

**Opis przedmiotu zamówienia (OPZ)**

Zamówienie współfinansowane ze środków:

FUNDUSZY EUROPEJSKICH NA ROZWÓJ CYFROWY  
2021-2027 (FERC)

Priorytet II: Zaawansowane usługi cyfrowe

Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

Nazwa zamówienia: **Dostawa i montaż urządzeń i oprogramowania w ramach projektu „Wzmocnienie cyberbezpieczeństwa w Urzędzie Gminy Lubartów”**

Zamawiający: Gmina Lubartów

Czerwiec 2025

**Wymagania ogólne dla urządzeń i oprogramowania sieciowego.**

* Dostarczony sprzęt musi być wolny od wad prawnych i fizycznych oraz nienoszący oznak użytkowania.
* Dostarczony sprzęt musi być fabrycznie nowy (tzn. wyprodukowane nie wcześniej, niż na 9 miesięcy przed ich dostarczeniem), musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez producenta dla oferowanego modelu sprzętu.
* Niedopuszczalne są produkty prototypowe, nie dopuszcza się urządzeń długotrwale magazynowanych oraz pochodzących z programów wyprzedażowych producenta. Urządzenia nie mogą znajdować się na liście „end-of-sale” oraz „end-of-support” producenta.
* Wymagana ilość i rozmieszczenie (na zewnątrz obudowy) jakichkolwiek portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, itp., niedopuszczalne jest zastosowanie jakichkolwiek zewnętrznych przejściówek czy konwerterów.
* Wszystkie urządzenia będą zasilane bezpośrednio z sieci 230V.
* Całość sprzętu i oprogramowania objętego zamówieniem musi zostać zainstalowana i skonfigurowana zgodnie z wymaganiami opisanymi poniżej.
* Wykonawca jest odpowiedzialny za skonfigurowanie połączeń fizycznych, logicznych, podłączenie i skonfigurowanie urządzenia do działania, pozwalające na rozpoczęcie pracy oraz dostarczenie odpowiedniej ilości kabli zasilających, połączeniowych w celu przygotowania zamawianego sprzętu do działania.
* Wykonawca zobowiązany jest do skonfigurowania zamawianego sprzętu w uzgodnieniu z Zamawiającym.
* Prace instalacyjne będzie można realizować wyłącznie w terminach uzgodnionych z Zamawiającym.
* Wykonawca będzie zobowiązany do złożenia dokumentacji powykonawczej, zawierającej w szczególności wszystkie dane dostępu do urządzeń i oprogramowania, które będą wykorzystywane podczas instalacji i konfiguracji sprzętu i oprogramowania.
* Dla dostaw sprzętu informatycznego z systemem operacyjnym Zamawiający wymaga fabrycznie nowego systemu operacyjnego (nieużywanego nigdy wcześniej), w wersji z certyfikatem autentyczności dla każdej licencji, o ile producent oferowanego oprogramowania stosuje certyfikaty autentyczności. Wykonawca zobowiązany jest do dostarczenia fabrycznie nowego systemu operacyjnego nieużywanego oraz nigdy wcześniej nieaktywowanego na innym urządzeniu oraz pochodzącego z legalnego źródła sprzedaży. W przypadku systemu operacyjnego naklejka hologramowa winna być zabezpieczona przed możliwością odczytania klucza za pomocą zabezpieczeń stosowanych przez producenta, o ile producent oferowanego oprogramowania stosuje takie zabezpieczenia. Zamawiający zastrzega możliwość weryfikacji dostarczonego oprogramowania na etapie oceny ofert jak i na etapie dostawy pod kątem legalności oprogramowania bezpośrednio u producenta oprogramowania. Zamawiający zastrzega możliwość żądania od Wykonawcy na etapie dostawy przedstawienia dokumentów dotyczących zakupu oprogramowania w autoryzowanym kanale dystrybucyjnym producenta oprogramowania.

**Wymagania gwarancyjne.**

* na dostarczany sprzęt musi być udzielona min. 36 miesięczna gwarancja, oparta na gwarancji producenta, chyba że zapisy szczegółowe w danej pozycji sprzętu stanowią inaczej;
* serwis gwarancyjny świadczony ma być w miejscu instalacji sprzętu;
* czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć jednego dnia roboczego;
* Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon (w godzinach pracy Wnioskodawcy), fax, e-mail lub WWW (przez całą dobę); Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń dla dostarczanych rozwiązań. Każde zgłoszenie należy potwierdzić drogą pisemną lub elektroniczną w postaci potwierdzenia przyjęcia zgłoszenia;
* Zamawiający otrzyma dostęp do pomocy technicznej (telefon, e-mail lub WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Zamawiającego;
* wszystkie dostarczane moduły muszą pochodzić od producenta urządzeń sieciowych i być objęte serwisem gwarancyjnym opartym na świadczeniach producenta sprzętu;

UWAGA. Powyższe zapisy gwarancyjne znajdują zastosowanie w każdym przypadku i podlegają modyfikacji o uregulowania szczególne znajdujące w dalszej części SOPZ.

**Miejsce instalacji sprzętu i oprogramowania/systemu.**

* Wykonawca zapewni dostawę do wskazanej lokalizacji w siedzibie Zamawiającego.
* Dostarczony sprzęt i oprogramowanie powinny zostać zamontowane, zainstalowane i skonfigurowane zgodnie z wymaganiami opisanymi w dalszej części dokumentu.

**Zestawienie zakresu dostaw.**

1. Punkt dostępowy – 6 szt.
2. Switch – 6 szt.
3. Serwer – 2 szt.
4. Macierz – 1 szt.
5. UTM – 1 szt.
6. Urządzenie do zbierania logów – 1 szt.
7. UPS – 1 szt.
8. System do badania podatności – 1 szt.
9. Oprogramowanie DLP – 1 szt.
10. Oprogramowanie do zarządzania infrastrukturą IT – 1 szt.

|  |  |
| --- | --- |
| **Punkt dostępowy – 6 szt.** | |
| Interfejs sieciowy | Min. 2 porty GbE RJ45 |
| Port USB | Tak |
| Standard Wi-Fi | 802.11 a  802.11 ac  802.11 b  802.11 g  802.11 k  802.11 n  802.11 r  802.11 v |
| Częstotliwość pracy | 2.4 GHz  5 GHz |
| Montaż | Ścienne, sufitowe |
| Bezpieczeństwo sieci | WEP, WPA-PSK, WPA-Enterprise (WPA/WPA2, TKIP/AES) |
| Gwarancja | Minimum 12 miesięcy. |

|  |  |
| --- | --- |
| **Switch – 6 szt.** | |
| Typ obudowy | RACK |
| Interfejs sieciowy | Porty GbE RJ45 – min. 48  Porty SFP+ 1/10G – min. 4 |
| Zarządzanie | Zarządzalny L3 |
| Wilgotność robocza | 10-90% |
| Temperatura otoczenia pracy | -5 do 45 °C |
| Gwarancja | Minimum 12 miesięcy. |

|  |  |
| --- | --- |
| **Serwer – 2 szt.** | |
| Parametr | Charakterystyka (wymagania minimalne). |
| Obudowa | * Obudowa Rack o wysokości max 2U, * 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 56 rdzeniowych, * Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym, * Na płycie głównej powinno znajdować się minimum 32 sloty przeznaczone do instalacji pamięci, * Płyta główna powinna obsługiwać do 8TB pamięci RAM. |
| Chipset | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych. |
| Procesor | Zainstalowane dwa procesory min. 12-rdzeniowe klasy x86, min. 2GHz, dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 216 punktów w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej |
| RAM | Minimum 4 x 64GB DDR5 RDIMM 5600MT/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:   + 2x dysk SSD SATA o pojemności min. 480GB, 6Gb/s, Hot-Plug,   + Zainstalowane 2 dyski SSD NVMe (RAID1) o pojemności min. 240GB pełniące funkcję optymalizacji rozruchu. |
| Gniazda PCI | Min. osiem slotów PCIe. |
| Interfejsy sieciowe/FC/SAS | Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT, 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) oraz 2 porty 32Gb FibreChannel |
| Wbudowane porty | * 4 porty USB w tym min:   + 1 port USB 3.0 z tyłu obudowy,   + 1 port micro USB z przodu obudowy. * 2 port VGA z czego jeden z przodu obudowy, * Możliwość rozbudowy o port RS232. |
| Video | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024. |
| Wentylatory | Redundantne, Hot-Plug. |
| Zasilacze | Redundantne, Hot-Plug min. 1000W 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. |
| 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 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 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,   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. |
| System operacyjny | System operacyjny – fabrycznie nowy, nieużywany, nie pochodzący z recyklingu, z licencją na czas nieoznaczony, nie naruszający praw osób trzecich; System operacyjny wraz ze wszystkimi wymaganymi sterownikami podzespołów ma być zainstalowany lub preinstalowany na oferowanym urządzeniu komputerowym. Zabrania się instalowania lub preinstalowania systemu operacyjnego w jakimkolwiek środowisku wirtualnym. Zamawiający nie dopuszcza zaoferowania systemu operacyjnego, programów i planów licencyjnych opartych o rozwiązania chmurowe oraz rozwiązań wymagających wnoszenia przez Zamawiającego jakichkolwiek dodatkowych opłat związanych z użytkowaniem zakupionego systemu operacyjnego. Zamawiający wymaga, aby wszystkie elementy systemu operacyjnego oraz jego licencja pochodziły od tego samego producenta.  MS Windows Server 2022 Standard wersja polskojęzyczna z nieujawnianym wcześniej, nieaktywowanym wcześniej kluczem licencyjnym, pochodzący z oficjalnej sieci dystrybucji firmy Microsoft® pozwalający na utworzenie 6 wirtualny maszyn wraz z licencjami dostępowymi CAL dla 50 użytkowników lub równoważny.  Warunki równoważności:  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 2012 musi także być dostarczona możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server.  5. Licencja na system operacyjny musi być licencją stałą, 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: a) zarządzania użytkownikami, b) zarządzania certyfikatami dla użytkowników wraz ze wsparciem możliwości logowania do domeny kartą mikroprocesorową, c) możliwości przydzielania praw dostępu do zasobów sieciowych, d) instalacji zdalnej oprogramowania z pakietów msi, e) definiowania polityk bezpieczeństwa dla użytkowników, grup oraz stacji roboczych z systemami MS Windows: 7,8,8.1, 10. 11.  10. System operacyjny musi wspierać pracę domenową wraz z automatyczną synchronizacją dla dodatkowych serwerów.  11. System operacyjny musi wspierać zarządzanie przez dostępne narzędzia administracji serwera dla systemu Windows 10 (RSAT) oraz Windows Admin Centre.  12. System operacyjny musi posiadać obsługę zdalnego pulpitu poprzez protokół RDP.  13. System operacyjny musi umożliwiać ustawianie relacji zaufania pomiędzy domenami.  14. Wszystkie narzędzia i usługi systemu operacyjnego powinny być rozwiązaniem jednego producenta.  15. System operacyjny musi posiadać obsługę pamięci USB jako monitora klastra.  16. System operacyjny musi pozwalać na stopniowe uaktualnienia systemu operacyjnego klastra.  17. System operacyjny musi posiadać obsługę deduplikacji na potrzeby systemu plików ReFS.  18. System operacyjny musi posiadać obsługę optymalizacji transportu w tle pod kątem opóźnień.  19. 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.  20. System operacyjny musi posiadać możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny.  21. System operacyjny musi posiadać możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu.  22. System operacyjny musi posiadać domyślną obsługę PowerShell 5.1.  23. System operacyjny musi posiadać obsługę certyfikatów w Active Directory.  24. Wszystkie wymienione powyżej parametry, role, funkcje, itp. systemu operacyjnego objęte musza być dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).  Wymagania dla równoważnych licencji dostępowych dla urządzenia: - Licencja dostępowa dla urządzenia umożliwiająca podłączenie i wykorzystywanie wszystkich dostępnych funkcjonalności serwera Microsoft Windows Server 2022 typu Device Cal z wdrożoną rolą Active Directory. - Każda z licencji musi pozwalać na dostęp wielu użytkowników z jednego, licencjonowanego urządzenia do zasobów serwera. W przypadku zaproponowania przez Dostawcę oprogramowania równoważnego zobowiązuje się on do: − wdrożenia oprogramowania oraz przeprowadzenia certyfikowanych szkoleń dla użytkowników oferowanego rozwiązania w wymiarze co najmniej 40 godzin. − pokrycia wszelkich możliwych kosztów, wymaganych w czasie wdrożenia oferowanego rozwiązania, w szczególności związanych z dostosowaniem infrastruktury informatycznej, oprogramowania nią zarządzającego, systemowego i narzędziowego (licencje, wdrożenie), serwisu gwarancyjnego oraz kosztów certyfikowanych szkoleń dla administratorów i użytkowników oferowanego rozwiązania. |
| 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 aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania,   + możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania,   + możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiązań HCI, wraz z informacją o zalecanych wersjach oprogramowania,   + możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania,   + możliwość aktualizacji 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, * 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 min. 5 lat, * Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet, * 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 / 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 – oświadczenie potwierdzające należy załączyć do oferty. |
| Zakres wdrożenia | Przygotowanie serwera:   * Rozpakowanie i fizyczne połączenie serwera, * Konfiguracja macierzy RAID (jeśli wymagana), * Ustawienia BIOS/UEFI (włączenie wirtualizacji, kolejności bootowania).   Instalacja systemu:   * Instalacja systemu z nośnika lub pliku ISO, * Wybór wersji serwera (np. Standard, Datacenter), * Konfiguracja partycji dysków.   Aktualizacje systemu:   * Instalacja najnowszych poprawek i aktualizacji, * Instalacja sterowników urządzeń.   Konfiguracja nazwy i sieci:   * Nadanie unikalnej nazwy serwera, * Konfiguracja adresu IP (statycznego) oraz maski podsieci, bramy i DNS.   Dodanie ról i funkcji:   * Instalacja ról (Server Manager): * Active Directory Domain Services (jeśli konfigurujesz kontroler domeny), * DHCP, DNS, File Server (jeśli wymagane).   Konfiguracja Active Directory:   * Promowanie serwera do roli kontrolera domeny (jeśli to domena), * Utworzenie nowej domeny lub dołączenie do istniejącej.   Instalacja platformy wirtualizacji:   * Instalacja, * Konfiguracja hosta wirtualizacji (nazwa, adres IP, dostęp przez konsolę). |

|  |  |
| --- | --- |
| **Macierz – 1 szt.** | |
| Obudowa | Do instalacji w standardowej szafie RACK 19” rozwiązanie może zajmować maksymalnie 2U i pozwalać na instalacje 24 dysków 2.5”.  Posiadająca dodatkowy przedni panel zamykany na klucz, chroniący dyski twarde przed nieuprawnionym wyjęciem z serwera. |
| Kontrolery | Dwa kontrolery RAID pracujące w układzie active-active (dual-active) posiadające łącznie minimum osiem portów 25Gb SFP28. |
| Procesory | Kompatybilny z płytą główną. |
| Cache | 16GB na kontroler, pamięć cache zapisu mirrorowana między kontrolerami. Całkowita ilość cache 32GB, |
| Dyski | Zainstalowane 12 dysków Hot-Plug o pojemności nie mniejszej niż 1.92TB SSD SAS ss24Gb 1DWPD.  Możliwość rozbudowy przez dokładanie kolejnych dysków/półek dyskowych tak by uzyskać łącznie nie mniej niż 264 dysków. Możliwość mieszania typów dysków w obrębie macierzy oraz pojedynczej półki. |
| Oprogramowanie/  Funkcjonalności | Zarządzanie macierzą poprzez minimum przeglądarkę internetową, GUI oparte o HTML5. Powiadamianie mailem o awarii. Macierz powinna zostać dostarczona z licencją umożliwiającą utworzenie minimum 512 LUN’ów oraz 1024 kopii migawkowych na całą macierz.  Licencja zaoferowanej macierzy powinna umożliwiać podłączanie minimum 8 hostów bez konieczności zakupu dodatkowych licencji.  Konieczne jest posiadanie automatycznego, bez interwencji człowieka, rozkładania danych między dyskami poszczególnych typów (tzw. auto-tiering). Dane muszą być automatycznie przemieszczane między rożnymi typami dysków.  Możliwość wykorzystania dysków SSD jako cache macierzy.  Macierz musi posiadać funkcjonalność zdalnej replikacji danych do macierzy tej samej rodziny w trybie asynchronicznym. |
| Bezpieczeństwo | Ciągła praca obu kontrolerów nawet w przypadku zaniku jednej z faz zasilania. Zasilacze, wentylatory, kontrolery RAID redundantne. |
| Wentylatory | Redundantne. |
| Zasilacz | Redundantny, Hot-Plug maksymalnie 580W. |
| Diagnostyka | Poprzez kartę zarządzającą. |
| Certyfikaty | Macierz musi być wyprodukowany zgodnie z normą  ISO-9001:2015  Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzację producenta – oświadczenie potwierdzające załączyć do oferty  Serwer musi posiadać deklaracja CE. |
| Warunki gwarancji | 60 miesięcy gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Możliwość rozszerzenia gwarancji do 7 lat.  Wymagane dołączenie do oferty oświadczenia Producenta  potwierdzające, że w przypadku awarii dyski zostają u zamawiającego przez okres trwania gwarancji. |
| Dokumentacja użytkownika | Zamawiający wymaga dokumentacji w języku polskim lub angielskim.  Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |
| Zakres wdrożenia | Fizyczne podłączenie macierzy:   * Umieszczenie macierzy w szafie rack i jej montaż, * Podłączenie do zasilania (redundantne zasilacze), * Podłączenie kabli do serwerów, przełączników SAN lub urządzeń sieciowych.   Włączenie i pierwsze uruchomienie:   * Sprawdzenie stanu macierzy (np. poprzez diody LED kontrolerów i dysków), * Wykonanie wstępnych ustawień sieciowych (adresy IP kontrolerów).   Konfiguracja RAID:   * Wybór poziomu RAID (np. RAID 5, 6, 10) zgodnie z wymogami wydajności i bezpieczeństwa. * Tworzenie grup dyskowych i logicznych wolumenów (LUN).   Zarządzanie pojemnością:   * Podział przestrzeni na wolumeny zgodnie z wymaganiami aplikacji i systemów.   Sieciowa konfiguracja macierzy:   * Konfiguracja interfejsów FC/iSCSI lub NFS/SMB. * Konfiguracja LUN Masking (przypisywanie wolumenów do konkretnych hostów). |

|  |  |
| --- | --- |
| **UTM – 1 szt.** | |
| 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.  System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT,  transparentnym oraz monitorowania na porcie SPAN.  System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w  zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 7 administratorów do poszczególnych instancji systemu.  System wspiera protokoły IPv4 oraz IPv6 w zakresie:   * Firewall, * Ochrony w warstwie aplikacji, * Protokołów routingu dynamicznego. |
| Redundancja, monitoring i wykrywanie awarii | 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.  2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów  zabezpieczeń oraz łączy sieciowych.  3. Monitoring stanu realizowanych połączeń VPN.  4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych. |
| Interfejsy, Dysk, Zasilanie | 1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem  interfejsów:   * 8 portami Gigabit Ethernet RJ-45, * 2 gniazdami SFP+ 10 Gbps.   2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.  3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q.  4. System jest wyposażony w zasilanie AC. |
| Parametry wydajnościowe | 1. W zakresie Firewall’a obsługa nie mniej niż 1.5 mln jednoczesnych połączeń oraz 120 tys. nowych połączeń na sekundę.  2. Przepustowość Stateful Firewall: nie mniej niż 28 Gbps dla pakietów 512 B.  3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6.5 Gbps.  4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 25 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 4 Gbps.  6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2 Gbps.  7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 2.5 Gbps. |
| Funkcje Systemu Bezpieczeństwa | W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane  w postaci osobnych, komercyjnych platform sprzętowych lub programowych:  1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.  2. Kontrola Aplikacji.  3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.  4. Ochrona przed malware.  5. Ochrona przed atakami - Intrusion Prevention System.  6. Kontrola stron WWW.  7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.  8. Zarządzanie pasmem (QoS, Traffic shaping).  9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).  10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.  11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.  12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze  DNS jak i w ruchu przechodzącym przez system.  13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa). |
| Polityki, Firewall | 1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.  2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:   * Translację jeden do jeden oraz jeden do wielu. * Dedykowany ALG (Application Level Gateway) dla protokołu SIP.   3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np.  DMZ, LAN, WAN.  4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.  5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.  6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.  7. Element systemu realizujący funkcję Firewall 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.   2. 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.   2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.  3. 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.  4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. |
| Zarządzanie | 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.  2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.  3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.  4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.  5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.  6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.  7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.  8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).  9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP. |
| Logowanie | 1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.  2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.  3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.  4. Możliwość włączenia logowania per reguła w polityce firewall.  5. System zapewnia możliwość logowania do serwera SYSLOG.  6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS. |
| Testy wydajnościowe oraz funkcjonalne | 1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy. |
| Serwisy i licencje | Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:  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 nie krótszy niż do 18 czerwca 2026 r. |
| Wdrożenie | 1. Rejestracja urządzeń oraz licencji:   * Rejestracja urządzeń w systemie:   + Proces dodawania nowych urządzeń do systemu zarządzania,   + Konfiguracja parametrów urządzeń oraz weryfikacja poprawności rejestracji,   + Automatyczne wykrywanie urządzeń i integracja z istniejącymi zasobami. * Zarządzanie licencjami i subskrypcjami:   + Przegląd dostępnych licencji i subskrypcji,   + Procedury aktywacji i odnawiania licencji,   + Monitorowanie zużycia licencji oraz optymalizacja kosztów.   2. Aktualizacja oprogramowania i zmiana danych dostępowych:   * procedura aktualizacji oprogramowania:   + Przeprowadzanie aktualizacji firmware'u i oprogramowania urządzeń,   + Zasady bezpiecznego przeprowadzania aktualizacji (kopie zapasowe, testowanie),   + Automatyzacja procesu aktualizacji i harmonogramowanie. * Zmiana danych dostępowych (autoryzacja) do urządzeń:   + Procedury zmiany haseł i danych autoryzacyjnych,   + Implementacja polityk zmiany haseł i zarządzania dostępem,   + Audytowanie i zabezpieczanie danych dostępowych.   3. Konfiguracja metod dostępu i segmentacji sieci:   1. Konfiguracja metod dostępu do urządzeń:    * Konfiguracja \dDostępu SSH i HTTPS:      + Implementacja i konfiguracja bezpiecznego dostępu do urządzeń,      + Zarządzanie certyfikatami SSL/TLS.    * Wdrożenie dwuetapowej autoryzacji (2FA):      + Implementacja 2FA dla zwiększenia bezpieczeństwa dostępu,      + Konfiguracja aplikacji autoryzujących i tokenów sprzętowych. 2. Konfiguracja łącz dostępowych do internetu i redundancji:    * Ustawienie podstawowych łącz internetowych:      + Konfiguracja głównych połączeń internetowych,      + Monitorowanie i optymalizacja wydajności łączy.    * Konfiguracja łącz zapasowych i redundancji (WAN):      + Implementacja zapasowych łączy internetowych,      + Konfiguracja mechanizmów przełączania awaryjnego i load balancingu. 3. Segmentacja sieci LAN:    * Konfiguracja interfejsów sieciowych:      + Ustawienia interfejsów fizycznych i logicznych,      + Optymalizacja parametrów interfejsów dla różnych zastosowań.    * Konfiguracja VLAN i polityk dostępu do podsieci/VLAN:      + Tworzenie i zarządzanie VLANami,      + Implementacja polityk bezpieczeństwa dla poszczególnych VLANów.   4. Zarządzanie siecią i polityki bezpieczeństwa:   1. Uruchomienie serwerów DHCP:    * Konfiguracja serwerów DHCP na poszczególnych podsieciach/VLAN:      + Ustawienia serwerów DHCP dla dynamicznego przydzielania adresów IP,      + Zarządzanie pulami adresów i rezerwacjami. 2. Konfiguracja routingu i agregacji portów:    * ustawienia routingu statycznego i dynamicznego:      + Konfiguracja tras statycznych i protokołów routingu dynamicznego (OSPF, BGP),      + Optymalizacja trasowania i zarządzanie tablicami routingu.    * konfiguracja agregacji portów dla zwiększenia przepustowości:      + Implementacja agregacji portów (LACP),      + Balansowanie obciążenia i redundancja portów. 3. Polityki Bezpieczeństwa:    * filtrowanie i blokowanie treści oraz aplikacji internetowych:      + Konfiguracja filtrów treści i aplikacji,      + Zarządzanie czarnymi i białymi listami.    * konfiguracja antywirusa, filtrów DNS, IPS i DLP:      + Implementacja zabezpieczeń antywirusowych i systemów wykrywania intruzji (IPS),      + Konfiguracja filtrów DNS i polityk zapobiegania wyciekom danych (DLP).   5. Integracja i zarządzanie systemem:   1. Integracja z domena:    * Konfiguracja urządzeń do współpracy z domena:      + Procedury integracji z domeną Active Directory,      + Zarządzanie kontami i politykami bezpieczeństwa domeny. 2. Konfiguracja SNMP:    * Ustawienia SNMP do monitorowania sieci:      + Konfiguracja protokołu SNMP dla monitorowania i zarządzania urządzeniami sieciowymi,      + Implementacja pułapek SNMP i zbieranie danych z urządzeń.   6. Logowanie, kopie Zapasowe i VPN:   1. Konfiguracja procesu logowania:    * Konfiguracja zawartości logów i okresu przechowywania:      + Definiowanie typów logów, które mają być przechowywane,      + Ustalanie okresów retencji logów i zarządzanie przestrzenią dyskową. 2. Wykonanie kopii zapasowej ustawień urządzeń:    * procedury tworzenia kopii zapasowych i przywracania ustawień:      + Automatyzacja tworzenia kopii zapasowych ustawień urządzeń,      + Procedury przywracania ustawień z kopii zapasowych. 3. Konfiguracja tuneli VPN IPsec / SSL:    * Konfiguracja tuneli VPN typu IPsec i SSL:      + Tworzenie i zarządzanie tunelami VPN dla bezpiecznej komunikacji,      + Konfiguracja polityk bezpieczeństwa VPN i zarządzanie certyfikatami.   Wdrożenie musi być prowadzone przez jednego certyfikowanego inżyniera, (nie dopuszcza się łączenia certyfikatów przez dwóch lub więcej inżynierów ze względu na poziom bezpieczeństwa oferowanej usługi), posiadającym co najmniej 4 aktywne certyfikaty producenta oferowanego rozwiązania na poziomie specjalista. |
| Gwarancja oraz wsparcie | System jest objęty serwisem gwarancyjnym producenta przez okres nie krótszy niż do 18 czerwca 2026 r., polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |
| Rozszerzone wsparcie serwisowe AHB/SOS | System jest objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres nie krótszy niż do 18 czerwca 2026 r. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7 Wymagania powinny być potwierdzone dokumentami:   * Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne  o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej), * Certyfikat ISO 9001 podmiotu serwisującego. |
| Opisy do wymagań ogólnych | 1. Zaleca się, aby zostało uzyskane oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.  2. Wykonawca wraz z ofertą winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, potwierdzające, że posiada odpowiednią wiedzę i doświadczenie, potwierdzone co najmniej 7 aktywnymi specjalizacjami, a także posiada autoryzację producenta do sprzedaży oferowanych rozwiązań. |

|  |  |
| --- | --- |
| **Urządzenie do zbierania logów – 1 szt.** | |
| Procesor | Czterordzeniowy o taktowaniu co najmniej 2,2 GHz |
| Obudowa | Rack 2U o wymiarach 88 × 482 × 306,6 mm + szyny do montażu w szafie rack. |
| Pamięć RAM | 32GB DDR4 ECC SODIMM RAM |
| Ilość obsługiwanych dysków | 8 dysków 3,5" lub 2,5" SATA HDD/SSD |
| Interfejsy sieciowe | 4 porty 1GbE RJ-45 |
| Porty | 2 x USB3.2 1 generacji, 1 x eSATA |
| Port PCIe | 1 x Gen3 x8 slot (x4 link) |
| Wskaźniki LED | Wskaźnik zasilania, Wskaźnik stanu, Wskaźnik alertów, Wskaźnik stanu dysków 1-8, Wskaźniki zasilacza. |
| Obsługa RAID | Synology Hybrid RAID, Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 |
| Funkcje RAID | Możliwość zwiększania pojemności i migracja między poziomami RAID online. |
| Szyfrowanie | Możliwość szyfrowania wybranych udziałów sieciowych, kluczem AES-256bitów. |
| System Operacyjny | Windows® 7 i nowsze, macOS® 10.12 i nowsze. |
| Licencja na Kamery IP | W zestawie licencja na dwie kamery z możliwością rozszerzenia do 40. |
| Protokoły | SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP, VPN (PPTP, OpenVPN™, L2TP) |
| Usługi | Wsparcie dla High Availability, Serwer VPN, Central Management System, Serwer pocztowy dla kilku domen, Stacja monitoringu, Windows ACL, Time Backup, Integracja z Windows ADS, Firewall z kontrolą ruchu, Serwer wydruku, Serwer WWW, Serwer plików, Manager plików przez WWW, Floating Point, Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie, Antyvirus, Klient VPN, Cloud Station, Usługa DDNS, wysyłanie powiadomień z konta Skype i Microsoft Messenger, Certyfikaty Citrix, VMware vSphere**,**Zarządzanie przez komórkę, Virtual Drive, Serwer i klient LDAP, Możliwość utworzenia kilku wolumenów, MailPlus, praca w klastrze (HA), backup plików bez instalowania aplikacji klienckiej na komputerze, możliwość tworzenia backupu z maszyn wirtualnych bez konieczności kupowania dodatkowych licencji. |
| Zarządzanie dyskami | SMART, sprawdzanie złych sektorów, dynamiczne mapowanie uszkodzonych sektorów. |
| Język GUI | Polski |
| Gwarancja | 60 miesięcy   * + pomoc telefoniczna lub e-mailowa przy uruchomieniu i wdrożeniu produktu,   + wsparcie techniczne w przypadku problemów ze współpracą z innymi elementami sieci,   + pełna asysta telefoniczna / e-mailowa przy aktualizacji oprogramowania,   + pomoc techniczna w sprawach nietypowych, modyfikacjach oprogramowania itp.   + gwarancja „door-door” w całości pokrywana przez oficjalnego dystrybutora,   + priorytetowy tryb rozpatrywania gwarancji i prowadzenia naprawy |
| Waga | 6.9kg |
| Pobór mocy | 49.89 W (dostęp), 22.64 W (hibernacja dysku twardego (HDD)) |
| System plików | Dyski wewnętrzne Btrfs, EXT4. Dyski zewnętrzne Btfrs, FAT, NTFS, EXT4, EXT3, HFS+, exFAT |
| Liczba wolumenów | 64 |
| Liczba iSCSI Targetów | 128 |
| Liczba iSCSI LUN | Do 256 |
| Liczba kont użytkowników | 1500 |
| Liczba grup | 256 |
| Liczba folderów udostępnionych | 512 |
| Maks. liczba zadań synchr. folderów udostępnionych | 16 |
| Ilość jednoczesnych połączeń | 1000 dla SMB/AFP/FTP, 2000 z rozbudową pamięci RAM |
| Zasilanie | 250W |
| Chłodzenie | 2x FAN 80 mm x 80 mm |
| Dyski | 8 dysków o pojemności 8TB, znajdujących się na liście kompatybilności urządzenia, pochodzących od tego samego producenta co urządzenie. |

|  |  |
| --- | --- |
| **UPS – 1 szt.** | |
| Technologia | online, VFI-SS-111 |
| Moc wyjściowa | 15kVA/15kW; PF=1 |
| Moc bierna pojemnościowa (bez zewnętrznych układów kompensujących, realizowane za pomocą układu prostownika) | 0 var |
| Napięcie wejściowe | 173 ÷ 485 V AC ± 2 % |
| Napięcie wyjściowe (wartość skuteczna) | 3x400 V AC |
| Częstotliwość napięcia wejściowego (oraz tolerancja) | 45 ÷ 55 Hz ± 1 Hz |
| Częstotliwość napięcia wyjściowego praca sieciowa / rezerwowa | Synchroniczne / 50Hz ± 0,1 Hz |
| Współczynnik szczytu CF | 5:1 |
| Parametry styków przekaźników wyjść programowalnych | 1A / 250 V AC / w standardzie NO i NC dla każdego wyjścia |
| Zniekształcenia prądu wejściowego THDi (bez zewnętrznych układów filtrujących, realizowane za pomocą układu prostownika) | < 3% |
| Zniekształcenia napięcia wyjściowego THDu | < 2% dla Pmax (liniowe)  < 5% (nieliniowe wg PN EN 62040-3 |
| Współczynnik tg φ (bez zewnętrznych układów kompensujących, realizowane za pomocą układu prostownika) | < 0,4 |
| Czas podtrzymania dla obciążenia 15kW | Minimum 16 minut (w oparciu o minimum 64szt akumulatorów 12V10Ah zamontowanych wewnątrz UPS) |
| Przeciążalność | 130% - 10min / 160% - 1min / 300% 100ms |
| EPO | Wymagane – standard NC |
| Bypass zewnętrzny | Wymagany (odpowiedni do oferowanego zasilacza, w obudowie naściennej) |
| Sygnalizacja | akustyczno-diodowa, wyświetlacz LCD, menu w języku polskim i angielskim (do wyboru przez użytkownika) |
| Język oprogramowania i menu | polski i angielski do wyboru z poziomu interfejsu użytkownika |
| Wymagane certyfikaty | ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisu; (załączyć certyfikat) |
| Komunikacja z urządzeniem | RS232, USB, MODBUS RTU, bezpotencjałowe wyjścia programowalne (min. 4), wejścia sterujące (min 4), SNMP - dopuszczalna jako opcjonalna karta |
| Wymiary UPS (wys x szer x gł) | Nie więcej niż 899 x 440 x 861 mm |
| Podłączenie zasilania | Umiejscowione z tyłu UPS’a, w dolnej części obudowy |
| Oprogramowanie do monitorowania pracy zasilacza UPS | Tego samego producenta co UPS, bezpłatne bez ograniczeń funkcjonalności oraz ilości podłączonych stanowisk komputerowych; możliwość pobierania ze strony producenta i dokonywania aktualizacji przez użytkownika bez dodatkowych kosztów |
| Serwis producenta | wymagany, zlokalizowany na terenie Polski, autoryzacja serwisowa lub oświadczenie producenta - załączyć do oferty |
| Gwarancja | Gwarancja na elektronikę 24 mce  Gwarancja na akumulatory 12 mcy; serwis onsite, czas naprawy do 7 dni roboczych |
| Inne wymagania gwarancyjne | w przypadku niemożności naprawy urządzenia w trakcie trwania gwarancji na miejscu u klienta podstawiony zostanie bezpłatnie UPS o minimum tych samych, a na pewno nie gorszych parametrach na czas naprawy (podmiana i dostawa na koszt dostawcy lub autoryzowanego serwisu producenta UPS) – oświadczenie producenta |
| Oświadczenia | Oświadczenie producenta, że sprzęt będzie pochodził z oficjalnego kanału sprzedaży, będzie fabrycznie nowy, wyprodukowany nie później niż na 3 miesiące przed datą dostawy |
| Dokumentacja | Instrukcja w języku polskim |
| Szkolenie | Przeszkolenie pracownika z zakresu obsługi urządzenia w dniu instalacji. Przedstawienie wykazu obowiązków pracownika w zakresie konserwacji oraz monitoringu urządzenia oraz postępowania na wypadek awarii. |

|  |  |
| --- | --- |
| **System do badania podatności – 1 szt.** | |
| Rozwiązanie musi umożliwiać instalację na 150 użytkowników, a licencja musi być ważna do 18 czerwca 2026 roku. | |
| Wymagania ogólne | 1. Rozwiązanie zapewnia monitorowanie ekspozycji na potencjalny atak środowiska informatycznego organizacji.  2. Zarządzanie ekspozycją na atak odbywa się na wielu poziomach: detekcji obiektów znajdujących się w sieci lokalnej, skanowaniu w poszukiwaniu podatności, skanowaniu usług web, monitorowaniu tożsamości na poziomie Entra ID.  3. Wszystkie mechanizmy związane z zarządzaniem ekspozycją na atak zarządzane i konfigurowane są z jednej konsoli zarządzającej.  4. Dostęp do konsoli centralnego zarządzania odbywa się z poziomu interfejsu WWW, niezależnie od zastosowanej platformy sprzętowej i programowej.  5. Konsola zarządzania jest dostępna w postaci usługi hostowanej na serwerach producenta  6. Konsola zarządzania oferuje dostęp za pomocą następujących wspieranych przeglądarek internetowych:   * + Microsoft Edge   + Mozilla Firefox   + Google Chrome   + Safari   7. Konsola zarządzająca dostępna jest w języku polskim.  8. Poza językiem polskim konsola wspiera języki: angielski, niemiecki, francuski, hiszpański, fiński, włoski.  9. Logowanie do konsoli umożliwia wykorzystanie mechanizmów wieloskładnikowego uwierzytelniania (2FA) dla kont posiadających dostęp do konsoli zarządzającej.  10. Mechanizm 2FA służący zabezpieczeniu dostępu do konsoli zarządzającej w swoim działaniu wykorzystuje mechanizmy: powiadomień SMS, oraz tokenów jednorazowych generowanych w aplikacjach mobilnych (np. Google Authenticator, Microsoft Authenticator).  11. Konsola wyposażona jest w panel kontrolny, w którym wyświetlane są informacje podsumowujące dotyczące poziomu bezpieczeństwa chronionej organizacji.  12. Ta sama konsola umożliwia zarządzanie innymi produktami w przypadku posiadania odpowiedniej licencji w tym co najmniej ochrony antymalware, systemem EDR, ochroną usług Microsoft 365  13. Konsola pozwala na podgląd posiadanych licencji.  14. Rozwiązanie na podstawie uzyskanych wyników pochodzących z monitorowanego środowiska wskazuje administratorowi krytyczne detekcje, które powinny zostać naprawione w 1 kolejności w celu przerwania potencjalnej ścieżki ataku.  15. Poza najbardziej krytycznymi rekomendacjami, rozwiązanie pozwala administratorowi na przegląd wszystkich nieprawidłowości wykrytych przez wykorzystywane mechanizmy skanujące.  16. Rozwiązanie w swoim działaniu wykorzystuje mechanizmy umożliwiające graficzne tworzenie ścieżek potencjalnego ataku.  17. Rozwiązanie posiada wbudowany panel kontrolny, za pomocą którego administrator ma podgląd na aktualny poziom bezpieczeństwa organizacji.  18. Dedykowany panel kontrolny dla mechanizmu zarządzania ekspozycją na atak, zawiera dynamiczne diagramy wskazujące na którym poziomie monitorowania bezpieczeństwa organizacji jest najniższy (poziom sieciowy, urządzeń, tożsamości, usług chmurowych).  19. Rekomendacje wymagające najpilniejszych działań zawierają informacje o: typie rekomendacji, lokalizacji działań naprawczych (na poziomie: usług chmurowych, urządzeń, tożsamości, sieci), wielkość nakładu pracy wymaganego do naprawienia wykrytej nieprawidłowości.  20. Panel kontrolny wskazuje administratorowi obiekty stanowiące największe zagrożenie dla poziomu bezpieczeństwa organizacji. |
| Mechanizm skanowania w poszukiwaniu podatności | 1. Rozwiązanie realizuje skanowania podatności za pomocą dedykowanego oprogramowania, instalowanego w środowisku organizacji, zarządzanego z poziomu konsoli centralnego zarządzania.  2. Oprogramowanie skanujące podatności bez agentowo (lokalny scan node) dostępne jest w postaci aplikacji instalowanej lokalnie i wspiera poniższe systemy operacyjne:   * + Windows Server 2016 i nowsze   + Ubuntu server (wersje 64 bitowe 16.x 18.x, 20.x)   + Debian (wersje 64 bitowe 9,10,11)   3. Rozwiązanie umożliwia również agentowe skanowanie w poszukiwaniu podatności na komputerach z systemem Windows.  4. Agent instalowany na systemach Windows wspiera systemy MS Windows 10 i 11 oraz systemy serwerowe MS Windows Server 2016 i nowsze.  5. Ten sam agent zainstalowany na wspieranych systemach Windows w przypadku posiadania odpowiedniej licencji może dodatkowo zapewniać również ochronę antymalware i funkcjonalność systemu EDR.  6. Skanowanie agentowe odbywać się może w cyklach co:4,6,12,24 godzin.  7. Istnieje możliwość włączenia i wyłączenia funkcji skanowania agentowego.  8. Wyłączenie funkcji skanowania agentowego nie powoduje deinstalacji agenta na danym hoście.  9. Rozwiązanie umożliwia przeprowadzenie skanowania, wykrywającego urządzenia pracujące w skanowanej sieci komputerowej.  10. Skanowanie wykrywające urządzenia pracujące w skanowanej sieci umożliwia:   1. wykrywanie urządzeń pracujących w skanowanej sieci na podstawie protokołów: ARP, ICMP PING, SSH, HTTP, HTTPS, RDP. 2. wykrycie pracujących urządzeń w oparciu o analizę wszystkich dostępnych otwartych portów sieciowych. 3. Pozwala na konfigurację parametrów skanowania takich jak:  * zakres przeszukiwanych portów (osobne wartości dla TCP i UDP), * wydajność skanowania (6 poziomów), * liczbę jednoczesnych wątków skanowania (1,2,4,8,16,24,32), * możliwość wykrycia wersji systemu operacyjnego.  1. konfigurację harmonogramu uruchamiania skanu (np. dziennie, tygodniowo, w określony dzień miesiąca, kwartalnie oraz wskazanie godziny rozpoczęcia skanowania). 2. określenia maksymalnej ilości wykonanych skanowań (1-100) lub bez ograniczenia. 3. konfigurację wysyłania powiadomień na wskazane adresy e-mail. 4. powiadomienia dotyczyć mogą: informacji o rozpoczęciu skanowania, jego zakończeniu, zmiany ilości hostów w stosunku do poprzedniego skanowania, zmiany ilości portów w stosunku do poprzedniego skanowania.   11. Konsola zarządzająca umożliwia podgląd listy skonfigurowanych skanów wykrywających dostępne hosty w sieci, wraz z informacją o zmianach w stosunku do ostatniego przeprowadzonego skanu.  12. Widok listy dostępnych skanowań wykrywających obiekty pozwala na zaawansowane filtrowanie.  13. Konsola pozwala na uruchomienie z poziomu listy dostępnych skanowań, wskazanego skanowania wykrywającego obiekty na żądanie z pominięciem harmonogramu.  14. Trwające zadanie skanowania w poszukiwaniu obiektów może zostać przerwane na żądanie.  15. Konsola zarządzania umożliwia eksport wyniku skanu wykrywającego dostępne urządzenia w sieci do pliku XLSX oraz XML.  16. Rozwiązanie umożliwia uruchomienie skanowania wykrywającego znane podatności bezpieczeństwa na urządzeniach sieciowych.  17. Skan wykrywający znane podatności bezpieczeństwa na urządzeniach sieciowych umożliwia:   1. określenie skanowanego celu za pomocą adresu IP, oraz grupy celów za pomocą adresu podsieci IP. 2. masowe wprowadzenie listy skanowanych celów (adresów IP), za pomocą ustrukturyzowanego pliku z rozszerzeniem CSV. 3. konfigurację parametrów skanowania, takich jak:  * zakres skanowanych portów sieciowych TCP/UDP, * parametr wydajności skanowania (6 poziomów) * rodzaj uwierzytelniania na skanowanej stacji.  1. konfigurację harmonogramu uruchamiania skanu: dziennie, tygodniowo, w określony dzień miesiąca, oraz wskazanie godziny rozpoczęcia. 2. konfigurację wysyłania powiadomień na wskazane adresy e-mail informujących o momencie rozpoczęcia skanowania oraz jego zakończeniu.   18. W przypadku tworzonego zadania skanowania administrator posiada możliwość określenia czy do celu skanowania mają zostać wykorzystane wszystkie dostępne pluginy skanujące, tylko wybrane, wszystkie pluginy poza wskazanymi.  19. Administrator posiada możliwość podglądu dostępnych pluginów skanujących podatności i przeszukiwania ich listy.  20. Konsola zarządzania umożliwia podgląd listy skonfigurowanych skanów wykrywających znane podatności bezpieczeństwa.  21. Konsola pozwala na uruchomienie i zatrzymanie skanowania w poszukiwaniu znanych podatności na żądanie.  22. Konsola zarządzania umożliwia eksport wyniku skanu wykrywającego znane podatności bezpieczeństwa do pliku docx i xml.  23. Dla danego hosta widoczne są wyniki skanowania w poszukiwaniu podatności.  24. Wyniki zawierają listę wykrytych podatności wraz z poziomem ich krytyczności.  25. Dla danej wykrytej podatności dostępny jest: jej opis, poziom krytyczności w oparciu o punktację CVSS, datę wykrycia, wersję pluginu który wykrył podatność, sugestię rozwiązania (jeśli jest dostępna), informację o publicznie dostępnym exploicie (jeśli jest dostępna), zewnętrzne referencje (jeśli są dostępne).  26. Rozwiązanie umożliwia uruchomienie skanu wykrywającego luki bezpieczeństwa w aplikacjach webowych.  27. Skanowanie wykrywające luki bezpieczeństwa w aplikacjach webowych umożliwia:   1. określenie skanowanego celu za pomocą adresu URL. 2. konfigurację parametrów skanowania takich jak:  * rodzaje testowanych ataków, * wyjątki ze skanowania (adresy URL omijane podczas testowania aplikacji web), * parametr wydajności skanowania (ilość jednoczesnych zapytań przesyłanych do skanowanej aplikacji).  1. konfigurację uwierzytelniania w testowanej aplikacji web. 2. konfigurację harmonogramu uruchamiania skanowania: dziennie, tygodniowo, w określony dzień miesiąca oraz wskazanie godziny rozpoczęcia skanowania. 3. konfigurację wysyłania powiadomień na wskazany adres e-mail informujących o momencie rozpoczęcia skanowania oraz jego zakończeniu.   28. Konsola zarządzania umożliwia podgląd listy skonfigurowanych skanów wykrywających luki w aplikacjach webowych.  29. Rozwiązanie umożliwia skorzystanie z narzędzia do identyfikacji zasobów informatycznych dostępnych z publicznej sieci Internet.  30. Narzędzie do identyfikacji zasobów informatycznych dostępnych z publicznej sieci Internet umożliwia:   1. przeszukiwanie adresów internetowych, skatalogowanych przez automatyczne systemy producenta, spełniających wskazane warunki wyszukiwania. 2. zapisywanie wskazanych warunków wyszukiwania jako szablony. 3. podgląd listy wyników wyszukiwania z informacją o wykrytym adresie IP, nazwie oraz słowach kluczowych. 4. dodanie wybranych wyników wyszukiwania do grupy skanowania podatności bezpieczeństwa.   31. Rozwiązanie umożliwia podgląd listy wszystkich wykrytych podatności bezpieczeństwa z wszystkich przeprowadzonych skanowań.  32. Lista wszystkich wykrytych podatności musi umożliwiać:   1. filtrowanie podatności ze względu na ich rodzaj, przypisany znacznik (tag), urządzenie sieciowe na którym została znaleziona podatność, stopień zagrożenia, 2. wyświetlenie szczegółów poszczególnych podatności bezpieczeństwa wraz z informacjami na jakich urządzeniach sieciowych dana podatność została wykryta, 3. eksport listy urządzeń na których została wykryta dana podatność bezpieczeństwa do pliku CSV.   33. Rozwiązanie umożliwia utworzenie nowego raportu podsumowującego wykryte podatności.  34. Rozwiązanie umożliwia podgląd listy wygenerowanych raportów.  35. Raport podsumowujący umożliwia:   1. konfigurację szablonu jaki będzie wykorzystany do przygotowania raportu, 2. wybranie grup urządzeń, które będą znajdowały się w raporcie, 3. wybranie poszczególnych statusów oraz poziomu zagrożenia podatności, które będą znajdowały się w raporcie, 4. Utworzenie harmonogramu generowania raportu 5. Wskazanie adresu email na który zostanie wysłany link udostępniający wygenerowany raport, wraz z określeniem czasu ważności linku.   36. Lista wygenerowanych raportów musi umożliwiać:   1. Wygenerowanie raportu na żądanie, 2. eksport wyniku raportu do pliku XML(pogrupowany hostami), DOCX(pogrupowany hostami lub wykrytymi podatnościami lub podsumowujący), XLSX (pogrupowany wykrytymi podatnościami).   37. Administrator ma możliwość określenia: strefy czasowej dla swojej organizacji, długości przetrzymywania raportów (miesiąc, kwartał, pół roku, rok, 2 lata),  38. Dostęp do konsoli może być ograniczony na podstawie adresów IP lub ich zakresu. |
| Monitorowanie tożsamości na poziomie EntraID | 1. Rozwiązanie pozwala na monitorowanie tożsamości znajdujących się w ramach usługi Entra ID.  2. Aktywacja synchronizacji pomiędzy systemem monitorującym a usługą Entra ID obywa się przy wykorzystaniu dedykowanego kreatora wbudowanego w system.  3. Administrator w ramach konsoli ma dostęp do dedykowanej zakładki zawierającej listę tożsamości objętych monitorowaniem przez system.  4. Lista tożsamości zawiera następujące informacje: Konto, Nazwę użytkownika, status ryzyka, Typ, poziom ważności, kontekst biznesowy, informacje dotyczące wykrycia konta w wyciekach danych, status konfiguracji MFA, informację dotyczącą daty ostatniej zmiany hasła.  5. Po wybraniu danego konta, administrator posiada możliwość zmiany poziomu ważności konta, wartości dostępne to: niska, normalna, wysoka ważność.  6. Zmiana poziomu ważności konta ma wpływ na mechanizm tworzący detekcje.  7. Administrator ma możliwość ręcznego wprowadzenia komentarza dotyczące kontekstu biznesowego dla danego konta.  8. Wybierając szczegóły dla danego konta, administrator otrzymuje informacje dotyczące podsumowania konta oraz informacji związanych z ewentualnym ryzykiem dla konta.  9. Informacje związane z zarządzaniem ryzykiem dla konta zawierają: Status ryzyka, informacje czy konto pojawiło się w wycieku danych, opis dotyczący informacji związanych z wyciekiem danych, datę wycieku w którym konto się pojawiło, datę detekcji.  10. Administrator ma wgląd we wszystkie wykryte nieprawidłowości związane z monitorowanymi kontami,  11. Rozwiązanie na podstawie wykrytych nieprawidłowości na poziomie monitorowanych kont, wskazuje administratorowi sugerowane rozwiązanie danego problemu. |
| Wymagania dodatkowe | Wraz z dostawą zamawiający wymaga wdrożenie zaoferowanego rozwiązania. Wdrożenie musi być przeprowadzone przez certyfikowanego inżyniera. W celu potwierdzenie kompetencji wykonawca wraz z ofertą przedłoży oświadczenie producenta potwierdzające, że wykonawca posiada odpowiednie zasoby do  świadczenia usług wsparcia technicznego, a także posiada status partnerski co najmniej Silver na terenie Polski - oświadczenie należy dołączyć do oferty. |
| Zakres wdrożenia | Instalacja i konfiguracja   * Instalacja oprogramowania, * Podstawowa konfiguracja i wprowadzenie do interfejsu użytkownika.   Skany podatności   * Konfiguracja i uruchomienie skanów podatności, * Analiza wyników skanowania.   Zaawansowane funkcje skanowania   * Harmonogramy skanów i powtarzające się skany, * Wykorzystanie skanów uwierzytelnionych.   Ocena i priorytetyzacja podatności   * Analiza wyników skanowania, * Ustalanie priorytetów naprawy podatności.   Raportowanie i powiadomienia   * Generowanie raportów o podatnościach, * Konfiguracja powiadomień o nowych podatnościach. |

|  |  |
| --- | --- |
| **Oprogramowanie DLP – 1 szt.** | |
| Rozwiązanie musi posiadać 150 licencji bezterminowych oraz wsparcie do dnia 18 czerwca 2026 r. | |
| Wymagania ogólne | 1. Pomoc i dokumentacja programu dostępne w języku angielskim.  2. Konsola administracyjna i komunikaty klienta muszą być w języku polskim.  3. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.  4. Serwer administracyjny musi umożliwiać instalację/dezinstalację zdalnego klienta na stacjach roboczych.  5. Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym.  6. Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia.  7. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli.  8. System musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych, usuwając najstarsze informacje, gdy rozmiar bazy osiągnie skonfigurowany limit.  9. Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania.  10. Administrator musi mieć możliwość aby tworzyć, usuwać i konta administratorów w konsoli programu.  11. Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu).  12. Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory.  13. Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą a serwerem w czasie rzeczywistym.  14. Serwer administracyjny musi umożliwiać ustawienie powiadomień dla użytkownika końcowego w przypadku złamania reguł związanych z ochroną DLP, z możliwością dostosowania grafiki, adresu e-mail i odnośnika do polityki bezpieczeństwa.  15. Administrator musi mieć możliwość wykonać audyt stacji roboczych/użytkowników w oparciu o różne czynności, takie jak uruchomione aplikacje, podłączone urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, wysyłane i odebrane wiadomości email oraz czynności na plikach.  16. Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji i typów plików.  17. Administrator musi mieć możliwość filtrowania i sortowania zebranych danych.  18. Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości email.  19. Dashboardy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu.  20. Serwer administracyjny musi posiadać wbudowany serwer SMTP dostarczony przez producenta oprogramowania.  21. Serwer administracyjny musi umożliwiać wykonywanie zadań kategoryzacji plików, zarówno istniejących na stacjach roboczych i zasobach sieciowych, jak i nowo powstałych na bazie już skategoryzowanych plików.  22. Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku.  23. Dla plików skategoryzowanych, wymagana jest możliwość tworzenia reguł dotyczących blokowania i zezwalania na różne operacje, takie jak zapisywanie, przenoszenie, drukowanie, wysyłanie pocztą, wysyłanie do chmury, przesyłanie komunikatorami itp.  24. Serwer administracyjny musi umożliwiać wyszukiwanie i ochronę plików w oparciu o różne kryteria, takie jak numery kart kredytowych, numer PESEL, numer dowodu osobistego, numer paszportu, wyrażenia regularne, określone ciągi znaków i numer IBAN.  25. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.  26. Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM.  27. Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP.  28. Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania.  29. System musi ochraniać pocztę e-mail Microsoft 365, sprawdzając każdą wiadomość e-mail wysyłaną przez użytkowników Microsoft 365.  30. System musi ochraniać pliki w Microsoft 365, kontrolując aktywność plików w Microsoft SharePoint, Microsoft OneDrive dla Firm i Microsoft Teams.  31. System musi wykorzystywać mechanizm OCR (optical character recognition), aby wykrywać poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach  32. System musi posiadać możliwość integracji z systemami do analizy danych (PowerBI, Tableau, etc.)  33. System musi zapewniać możliwość zarządzania szyfrowaniem dysków twardych oraz urządzeń wymiennych. |
| System operacyjny | * Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi * Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi * MacOS 12 lub nowszy. |
| Serwer administracyjny musi obsługiwać instalację na systemach | Windows Server 2016 (64-bit) i nowszych |
| Serwer administracyjny musi obsługiwać bazy danych | * MS SQL Server 2016 lub nowsze, * MS SQL Express, * AzureSQL S3 lub nowsze. |

|  |  |
| --- | --- |
| **Oprogramowanie do zarządzania infrastrukturą IT – 1 szt.** | |
| Rozwiązanie musi posiadać 150 licencji na stacje robocze oraz wsparcie do dnia 18 czerwca 2026 r. | |
| Wymagania ogólne | Oprogramowanie musi posiadać budowę modułową, składać się z serwera zarządzającego, zdalnych konsoli oraz agentów. Komunikacja pomiędzy Serwerem a Agentami i Konsolami powinna być nawiązywana przy użyciu szyfrowanego protokołu TLS 1.2. Program musi umożliwiać zmianę portu komunikacyjnego wykorzystywanego przez konsolą zarządzającą.  Moduły musi umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem. Program musi wykorzystywać darmowy silnik bazy danych z kodem źródłowym dostępnym na licencji open-source (PostgreSQL w wersji min.12) dzięki czemu nie jest objęty limitem ilości danych, baza danych jest rozwiązaniem darmowym niewymagającym dodatkowego licencjonowania. Instalacja Serwera oraz Konsol zarządzających wymaga 64-bitowego systemu operacyjnego Windows.  Dane, które dotyczą działań pracownika na komputerze, a więc: historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., muszą być odseparowane od danych stricte technicznych tj. informacji o stacji roboczej. Są one również grupowane w osobnym, dedykowanym oknie. Oprogramowanie musi mieć możliwość, zgodne z obowiązującymi przepisami o ochronie danych osobowych RODO, usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej.  Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, musi być objęty kontrolą na poziomie wybranych Administratorów.  Oprogramowanie musi posiadać możliwość nadawania kontom administracyjnym różnych poziomów dostępu oraz uprawnień zarówno do funkcji Programu, grup urządzeń, jak i użytkowników. Główny Administrator musi mieć możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną, m.in. musi móc wyłączyć możliwość zdalnej deinstalacji Agenta, ograniczyć dostęp do Opcji programu oraz logów działań innych administratorów. Działania administratorów muszą być logowane oznacza to, że program musi posiadać dziennik z listą czynności wykonanych przez administratorów, które zmodyfikowały obiekty znajdujące się w systemie w tym m.in. logowanie dostępu do Opcji programu, logowanie dostępu do informacji o aktywności użytkownika, logowanie poleceń deinstalacji Agenta. Działania administratorów mogą być automatycznie eksportowane do zewnętrznego kolektora Syslog. Oprogramowanie musi mieć możliwość synchronizacji z Active Directory, również przez szyfrowane połączenie LDAPS listy kont użytkowników, w tym administratorów.  Program musi umożliwiać konfigurację polityki haseł do lokalnych kont użytkowników konsoli. Polityki muszą pozawalać na określenie: minimalnej długości hasła, liter, cyfr, znaków specjalnych oraz automatycznie wymuszać dostosowanie bieżących haseł do obowiązujących zasad.  Program musi zawierać mechanizmy uwierzytelniania logowań administratorów do konsoli z wykorzystaniem weryfikacji dwuskładnikowej (MFA). Kod autoryzacyjny może być wysyłany za pomocą e-mail i/lub SMS. W weryfikacji MFA musi być możliwość skonfigurowania okresu, po którym należy ponownie zautoryzować logowanie. W przypadku awarii autoryzacja logowania może być pominięta tylko w lokalnej konsoli serwera. |
| Monitorowanie infrastruktury | Monitorowanie musi odbywać się bezagentowo i obejmować serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:   * wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping, * wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU), * wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci, * wizualizacji urządzeń na mapach z funkcją siatki umożliwiającej korygowanie pozycji ikon na mapie do najbliższej linii siatki, * wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła, * wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku, * wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach o dowolnym rozmiarze i kolorze, * wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie, * wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny, * zablokowania mapy urządzeń przed przypadkową edycją, * serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów * serwerów pocztowych:   + program monitoruje czas logowania do serwisu odbierającego oraz czas wysyłania poczty,   + program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem),   + program ma możliwość wykonywania operacji testowych,   + program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa. * monitorowania serwerów WWW i adresów URL, * cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS, * obsługi szyfrowania SSL/TLS w powiadomieniach e-mail, * obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID, * obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych, * monitoringu routerów i przełączników wg:   + zmian stanu interfejsów sieciowych,   + ruchu sieciowego,   + podłączonych stacji roboczych – graficzna prezentacja panelu switcha,   + ruchu generowanego przez podłączone do portów stacje robocze. * serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/ zatrzymanie/ zrestartowanie, * wyświetlania statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu, * monitorowania stanu maszyn wirtualnych Vmware: działa, nie działa, wstrzymano, * zarządzania stanem maszyn wirtualnych Vmware: wysyłanie poleceń włączenia, wstrzymania i wyłączenia zasilania do każdej maszyny, * wydajności systemów Windows:   + obciążenie CPU,   + pamięci,   + zajętość dysków,   + transfer sieciowy.   Program posiada Inteligentne Mapy i Oddziały, które służą do lepszego zarządzania logiczną strukturą urządzeń w przedsiębiorstwie (Oddziały) oraz tworzą dynamiczne mapy wg własnych filtrów (Mapy Inteligentne). Kryteria automatycznego filtrowania dotyczyć mogą m.in. statusu Agenta, wygenerowanych alarmów, zainstalowanych aplikacji, przynależności do oddziału, serwisów sieciowych, danych z SNMP, danych z inwentaryzacji urządzenia itp. Program posiada również funkcję kompilatora plików MIB, który umożliwia dodawanie definicji dla modułów SNMP.  Program umożliwia również nakładanie na urządzenia liczników wydajności WMI oraz SNMP wg szablonów definiowanie alarmów z wykorzystaniem akcji związanych ze zdarzeniami w systemie, m.in.: wysłanie komunikatu pulpitowego, wysłanie wiadomości e-mail, wysłanie SMS, wysłanie wiadomości SMS poprzez integrację z serwisem smsapi.pl, wysłanie wiadomości przez Microsoft Teams oraz Slack, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi Windows, wyłączenie/restart komputera. Alarmy budowane są przez administratora z wykorzystaniem ciągu przyczynowo skutkowego – oznacza to, że administrator samodzielnie może wskazać dowolne zdarzenie z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie. Wykonywanie akcji alarmów można skonfigurować automatycznie po wykryciu zdarzenia, z opóźnieniem, na końcu zdarzenia oraz cyklicznie np. co 5 minut. Dla akcji można nałożyć ograniczenie czasowe np. nie wykonuj między 8:00-16:00.  Alarmy pozwalają na priorytetyzację urządzeń, grupowanie wg ważności i typu urządzenia.  Oprogramowanie umożliwia wykorzystanie w alarmowaniu skrzynek e-mail z wykorzystaniem autoryzacji OAuth 2.0  Program ma możliwość integracji ze sprzętową bramką GSM w celu wysyłania powiadomień SMS z wykorzystaniem protokołu netGSM (SOAP). |
| Inwentaryzacja | W zakresie inwentaryzacji program musi automatycznie gromadzić informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz:  1. Prezentuje szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.  2. Umożliwia odczyt parametrów S.M.A.R.T. dysków twardych, dysków SSD, w tym NVMe.  3. Obejmuje m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.  4. Informuje o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji.  5. Zbiera informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej:  instalacji/deinstalacji aplikacji, zmian adresu IP itd.  6. Posiada możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera.  7. Umożliwia odczytanie numeru seryjnego (klucze licencyjne).  8. Umożliwia automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.  9. Umożliwia przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.  10. Umożliwia utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu).  11. Umożliwia wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji są logowane.  Moduł inwentaryzacji zasobów umożliwia prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania:   * przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji, * przydzielania dostępu administratorów do zasobów na podstawie praw do oddziałów, * tworzenia powiązań między zasobami a urządzeniami, * tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych, * wskazania osób uprawnionych do użycia zasobów, * definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości, * dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz, * określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów, * określenia atrybutów dodatkowych tylko dla wybranych typów zasobów, * masową edycję atrybutów zasobów, * definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie, * importu danych z zewnętrznego źródła (.CSV), * przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp., * tworzenia powiązań między zasobami a dokumentami w relacji 1:N, * oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp., * ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności, * generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania, * przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji, * konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca, * konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca, * archiwizacji i porównywania audytów zasobów, * tworzenia kodów kreskowych dla zasobów, * drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy, * inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet, * możliwość zmiany portu komunikacyjnego wykorzystywanego przez aplikację mobilną dla systemu Android, * inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline), * definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja”).   Inwentaryzacja oprogramowania zapewnia funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:  1. Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP.  2. Informacje o aplikacjach używanych w organizacji.  3. Tworzenie własnych wzorców aplikacji.  4. Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.  5. Informacje o komputerach, na których aplikacja została wykryta.  6. Zarządzanie posiadanymi licencjami.  7. Wskazywanie osób odpowiedzialnych za licencję.  8. Wskazanie użytkowników licencji.  9. Tworzenia powiązań między licencjami a dokumentami w relacji 1:N.  10. Rozbudowane i konfigurowalne scenariusze zarządzania licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu.  11. Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych.  12. Zarządzanie posiadanymi licencjami: raport zgodności licencji.  13. Możliwość przypisania do programów numerów seryjnych, wartości itp.  Okna audytowe posiadają możliwość filtrowania elementów per oddział. |
| Obsługa użytkownika | W zakresie obsługi użytkowników program musi  umożliwiać monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie:   * Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy), * Procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach, * Rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność, * Informacji o edytowanych przez użytkownika dokumentach, * Historii pracy (cykliczne zrzuty ekranowe), * Listy odwiedzanych stron WWW (tytuły, adresy, liczba i czas wizyt), * Transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika), * Wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program ma możliwość monitorowania kosztów wydruków, * Nagłówków przesyłanej w aplikacjach klienckich poczty e-mail.   Program ponadto posiada możliwość:   * wykrywania podejrzanej aktywności przez popularne „jigglery”, mającej na celu symulowanie faktycznej pracy, * zdefiniowania czasu (min. 15 minut) gdy wykrywana będzie symulowana aktywność wyłącznie przez ruch myszą bez kliknięcia lub wprowadzanie tego samego znaku z klawiatury, * wyszczególnienia podejrzanej aktywności w raportach. * wygenerowania alarmu i wykonania akcji po wykryciu podejrzanej aktywności, * automatycznego włączenia zapisywania zrzutów ekranowych po wykryciu podejrzanej aktywności, * blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. \*.domena.pl). Reguły w postaci listy domen tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane lub współdzielone pomiędzy grupami lub kontami, * integracji list stron w formie plików .TXT z dowolnego adresu zewnętrznego np. CERT, * skorzystania z wbudowanej listy stron sklasyfikowanych jako zagrożenia, * automatycznego odświeżania list stron zintegrowanych z adresów zewnętrznych, * blokowania ruchu na wskazanych portach TCP/IP, * blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem, * prowadzenia rejestru naruszeń blokad, * wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia, naruszy skonfigurowane blokady, * przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika), * definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone.   Możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie.  Mechanizm blokowania uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku. Reguły w postaci listy blokowanych plików lub lokalizacji tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami.  Program posiada grupy użytkowników oraz grupy Inteligentne, które służą do lepszego zarządzania użytkownikami, polityką monitorowania oraz blokowania aplikacji i stron internetowych. |
| Pomoc użytkownikom | Program umożliwia realizację zdalnej pomocy użytkownikom. W ramach kontroli stacji użytkownika dostępny musi być podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połącznie i opcją odrzucenia takiego połącznia przez użytkownika (np. w przypadku pracowników wysokiego szczebla). Podczas dostępu zdalnego, zarówno użytkownik jak i administrator widzą ten sam ekran. Administrator w trakcie zdalnego dostępu ma możliwość wyboru dowolnego ekranu (monitora) oraz zablokowania działania myszy oraz klawiatury dla użytkownika. Funkcja zdalnego dostępu umożliwia równoczesne podłączenie do tego samego komputera kilku administratorom.  W niniejszym module znajduje się baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych poprzez dedykowany portal oraz przetwarzanie wiadomości e-mail, które są przetwarzane i przyporządkowywane odpowiednim  administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie. Oprogramowanie pozwala na integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0. Moduł umożliwia również przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o sygnalistach”) oraz zawiera dokumenty prawne dot. ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę. Kolejną ważną funkcjonalnością jest umożliwienie użytkownikom monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron. System umożliwia użycie pośredniego statusu „zgłoszenie rozwiązane” przed ostatecznym zamknięciem zgłoszenia.  Moduł ten musi zawierać również komunikator (czat), który umożliwia prowadzenie rozmów w czasie rzeczywistym oraz archiwizację historii wiadomości pomiędzy zalogowanymi użytkownikami, pracownikami pomocy technicznej i administratorami (wraz z wyszukiwarką rozmów i wiadomości wg słów kluczowych oraz automatycznym oczyszczaniem historii rozmów). Ponadto czat pozwala na:   * zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej, * rozmowy również między „zwykłymi” użytkownikami, * przesyłanie plików między rozmówcami w trybie online, * tworzenie pokojów tematycznych, rozmów grupowych, * oznaczanie kontaktów jako „ulubionych” na liście kontaktów, * uruchomienie z poziomu ikony dostępowej Agenta oraz bezpośrednio w interfejsie WWW heldpesku, * może być wyświetlany w trybie jasnym lub ciemnym.   W module zawarta jest również baza wiedzy pomagająca użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy wraz z możliwością nadawania artykułom 1 z 3 statusów (opublikowany, wewnętrzny, szkic). Program umożliwia informowanie pracowników o zdarzeniach, np. planowanych przestojach w dostępie do usług, przez komunikaty z graficznym formatowaniem treści oraz łączami do artykułów w bazie wiedzy. Użytkownik ma możliwość przeglądnięcia historii odczytanych komunikatów bezpośrednio z poziomu ikony Agenta. Administrator ma możliwość tworzenia szkiców i archiwizowania komunikatów.  Dostęp do systemu zgłoszeń oraz bazy wiedzy realizowany jest przez dedykowany portal dostępny przez przeglądarkę internetową, który może być wyświetlany w trybie jasnym lub ciemnym.  Funkcjonalność modułu umożliwia również uzyskanie dostępu z prywatnego komputera tylko do swojego komputera firmowego, który pozostał w organizacji, za pomocą funkcji zdalnego dostępu przez każdego pracownika.  Moduł pomocy zdalnej umożliwia również:   * pobieranie listy użytkowników z Active Directory, * wyświetlanie w systemie zgłoszeń wizytówki użytkownika wraz z jego numerem telefonu, adresem e-mail oraz informacją o przełożonym, * zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont, * zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez rozbudowany system zarządzania regułami widoczności zgłoszeń, * zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii zgłoszeń, * zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii artykułów bazy wiedzy, * tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO, * automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników, * definiowanie ścieżek akceptacji zgłoszeń – procesu, w którym użytkownik uzyskuje akceptację na realizację zgłoszenia od wyznaczonych osób w organizacji, * przypisywanie ścieżek akceptacji zgłoszeń do określonych kategorii, * procesowanie zgłoszeń użytkowników z wiadomości e-mail, * eksportowanie listy zgłoszeń do plików CSV i XLSX, * integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0, * tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń, * wykonywanie operacji na wielu zgłoszeniach równocześnie, * dołączanie załączników do zgłoszeń, * rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy, * szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników, * wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia, * zrzuty ekranowe (podgląd pulpitu), * zdalną modyfikację rejestrów, * dystrybucję oprogramowania przez Agenty, * definiowanie aplikacji dozwolonych do samodzielnej instalacji przez użytkowników z pakietów MSI w postaci Kiosku z Aplikacjami, * przypisywanie dostępnych w Kiosku instalatorów do grup użytkowników, * dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI), * zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku, * możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych osób w zgłoszeniu, * możliwość skonfigurowania automatyzacji dodających komentarze publiczne wraz z załącznikami i odnośnikami do artykułów w Bazie Wiedzy, * planowanie nieobecności pracowników helpdesk, * obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem, * generowanie raportów obsługi helpdesk, * zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu), * zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami), * wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików bez blokowania interfejsu programu podczas przesyłania plików. |
| Ochrona danych | Rozwiązanie musi posiadać możliwość ochrony danych przed wyciekiem poprzez blokowanie urządzeń.  1. Blokowanie urządzeń i nośników danych.  Program ma możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny.  2. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek.  3. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.  4. Blokownie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane.  5. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych.  6. Funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender.  7. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker.  8. Funkcje wspierające bezpieczeństwo systemu: zdalne szyfrowanie dysków za pomocą BitLocker.  9. Funkcje wspierające bezpieczeństwo systemu: zapisywanie klucza odzyskiwania do pliku oraz jako zasób w bazie danych programu.  10. Funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu.  11. Funkcje wspierające bezpieczeństwo systemu: odczytanie informacji o aktywnym oprogramowaniu antywirusowym firm trzecich, innym niż Windows Defender.  12. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM.  Zarządzanie prawami dostępu do urządzeń:  1. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.  2. Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive’ów, dysków itp.  - urządzenia prywatne są blokowane.  3. Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników.  4. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci.  5. Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane.  Audyt operacji na plikach na urządzeniach przenośnych: zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych; podłączenie/odłączenie urządzenia przenośnego.  Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika.  Definiowanie reguł monitorowanych folderów w postaci list.  Monitorowanie operacji na plikach na udostępnionych zasobach sieciowych (udziałach) na urządzeniach nieobsługiwanych przez Agenta (np. macierze, NAS itp.)  Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. Przydzielanie uprawnień również do kont użytkowników lokalnych.  Program umożliwia prowadzenie rejestru naruszeń blokad podłączanych nośników. |
| Zarzadzanie czasem | Program musi wspierać zarzadzanie czasem i analizowanie aktywności użytkowników poprzez dostarczenie informacji o czasie poświęconym na pracę w poszczególnych aplikacjach i na stronach WWW z dowolnie wybranego okresu. Każdy pracownik organizacji może oznaczyć sesję aktywności jako czas prywatny gdy wykonuje czynności prywatne na sprzęcie firmowym. Może również uzyskać dostęp do własnych wskaźników aktywności w czasie pracy. Menedżerowie oraz przełożeni mogą uzyskać  automatyczny dostęp do aktywności podwładnych w zespołach i indywidualnie oraz mogą przeanalizować aktywności w danym okresie i zyskać pełny obraz obszarów wymagających największego zaangażowania. Pracownik może przeglądać swoje historyczne dane, wybierając okres aktywności, który go interesuje. Zastosowane reguły pozwalają zidentyfikować różnego rodzaju rozpraszacze i nieefektywne działania. Dostęp realizowany jest przez przeglądarkę internetową a strona  może być wyświetlana w trybie jasnym lub ciemnym.  1. Statystyki czasu pracy i osobistej aktywności w wybranym przedziale czasu.  2. Statystyki aktywności grupy i jej członków widoczne dla menedżera grupy.  3. Statystyki aktywności podwładnych widoczne dla przełożonego.  4. Lista odwiedzanych stron internetowych i aplikacji wraz ze spędzonym na nich czasem.  5. Podgląd listy użytkowników korzystających z wybranej aplikacji we wskazanym zakresie czasu.  6. Statystyki popularności stron i aplikacji w organizacji, grupie i u poszczególnych użytkowników.  7. Ocena produktywności użytkownika na podstawie czasu spędzonego w aplikacjach i na stronach internetowych.  8. Grupowanie stron internetowych i aplikacji z podziałem na: produktywne, neutralne i nieproduktywne.  9. Możliwość przypisywania wyjątków produktywności dla określonych grup użytkowników w przypadku aplikacji globalnie sklasyfikowanych jako nieproduktywne co pozwala na sklasyfikowanie aktywności użytkowników będących członkami takiej grupy jako produktywnej  przy ocenie ich pracy.  10. Jednoczesna edycja klasyfikacji aplikacji pod kątem oceny produktywności oraz przeznaczenia (kategoryzowanie).  11. Wskaźnik czasu poświęconego na aktywność produktywną.  12. Definiowanie wymaganego progu produktywności i limitu nieproduktywności, możliwość włączenia dla nich alarmów e-mail.  13. Przypisywanie kategorii aplikacjom i stronom internetowym, np. Biuro, Produkcja, Rozrywka -  predefiniowana lista kategorii z możliwością edycji.  14. Lista kontaktów w organizacji z wbudowaną wyszukiwarką dostępna dla każdego pracownika  w organizacji z możliwością ukrycia wybranych kontaktów. |
| Ochrona przed usunięciem | Program musi być zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora stacji roboczej, na której pracuje. |
| Funkcjonalność Agenta | Możliwość automatycznego wyszukiwania serwera przez programowanie monitorujące stacje robocze. |
| Wdrożenie | Instalacja i konfiguracja systemu   * Instalacja oprogramowania zarządzającego na centralnym serwerze, * Wdrożenie agentów monitorujących na wszystkich stacjach roboczych i serwerach, * Integracja z usługami katalogowymi (np. Active Directory) w celu automatycznej synchronizacji użytkowników i urządzeń, * Konfiguracja monitorowania sieci – mapowanie urządzeń, analiza ruchu sieciowego, wykrywanie nieautoryzowanych połączeń, * Ustawienie polityk dostępu do danych – ograniczenie możliwości podłączania zewnętrznych nośników USB i drukarek, * Konfiguracja alertów i raportów – definiowanie powiadomień o krytycznych zdarzeniach, takich jak awarie sprzętu, nietypowa aktywność użytkowników czy naruszenia polityki bezpieczeństwa.   Wdrożenie musi być prowadzone przez certyfikowanego inżyniera oferowanego rozwiązania. Certyfikat potwierdzający należy dostarczyć wraz z ofertą. |