN) • 1 Port 1GE SFP WAN/LAN • 8 Portów 1GE RJ45 WAN/LAN • 1 Port konsolowy RJ45 • 2 Porty USB (Modem 4G/3G USB jako łącze zapasowe WAN) |
| **Ilość wentylatorów** | 2 |
| **Zasilanie** | Zasilanie redundantne (100–240 VAC, 50/60 Hz) |
| **Pamięć Flash** | 4MB SPI NOR + 256 MB NAND |
| **Pamięć DRAM** | 4 GB DDR4 |
| **Ochrona** | Zabezpieczenie przeciwprzepięciowe 4 kV |
| **Montaż** | Możliwość montażu w szafie Rack |
| **Przepustowość IPS** | TCP: 4924 Mb/s UDP: 4521 Mb/s |
| **Przepustowość DPI** | TCP: 5524 Mb/s UDP: 3547 Mb/s |
| **Przepustowość VPN IPsec** | • ESP-SHA1-AES256: 3099,4 Mb/s • ESP-SHA256-AES256: 2928,4 Mb/s • ESP-SHA384-AES256: 2935,7 Mb/s • ESP-SHA512-AES256: 2878 Mb/s |
| **OpenVPN** | UDP: 4424,1 Mb/s |
| **Przepustowość SSL VPN** | 4486 Mb/s |
| **Typ połączenia WAN** | • Statyczne/dynamiczne przydzielanie adresów IP • PPPoE • PPTP • L2TP • Tunel 6to4 • Pass-Through • Łącze mobilne: Modem 4G/3G USB jako łącze zapasowe |
| **DHCP** | • Serwer/Klient DHCP • Rezerwacja adresów DHCP • Multi-net DHCP • Interfejsy Multi-IP |
| **Kontrola przepustowości** | • Kontrola przepustowości w oparciu o adres IP/port • Gwarantowana i ograniczana przepustowość |
| **NAT** | • Jeden-do-Jeden NAT\*5 • Multi-Net NAT • Serwery wirtualne • Port Triggering\*5 • NAT-DMZ • FTP/H.323/SIP/IPSec/PPTP ALG • UPnP |
| **SSL VPN** | • Serwer SSL VPN • Klient SSL VPN • 500 Tuneli SSL VPN |
| **IPsec VPN** | • 300 tuneli IPsec VPN • LAN-to-LAN, Client-to-LAN • 2 tryby negocjacji - Main/Aggressive • Szyfrowanie DES, 3DES, SHA1, SHA256, SHA384, SHA512, AES128, AES192, AES256 • IKEv1/v2 • Uwierzytelnianie MD5, SHA1 • NAT Traversal (NAT-T) • Dead Peer Detection (DPD) • Perfect Forward Secrecy (PFS) |
| **Funkcje panelu zarządzania** | • Automatyczne wykrywanie urządzeń • Inteligentne monitorowanie stanu sieci • Ostrzeżenia o nietypowych zdarzeniach • Ujednolicony proces konfiguracji • Harmonogram restartu • Spersonalizowana strona logowania do siec |
| **Certyfikaty** | CE, FCC, RoHS |
| **Gwarancja** | Minimum 12 miesięcy |
| **ilość** | 1 sztuka |

# Zakup UPSów do serwerowni wraz z instalacją dla Urzędu Gminy oraz Gminnego Ośrodka Pomocy Społecznej w Trzebiechowie

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Wymagania szczegółowe** | |  |  | | --- | --- | | **2 sztuki - UPS o specyfikacji** | | | Typ zasilacza | line-interactive | | **Moc** | | | Moc pozorna | 3000VA | | Moc skuteczna | 2400W | | **Wyświetlacz** | | | Wskaźnik na panelu | wyświetlacz LCD + diody LED | | **Tryb AC** | | | Napięcie wejściowe | 230V ±25% | | Napięcie wyjściowe | 230V ±10% | | Częstotliwość | 50 / 60Hz | | Kształt napięcia wyjściowego | sinusoida | | Przeciążenie | 110% przejście w tryb obejścia w ciągu 120s; 125% przejście w tryb obejścia w ciągu 60s; 150% przejście w tryb obejścia w ciągu 10s | | **Tryb Inwertera** | | | Napięcie wejściowe | 230V ±25% | | Napięcie wyjściowe | 230V ±25% | | Współczynnik mocy | 0.8 | | Częstotliwość | 50 / 60Hz | | Kształt napięcia wyjściowego | sinusoida | | Czas przełączania | ≤ 10ms | | THDV (obciążenie rezystancyjne) | ≤ 5% | | Sprawność | Max 85% | | Tryb oszczędzania energii | Ustawialne (< 3% obciążenia), przejście w 80s | | Brak zasilania | Ustawialne (< 3% obciążenia), wyłączenie w 80s | | Przeciążenie | 110% przejście w tryb obejścia w ciągu 60s; 125% przejście w tryb obejścia w ciągu 10s; 150% wyłączenie w ciągu 5s | | **Alarm** | | | Awaria sieci zasilającej | raz na sekundę | | Słaba bateria | 3 razy na sekundę | | Przeciążenie | Długi dźwięk raz na 2 sekundy | | Wyciszenie alarmu | Automatyczne po upływie 60s lub ręczne | | **Akumulator** | | | Model | bezobsługowy, w technologii AGM | | Napięcie DC | 48V | | Ilość | 4x 9Ah/12V | | Prąd ładowania | 1A | | Czas ładowania | 90% pojemności po 8 godzinach ładowania | | **Zabezpieczenia** | | | Przeciwzwarciowe akumulatora | elektroniczne + bezpiecznik topikowy | | Przeciążeniowe akumulatora | ogranicznik prądu wyjściowego | | Przeciwprzepięciowe RJ45 (in/out) | Tak | | Filtracja napięcia wyjściowego akumulatora | elektroniczna | | Filtr przeciwzakłóceniowy | EMI/RFI | | **Inne** | | | Ilość gniazd wyjściowych | 3x Schuko, 3x IEC C13 | | Port komunikacyjny | USB 2.0 | | Hałas | ≤ 50 dB (1 m) | | Temperatura | 5°C ~ 40°C | | Wilgotność | Relatywna ≤ 93% | | Waga | 27kg | | Wymiary | 440 x 132 x 410mm (3U) | | Gwarancja | 24 miesiące | |
| **Wymagania szczegółowe** | |  |  | | --- | --- | | **26 sztuk - UPSy o specyfikacji** | | | Typ zasilacza | line-interactive | | **Moc** | | | Moc pozorna | 1200VA | | Moc skuteczna | 720W | | **Wejście** | | | Faza | jednofazowy | | Napięcie | 230V ±25% | | Częstotliwość | 50 / 60Hz | | **Wyjście** | | | Napięcie | 230V ±10% | | Częstotliwość | 50 / 60Hz | | Kształt napięcia wyjściowego | aproksymowana sinusoida | | Współczynnik szczytu | 3:1 | | Czas przełączania | 2-7ms, max. 10ms | | Ilość gniazd | 3x Schuko | | **Akumulator** | | | Model | bezobsługowy, w technologii AGM | | Ilość | 2x 7Ah/12V | | Napięcie DC | 24V | | Czas ładowania | 6 ~ 8h | | **Zabezpieczenia** | | | Przeciwzwarciowe akumulatora | elektroniczne + bezpiecznik topikowy | | Przeciążeniowe akumulatora | ogranicznik prądu wyjściowego | | Przeciwprzepięciowe RJ45 (in/out) | Tak | | Filtracja napięcia wyjściowego akumulatora | elektroniczna | | Filtr przeciwzakłóceniowy | EMI/RFI | | **Inne** | | | Port komunikacyjny | USB 2.0 | | Hałas | ≤ 45 dB (1m) | | Temperatura pracy | 0°C ~ 40°C | | Wilgotność | 20 ~ 90% RH (bez kondensacji) | | Waga | 9kg | | Wymiary | 135 x 345 x 170mm | | Gwarancja | 24 miesiące | |
| **Ilość** | 1 komplet |

# Zakup zarządzalnych urządzeń sieciowych z obsługą VLAN

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Wymagania ogólne** | Wymaga się aby urządzenie obsługiwało następujące funkcje, protokoły oraz spełniało następujące wymagania:   * IEEE 802.3af * IEEE 802.1Q * Protected porty * IEEE 802.1p (CoS) * Port-based QoS * DSCP-based QoS * DiffServ * IEEE802.3ad * IEEE 802.1s Multiple Spanning Trees Protocol (MSTP) * IEEE 802.1ab Link Layer Discovery Protocol (LLDP) * SNMP v1, v2c, v3 * RFC 1213 MIB II * RFC 1643 Ethernet Interface MIB * RFC 1493 Bridge MIB * RMON group 1, 2, 3, 9 * Auto Voice VLAN * DHCP Filtering * Auto denial-of-service (DoS) protection * Wyłączanie portu przy braku połączenia * RFC 2131 DHCP client * IEEE 802.1x * Zabezpieczenie portu poprzez blokowanie adresu MAC * ACL w oparciu o MAC oraz IP * Ochrona przed burzami broadcast, multicast oraz unicast * IGMP Snooping v1/v2 * Zarządzanie przepustowością na wyjściu * SNTP * Wsparcie dla Port mirroring * Konfiguracja poprzez web * Zapis oraz odczyt konfiguracji * Dostęp zabezpieczony hasłem * RADIUS Support * TACACS+ and RADIUS support * Syslog * Min. budżet PoE 55 Wat * Min. czas pracy pomiędzy awariami (MTBF): 1200041 godzin * Emisja hałasu: 0 dB * Maksymalna konsumpcja energii 69,5W * Porty sieciowe: 8 x 10/100/1000 Mb/s PoE + 2 x Gigabit SFP * Metoda przekazywania ramek: Store-and-forward * Przepustowość min.: 20 Gbps * Zewnętrzny zasilacz 54V 1.25A   Urządzenie powinno być objęte ograniczoną wieczystą gwarancją producenta trwającą do 5 lat po ogłoszeniu zaprzestania produkcji wraz z wymianą na następny dzień roboczy przez cały okres gwarancji. Urządzenie powinno być objęte 90 dniowym wsparciem technicznym realizowanym przez producenta oraz pomocą techniczną w formie czat przez cały okres gwarancji. |
| **Ilość** | 8 sztuk |

# Zakup oprogramowania przeciwdziałającemu wyciekowi danych wraz z licencją, wdrożeniem i rocznym wsparciem

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Wymagania ogólne** | 1. System musi obsługiwać systemy operacyjne:    1. Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi    2. Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi    3. MacOS 12 lub nowszy. 2. Serwer administracyjny musi obsługiwać instalację na systemach: a. Windows Server 2016 3. (64-bit) i nowszych. 4. Serwer administracyjny musi obsługiwać bazy danych: a. MS SQL Server 2016 lub nowsze, b. 5. MS SQL Express, c. AzureSQL S3 lub nowsze. 6. Pomoc i dokumentacja programu dostępne w języku angielskim. 7. Konsola administracyjna i komunikaty klienta muszą być w języku polskim. 8. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta. 9. Serwer administracyjny musi umożliwiać instalację/dezinstalację zdalnego klienta na 10. stacjach roboczych. 11. Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a 12. serwerem zarządzającym. 13. Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie 14. informacji i zebranych danych do czasu ponownego połączenia. 15. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli. 16. System musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy 17. danych, usuwając najstarsze informacje, gdy rozmiar bazy osiągnie skonfigurowany limit. 18. Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania 19. stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego 20. pobierania. 21. Administrator musi mieć możliwość aby tworzyć, usuwać i konta administratorów w konsoli 22. programu. 23. Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych 24. modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie 25. logów modułu). 26. Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory. 27. Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą a 28. serwerem w czasie rzeczywistym. 29. Serwer administracyjny musi umożliwiać ustawienie powiadomień dla użytkownika 30. końcowego w przypadku złamania reguł związanych z ochroną DLP, z możliwością dostosowania 31. grafiki, adresu e-mail i odnośnika do polityki bezpieczeństwa. 32. Administrator musi mieć możliwość wykonać audyt stacji roboczych/użytkowników w 33. oparciu o różne czynności, takie jak uruchomione aplikacje, podłączone urządzenia, 34. odwiedzane strony internetowe, wydrukowane dokumenty, wysyłane i odebrane wiadomości email oraz czynności na plikach. 35. Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, 36. aplikacji i typów plików. 37. Administrator musi mieć możliwość filtrowania i sortowania zebranych danych. 38. Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem 39. wiadomości email. 40. Dashboardy muszą być generowane na podstawie wskazanych stacji roboczych, 41. użytkowników lub grup w określonym przedziale czasu. 42. Serwer administracyjny musi posiadać wbudowany serwer SMTP dostarczony przez 43. producenta oprogramowania. 44. Serwer administracyjny musi umożliwiać wykonywanie zadań kategoryzacji plików, zarówno 45. istniejących na stacjach roboczych i zasobach sieciowych, jak i nowo powstałych na bazie już 46. skategoryzowanych plików. 47. Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie 48. aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku. 49. Dla plików skategoryzowanych, wymagana jest możliwość tworzenia reguł dotyczących 50. blokowania i zezwalania na różne operacje, takie jak zapisywanie, przenoszenie, drukowanie, 51. wysyłanie pocztą, wysyłanie do chmury, przesyłanie komunikatorami itp. 52. Serwer administracyjny musi umożliwiać wyszukiwanie i ochronę plików w oparciu o różne 53. kryteria, takie jak numery kart kredytowych, numer PESEL, numer dowodu osobistego, numer 54. paszportu, wyrażenia regularne, określone ciągi znaków i numer IBAN. 55. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym. 56. Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM. 57. Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP. 58. Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania 59. klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania. 60. System musi ochraniać pocztę e-mail Microsoft 365, sprawdzając każdą wiadomość e-mail 61. wysyłaną przez użytkowników Microsoft 365. 62. System musi ochraniać pliki w Microsoft 365, kontrolując aktywność plików w Microsoft 63. SharePoint, Microsoft OneDrive dla Firm i Microsoft Teams. 64. System musi wykorzystywać mechanizm OCR (optical character recognition), aby wykrywać 65. poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach 66. System musi posiadać możliwość integracji z systemami do analizy danych (PowerBI, Tableau, etc.) 67. 36. System musi zapewniać możliwość zarządzanie szyfrowaniem dysków twardych oraz urządzeń wymiennych. |
| **Licencja i serwis** | Licencja wieczysta, z serwisem na minimum 12 miesięcy, obejmująca minimum 26 użytkowników. |
| **Ilość** | 1 sztuka |

# Zakup oprogramowania do backupu danych wraz z instalacją, konfiguracją i wsparciem

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Wymagania szczegółowe** | Ogólne:   * Oprogramowanie może być dostarczane w dwóch scenariuszach:   + Cloud(Software as Service),   + On-premise. * Istnieje możliwość migracji w obie strony pomiędzy środowiskiem on-premise oraz cloud. * Interfejs systemu dostępny jest w języku:   + polskim,   + angielskim, * Oprogramowanie nie preferuje platformy sprzętowej, nie jest profilowane pod konkretnego dostawcę sprzętu serwerowego oraz pamięci masowych, * Oprogramowanie może być uruchomione w kontenerze docker, * Możliwość instalacji oraz uruchomienia serwera zarządzania na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy:   + Debian: 9+   + Ubuntu: 16.04+   + Fedora: 29+   + centOS: 7+   + RHEL: 6+   + openSUSE: 15+   + SUSE Enterprise Linux (SLES): 12 SP2+   + Windows Client: 7, 8.1, 10 (1607+)   + Windows Server: 2008 R2+, * System wykonuje kopię własnej bazy danych, która umożliwia odtworzenie wszystkich ustawień i całej konfiguracji, * Oprogramowanie działa w architekturze wykluczającej pojedynczy punkt awarii(awaria jednego z komponentów nie spowoduje przestoju),   Wsparcie techniczne:   * Pomoc techniczna w językach:   + polskim,   + angielskim. * Materiały samopomocowe:   + Baza wiedzy:     - polski,     - angielski   Zarządzanie:   * Zarządzanie całością działania systemu (backup, przywracanie)z poziomu jednej konsoli webowej, * Zarządzanie całym systemem poprzez dashboardy, * Gradacja uprawnień kont administratorów z poziomu panelu zarządzającego, * System posiada wbudowane predefiniowane zadania backupowe, * System umożliwia tworzenie zadań backupowych w oparciu o kalendarz. * Automatyczne oraz ręczne uruchamianie kopii zapasowych zgodnie z ustalonym harmonogramem, * Automatyczne oraz ręczne uruchamianie procesu przywracania zgodnie z ustalonym harmonogramem, * Monitorowanie postępu działania zadania, * Posiada system powiadamiania poprzez e-mail o zdarzeniach w następujących przypadkach:   + Zadanie zostało zakończone pomyślnie,   + Zadanie zostało zakończone z ostrzeżeniami,   + Zadanie zostało zakończone z błędem,   + Zadanie zostało anulowane,   + Zadanie nie zostało uruchomione. * System generuje alerty na konsoli WEB w przypadku zaistnienia określonego zdarzenia systemowego. * Możliwość zdefiniowania okna backupowego dla każdego z zadań, * Oprogramowanie posiada wbudowany menadżer haseł do przechowywania kluczy szyfrujących oraz poświadczeń do magazynów, * System pozwala na klonowanie planów kopii zapasowych, * System umożliwia reset hasła administratora w przypadku jego utraty, * Oprogramowanie umożliwia definiowanie retencji według schematów:   + GFS(Grandfather-Father-Son),   + FIFO(First-In, First-Out). * Oprogramowanie umożliwia tworzenie kont użytkowników nie będących administratorami, * Konta użytkowników mogą być tworzone poprzez import pliku CSV, * Oprogramowanie umożliwia tworzenie grup urządzeń, * Oprogramowanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera(urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera(urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów). * System pozwala na zarządzanie multi-tenantowe - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.:   + System Administrator,   + Backup operator,   + Restore operator,   + Viewer.   Składowanie danych:   * Oprogramowanie jest systemem multi-storageowym i umożliwia tworzenie wielu repozytoriów danych jednocześnie, * System umożliwia składowanie danych:   + Lokalnie:     - Zasób SMB,     - Zasób NFS,     - Zasób ISCSI,     - Zasób S3,     - Katalog zabezpieczonego urządzenia.   + W chmurze:     - Amazon Web Service,     - Magazyn zgodny z S3,     - Dostarczanej przez producenta. * System pozwala na zdefiniowanie zapasowej ścieżki repozytorium, na wypadek niedostępności głównej lokalizacji, * System oferuje mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.   Odtwarzanie:   * Odtwarzanie granularne:   + Pojedynczych plików z kopii obrazu dysku,   + Pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365, * Wykorzystanie funkcjonalności Bare Metal Restore(kopii zapasowej całego dysku - łącznie z partycjami i danymi startowymi) dla odtwarzania systemu po awarii, wsparcie dostępne jest dla systemów:   + Windows: 7+,   + Windows Server: 2008 R2+, * Odtwarzanie Bare metal Restore może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika. * Uruchamianie procesu Bare Metal Restore odbywa się z bootowalnej płyty CD lub pendrive’a, * Oprogramowanie umożliwia odtwarzanie systemu w scenariuszach: P2P, P2V, V2P, V2V. * Oprogramowanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie(VHD, VHDX, VMDK), * Odtwarzanie zasobów plikowych bez praw dostępu(tzw. ACL), * Odtwarzanie zasobów plikowych z prawami dostępu, * Przywracanie plików pomiędzy systemami operacyjnymi(np. odtwarzanie danych plikowych Linux na systemie Windows), * Odtwarzanie danych według harmonogramu, * Przywracanie danych z określonego urządzenia/użytkownika, * Przywracanie kopii z wybranego magazynu. * Przywracanie danych Microsoft 365:   + do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku:     - pst,     - mbox.   + do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji), * System posiada możliwość nieodwracalnego kasowania danych, * Przywracanie repozytoriów GIT:   + Przywracanie pomiędzy hostingami repozytoriów(GitHub/BitBucket),   + przywracanie między kontami.   Backup:   * Wykonywanie pełnych, różnicowych, przyrostowych kopii zapasowych, a także backupu syntetycznego dla:   + Systemów operacyjnych:     - Alpine 3.10+,     - Debian: 9+,     - Ubuntu: 16.04+,     - Fedora: 29+,     - centOS: 7+,     - RHEL: 6+,     - openSUSE: 15+,     - SUSE Enterprise Linux(SLES): 12 SP2+,     - macOS: 10.13+,     - Windows: 7, 8.1, 10(1607+),     - Windows Server: 2008 R2+,   + Środowisk wirtualnych:     - Hyper-V,     - VMware: 6.7+.   + Repozytoriów GIT:     - GitHub,     - Bitbucket. * Wykonywanie pełnych, różnicowych oraz przyrostowych oraz logów transakcyjnych kopii zapasowych dla:   + Baz danych**:**     - Microsoft SQL,     - MySQL,     - PostgreSQL,     - Firebird,     - Dowolnych innych przez podpięcie skryptów pre/post. * Szyfrowanie danych wykonywana po stronie stacji roboczej za pomocą algorytmu AES w trybie CBC z kluczem szyfrującym o długości:   + 128 bit,   + 192 bit,   + 256 bit. * Kompresja danych wykonywana po stronie stacji roboczej za pomocą algorytmów:   + ZStandard,   + LZ4. * Oprogramowanie umożliwia zarządzanie poziomem kompresji, * Wykonywanie kopii zapasowej otwartych plików(VSS), * System umożliwia uruchamianie skryptów przed i po backupie, * System umożliwia uruchamianie skryptów po wykonaniu migawki VSS, * System umożliwia automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku błędów, * Backup jednego oraz wielu dysków/całego systemu operacyjnego(Windows) ze wsparciem dla partycji MBR oraz GPT, * Backup plikowy, * Oprogramowanie realizuje funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie dyskowe, * Oprogramowanie umożliwia konsolidację wersji kopii zapasowych, * Oprogramowanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia, * Oprogramowanie pozwala na automatyczne uruchomienie kopii zapasowej podczas zamykania systemu operacyjnego. * Oprogramowanie pozwala na backup zaszyfrowanych partycji.   GIT   * Oprogramowanie zapewnia wsparcie dla repozytoriów lokalnych oraz zdalnych(dostępnych w usługach zewnętrznych), * Oprogramowanie umożliwia zabezpieczenie metadanych repozytoriów(w zależności od zabezpieczanej usługi m.in.: issues, pull requests, actions/pipelines, wiki).   Licencjonowanie:   * Sposób licencjonowania opiera się na:   + Ilości serwerów/endpointów- dla fizycznych urządzeń,   + Ilości fizycznych hostów - dla środowisk wirtualnych,   + Ilości repozytoriów - dla GIT. * **Licencje powinny pozwalać na zabezpieczenie:**   + 28 stacji roboczych,   + 1 fizyczny serwer bez wirtualizacji. * Wsparcie techniczne: * Świadczone jest w języku polskim, bezpośrednio przez główną siedzibę producenta, * Zapewnia dostęp do aktualizacji oprogramowania, * Umożliwia korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego, * Obowiązuje przez okres minimum **18 miesięcy.** |
| **Ilość** | 1. sztuka |

# Zakup oprogramowania antywirusowego -przedłużenie licencji dla Urzędu Gminy

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla oprogramowania** |
| **Typ** | Oprogramowanie antywirusowe dla Urzędu Gminy |
| **Wymagania podstawowe** | Zamawiający posiada oprogramowania Eset Protect Advanced. Zamawiający wymaga przedłużenia posiadanych licencji oprogramowania antywirusowego dla min. 34 stanowisk na okres 12 miesięcy.  Zamawiający dopuszcza dostarczenia rozwiązania równoważnego. W przypadku dostarczenia rozwiązania równoważnego, Zamawiający wymaga:  - odinstalowania posiadanego rozwiązania  - zainstalowania i skonfigurowania nowego dostarczonego rozwiązania  - przeszkolenia administratora z dostarczonego rozwiązania |
| Wymagania dotyczące rozwiązania równoważnego | |
| **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 32 i 64-bitową systemu Windows. 3. Rozwiązanie musi wspierać architekturę ARM64. 4. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 5. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. 6. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 7. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 8. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 9. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. 10. 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. 11. Rozwiązanie musi integrować się z Intel Threat Detection Technology. 12. 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). 13. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 14. 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. 15. 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. 16. 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. 17. 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. 2. 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. 3. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. 4. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 5. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 6. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook. 7. 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 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. 9. Dodatkowe wymagania dla ochrony serwerów Windows: 10. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. 11. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS). 12. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. 13. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 14. 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. 15. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 16. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 17. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. 18. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu. 19. Dodatkowe wymagania dla ochrony serwerów Linux: 20. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. 21. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. 22. 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 10 i Microsoft Windows 11. 2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault). 3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia. 4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI. |
| **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:   a. usunięcie zawartości urządzenia,  b. przywrócenie urządzenie do ustawień fabrycznych,  c. zablokowania urządzenia,  d. uruchomienie sygnału dźwiękowego,  e. lokalizację GPS.   1. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. 2. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:   a. nazwę aplikacji,  b. nazwę pakietu,  c. kategorię sklepu Google Play,  d. uprawnienia aplikacji,  e. pochodzenie aplikacji z nieznanego źródła. |
| **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:   a) Czysty,  b) Podejrzany,  c) Bardzo podejrzany,  d) Szkodliwy.   1. 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. 2. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki. 3. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia. |
| **Licencja** | Licencja obejmująca min 34 stanowiska, ważna min 12 miesięcy |
| **Ilość** | 1 szt. |