|  |  |
| --- | --- |
| **OPIS PRZEDMIOTU ZAMÓWIENIA**  Przedmiotem zamówienia jest dostawa urządzeń oraz oprogramowania.  **Przedmiot zamówienia obejmuje niżej wymieniony asortyment** | |
| **Cecha/Funkcjonalność** | **Minimalne parametry wymagane przez Zamawiającego** |
| **Network Attached Storage - NAS– 4 szt.** | |
| **Obudowa** | RACK 1U |
| **Procesor** | Dwurdzeniowy procesor o taktowaniu 2,6 GHz (3.1 GHz w trybie turbo) |
| **Sprzętowy mechanizm szyfrowania** | Tak (AES-NI) |
| **Pamięć RAM** | min. 2 GB pamięci ECC |
| **Możliwości rozbudowy** | Sprzęt powinien być wyposażony w min. 4 kieszenie na dyski twarde typu hot-SWAP, zainstalowane 4 dyski o pojemności 16TB każdy. Oferowany dysk musi być tego samego producenta co producent serwera |
| **Porty zewnętrzne** | Min. 1 port USB 3.2.1 |
| **Porty sieciowe** | Min. 2 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego) |
| **Funkcja Wake on LAN/WAN** | Tak |
| **Wentylator obudowy** | Min. 3 wentylatory (40 × 40 × 20 mm) |
| **Obsługiwane protokoły sieciowe** | Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV |
| **Obsługiwane systemy plików** | * Wewnętrzny: Btrfs, ext4 * Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT |
| **Zarządzanie pamięcią masową** | * Maksymalny rozmiar pojedynczego wolumenu: 108 TB * Minimalny liczba wewnętrznych wolumenów: 64 * Minimalny liczba obiektów iSCSI Target: 128 * Minimalny liczba jednostek iSCSI LUN: 256 * Obsługa klonowania/migawek jednostek iSCSI LUN |
| **Obsługiwane typy macierzy RAID** | Min. SHR, Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 |
| **Funkcja udostępniania plików** | * Minimalna liczba kont użytkowników: 2 048 * Minimalna liczba grup użytkowników: 256 * Minimalna liczba folderów współdzielonych: 512 * Minimalna liczba jednoczesnych połączeń CIFS/AFP/NFS/FTP: 500 |
| **Uprawnienia** | Uprawnienia listy kontroli dostępu systemu Windows (ACL) i aplikacji |
| **Wirtualizacja** | Obsługa VMware vSphere with VAAI, Microsoft Hyper-V, Citrix, OpenStack |
| **Usługa katalogowa** | Integracja z usługami Windows AD, logowanie użytkowników domeny przez protokoły SMB/NFS/AFP/FTP lub aplikację File Station, integracja z LDAP |
| **Bezpieczeństwo** | Zapora, szyfrowanie folderu współdzielonego, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne  blokowanie logowania, obsługa Let's Encrypt i HTTPS (dostosowywane mechanizmy szyfrowania) |
| **Obsługiwane przeglądarki** | Google Chrome, Firefox, Microsoft Edge, Safari 13 i nowsze oraz Safari (iOS 13.0 i nowsze) na urządzeniach iPad, Chrome (Android 11.0 i nowsze) na tabletach |
| **Oprogramowanie** | 1. Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów współdzielonych 2. Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów 3. Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wpierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym. 4. Urządzenie musi umożliwiać pracę w trybie klastra wysokiej dostępności (HA) aby zapewnić nieprzerwany, natychmiastowy dostęp do zasobów bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system). Wszystkie dane z powodzeniem zapisane na serwerze aktywnym będą na bieżąco kopiowane do serwera pasywnego zapewniając replikację w czasie rzeczywistym i dostęp do danych oraz usług w przypadku uszkodzenia jednostki aktywnej dając gwarancję ciągłości pracy. Utworzenie klastra HA ma się opierać o 2 identyczne urządzenia. |
| **Konserwacja** | Możliwość przeprowadzenia konserwacji urządzenia przy użyciu dodatkowych, wygodnych w użyciu przesuwnych szyn RACK |
| **Gwarancja** | 24 miesiące gwarancji producenta |
| **Oprogramowanie do wykonywania kopii zapasowych – 1 szt.** | |
| **Ogólne** | Dostawa i konfiguracja licencji oprogramowania do zarządzania środowiskiem wirtualnym wraz z rozszerzeniem umożliwiającym obsługę do 30 systemów wirtualnych wraz ze zintegrowanym system kopii zapasowych. Licencja ma być wydana na zasadach wolnej licencji lub innej równoważnej.  Z licencji będą korzystać dwie jednostki objęte projektem: Urząd Gminy Somonino oraz Gminny Ośrodek Pomocy Społecznej Somonino. |
| **Wymagania funkcjonalne** | 1. Możliwość zarządzania środowiskiem wirtualnym, w tym uruchamianie, monitorowanie i zarządzanie maszynami wirtualnymi oraz kontenerami. 2. Obsługa do 30 systemów wirtualnych w ramach jednego środowiska. 3. Integracja z popularnymi narzędziami do tworzenia kopii zapasowych oraz odzyskiwania danych. 4. Możliwość konfiguracji klastrów i migracji maszyn wirtualnych między węzłami w czasie rzeczywistym. 5. Obsługa zaawansowanych funkcji sieciowych, takich jak VLAN, mostkowanie i routing. 6. Mechanizmy wysokiej dostępności (HA) dla maszyn wirtualnych. |
| **Optymalizacja środowiska wirtualnego** | 1. Thin Provisioning: Możliwość alokacji przestrzeni dyskowej według faktycznego zużycia. 2. Kontenery LXC: W przypadku lekkich aplikacji musi istnieć możliwość wykorzystania kontenerów, które zużywają mniej zasobów w porównaniu do pełnych maszyn wirtualnych. 3. Replikacja danych: Użycie wbudowanego mechanizmu replikacji danych dla szybkiego przywracania systemów w razie awarii. |
| **Kopie zapasowe i odzyskiwanie danych** | System musi posiadać zintegrowany system kopii zapasowych, umożliwiający:   * Regularne wykonywanie kopii zapasowych wszystkich 30 systemów wirtualnych. * Przechowywanie danych na zewnętrznych nośnikach (np. serwerach NFS, Amazon S3, lokalnych macierzach). |
| **Monitorowanie i zarządzanie** | 1. Interfejs webowy: Intuicyjny panel zarządzania musi pozwalać na monitorowanie obciążenia CPU, RAM oraz przestrzeni dyskowej. 2. Powiadomienia i alerty: Możliwość konfiguracji powiadomień o awariach lub przeciążeniach systemu. |
| **Skalowanie** | Środowisko dla 30 maszyn musi być łatwo skalowalne w postaci:   1. Możliwości dodania kolejnych węzłów do klastra. 2. Możliwość rozbudowy pamięci RAM i przestrzeni dyskowej w istniejących serwerach. |
| **Migracja danych** | Zamawiający wymaga migracji istniejących maszyn wirtualnych i / lub fizycznych do środowiska:   1. P2V (Physical to Virtual):  * Migracja serwerów fizycznych do maszyn wirtualnych.  1. V2V (Virtual to Virtual):  * Migracja istniejących VM z innych platform (np. VMware, Hyper-V).  1. Testy migracji:  * Przeprowadzenie migracji próbnej w celu weryfikacji poprawności działania systemów. |
| **Wymagania techniczne** | 1. Oprogramowanie powinno działać na otwartym systemie operacyjnym. 2. Wsparcie dla wirtualizacji opartej na KVM oraz obsługa kontenerów w technologii LXC. 3. Możliwość zarządzania środowiskiem przez interfejs webowy oraz wiersz poleceń. 4. Mechanizmy autoryzacji użytkowników z możliwością integracji z zewnętrznymi systemami uwierzytelniania (np. LDAP, Active Directory). 5. Obsługa standardowych protokołów sieciowych i pamięci masowej (np. iSCSI, NFS, CIFS). |
| **Wymagania licencyjne** | 1. Licencja musi być udzielona na zasadach wolnej licencji lub równoważnych, umożliwiających pełne wykorzystanie oprogramowania bez ograniczeń czasowych. 2. Rozszerzenie licencji musi obejmować obsługę do 30 systemów wirtualnych. |
| **Szkolenie i dokumentacja** | Zamawiający wymaga kompleksowego szkolenia dla Kierownika działu IT oraz dostarczenia pełnej dokumentacji powdrożeniowej:   1. Szkolenie dedykowane dla Kierownika działu IT. Zamawiający dopuszcza możliwość przeprowadzenia szkolenia w formie on-line. Wymaga ilość godzin przewidzianych na szkolenie to 5h.  * Obsługa i zarządzanie środowiskiem. * Tworzenie i zarządzanie kopią zapasową oraz monitorowanie.  1. Dokumentacja:  * Opis architektury środowiska, konfiguracji oraz procedur awaryjnych. |
| **Warunki serwisu i opieki nad konfiguracją** | 1. Monitoring i zarządzanie środowiskiem:  * Stały monitoring infrastruktury Systemu (dostępność, wydajność, obciążenie zasobów). * Zarządzanie węzłami klastra, maszynami wirtualnymi (VM) i kontenerami (LXC).  1. Aktualizacje i konserwacja:  * Regularne instalowanie poprawek systemowych, aktualizacji bezpieczeństwa oraz nowych wersji Systemu.  1. Zarządzanie kopią zapasową:  * Utrzymanie harmonogramów kopii zapasowych oraz testy odzyskiwania danych. * Weryfikacja integralności i bezpieczeństwa danych kopii zapasowych.  1. Reakcja na awarie:  * Usuwanie awarii serwerów fizycznych, maszyn wirtualnych oraz usług uruchomionych w środowisku Systemu. * Diagnoza i naprawa błędów konfiguracji.  1. Wsparcie techniczne:  * Zdalne wsparcie dla administratorów w zakresie rozwiązywania problemów. * Doradztwo w zakresie optymalizacji środowiska wirtualizacyjnego. |
| **Czas Reakcji** | W zależności od kategorii zgłoszenia, czas reakcji wynosi:   1. Awaria krytyczna (np. niedostępność całego klastra Systemu lub głównych usług):  * Czas reakcji: do 6 godziny. * Czas naprawy: maksymalnie 4 godziny (zdalnie)  1. Problem istotny (np. niedostępność pojedynczej maszyny wirtualnej, problemy z wydajnością):  * Czas reakcji: do 24 godzin od momentu przekazania przez Zamawiającego zgłoszenia. Przez reakcję rozumie się pisemne potwierdzenie przyjęcia zgłoszenia. * Czas naprawy: maksymalnie 24 godziny (zdalnie) od momentu potwierdzenia przyjęcia zgłoszenia. |
| **Warunki Gwarancyjne** | Do 31.12.2025r.   1. W ramach umowy serwisowej zapewniona musi być opieka nad środowiskiem Systemu oraz jego komponentami. 2. Gwarancja musi dotyczyć:  * Konfiguracji węzłów. * Funkcjonalności maszyn wirtualnych i kontenerów. * Działania usług związanych z monitoringiem i kopią zapasową.  1. Zamawiający wymaga, aby w ramach realizacji przedmiotu zamówienia Wykonawca zapewni wsparcie serwisowe w wymiarze 50h do 31.12.2025r. |
| **Oprogramowanie do wykonywania kopii zapasowych – warunki świadczenia usługi opieki serwisowej w okresie utrzymania projektu – 1 szt.** | |
| **Warunki serwisu i opieki nad konfiguracją** | 1. Monitoring i zarządzanie środowiskiem:  * Stały monitoring infrastruktury Systemu (dostępność, wydajność, obciążenie zasobów). * Zarządzanie węzłami klastra, maszynami wirtualnymi (VM) i kontenerami (LXC).  1. Aktualizacje i konserwacja:  * Regularne instalowanie poprawek systemowych, aktualizacji bezpieczeństwa oraz nowych wersji Systemu.  1. Zarządzanie kopią zapasową:  * Utrzymanie harmonogramów kopii zapasowych oraz testy odzyskiwania danych. * Weryfikacja integralności i bezpieczeństwa danych kopii zapasowych.  1. Reakcja na awarie:  * Usuwanie awarii serwerów fizycznych, maszyn wirtualnych oraz usług uruchomionych w środowisku Systemu. * Diagnoza i naprawa błędów konfiguracji.  1. Wsparcie techniczne:  * Zdalne wsparcie dla administratorów w zakresie rozwiązywania problemów. * Doradztwo w zakresie optymalizacji środowiska wirtualizacyjnego. |
| **Czas Reakcji** | W zależności od kategorii zgłoszenia, czas reakcji wynosi:   1. Awaria krytyczna (np. niedostępność całego klastra Systemu lub głównych usług):  * Czas reakcji: do 6 godziny. * Czas naprawy: maksymalnie 4 godziny (zdalnie)  1. Problem istotny (np. niedostępność pojedynczej maszyny wirtualnej, problemy z wydajnością):  * Czas reakcji: do 24 godzin od momentu przekazania przez Zamawiającego zgłoszenia. Przez reakcję rozumie się pisemne potwierdzenie przyjęcia zgłoszenia. * Czas naprawy: maksymalnie 24 godziny (zdalnie) od momentu potwierdzenia przyjęcia zgłoszenia. |
| **Warunki Gwarancyjne** | 2 lata od 01.01.2026r. do 31.12.2027r.   1. W ramach umowy serwisowej zapewniona musi być opieka nad środowiskiem Systemu oraz jego komponentami. 2. Gwarancja musi dotyczyć:  * Konfiguracji węzłów. * Funkcjonalności maszyn wirtualnych i kontenerów. * Działania usług związanych z monitoringiem i kopią zapasową.  1. Zamawiający wymaga, aby w ramach realizacji przedmiotu zamówienia Wykonawca zapewnił wsparcie serwisowe w wymiarze 100h przez okres 2 lat |
| **Oprogramowanie do monitorowania infrastruktury informatycznej – 1 szt.** | |
| **Ogólne** | Oprogramowanie musi umożliwiać zarządzanie 30 stacjami roboczymi. Z licencji będzie korzystać jedna z jednostek objętych projektem: Gminny Ośrodek Pomocy Społecznej Somonino.  Oprogramowanie musi posiadać budowę modułową, składać się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Instalacje zdalnych konsoli zarządzania nie może podlegać limitom i nie może być objęte dodatkowym licencjonowaniem. Komunikacja pomiędzy Serwerem a Agentami i Konsolami nawiązywana jest przy użyciu szyfrowanego protokołu TLS 1.2. Program musi umożliwiać zmianę portu komunikacyjnego wykorzystywanego przez konsolą zarządzającą.  Moduły muszą 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, bezpieczny, stabilny i wysoce wydajny silnik bazy danych z kodem źródłowym dostępnym na licencji open-source tj. PostgreSQL w wersji 15 lub równoważny, dzięki czemu nie może być objęty limitem ilości danych, baza danych musi być rozwiązaniem darmowym niewymagającym dodatkowego licencjonowania. Agent programu musi korzystać z bazy danych z wydajnym i stabilnym silnikiem SQLite lub równoważnym, która nie może wymagać dodatkowego licencjonowania. Instalacja Serwera oraz Konsol zarządzających wymaga 64-bitowego systemu operacyjnego Windows. Oprogramowanie musi zawierać rozbudowany system raportowy zawierający raporty predefiniowane oraz umożliwiający tworzenie własnych raportów wraz z możliwością pełnego dostosowania wyglądu.  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. Muszą być one również grupowane w osobnym, dedykowanym oknie. Musi pozwalać to na, zgodne z RODO, usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej.  Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, objęty musi być kontrolą na poziomie wybranych Administratorów – w programie musi być 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 np. może wyłączyć możliwość zdalnej deinstalacji Agenta, ograniczyć dostęp do Opcji programu oraz logów działań innych administratorów. Działania administratorów muszą być logowane, co oznacza, 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. Musi istnieć możliwość, aby działania administratorów były automatycznie eksportowane do zewnętrznego kolektora Syslog. Musi istnieć możliwość, aby lista kont użytkowników, w tym administratorów, była synchronizowana z Active Directory wraz z awatarami, również przez szyfrowane połączenie LDAPS. Program musi umożliwiać również tworzenie lokalnych kont użytkowników wraz z awatarami w środowiskach bez Active Directory. Liczba kont użytkowników w konsoli nie może być objęta limitem i nie może podlegać licencjonowaniu.  Program musi umożliwiać konfigurację polityki haseł do lokalnych kont użytkowników konsoli, 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 musi istnieć możliwość pominięcia tylko w lokalnej konsoli serwera. |
| **Monitorowanie infrastruktury (bezagentowo)** | Monitorowanie infrastruktury (bezagentowo) musi obejmować serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:   1. wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping 2. wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU) 3. wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci 4. wizualizacji urządzeń na mapach z funkcją siatki umożliwiającej korygowanie pozycji ikon na mapie do najbliższej linii siatki 5. wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła. 6. wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku 7. wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach o dowolnym rozmiarze i kolorze 8. wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie 9. wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny 10. zablokowania mapy urządzeń przed przypadkową edycją 11. serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów 12. serwerów pocztowych:  * program musi monitorować czas logowania do serwisu odbierającego oraz czas wysyłania poczty * program musi mieć 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 musi mieć możliwość wykonywania operacji testowych * program musi mieć możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa  1. monitorowania serwerów WWW i adresów URL 2. cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS 3. obsługi szyfrowania SSL/TLS w powiadomieniach e-mail 4. 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  1. obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych 2. 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  1. serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie 2. 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 3. monitorowania stanu maszyn wirtualnych Vmware: działa, nie działa, wstrzymano 4. zarządzania stanem maszyn wirtualnych Vmware: wysyłanie poleceń włączenia, wstrzymania i wyłączenia zasilania do każdej maszyny 5. wydajności systemów Windows:  * obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy   Program musi posiadać Inteligentne Mapy i Oddziały, które służą do lepszego zarządzania logiczną strukturą urządzeń (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 musi posiadać również funkcję kompilatora plików MIB, który umożliwia dodawanie definicji dla modułów SNMP.  Program musi umożliwiać 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 muszą być budowane 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 muszą pozwalać na priorytetyzację urządzeń, grupowanie wg. ważności i typu urządzenia. Oprogramowanie musi umożliwiać wykorzystanie w alarmowaniu skrzynek e-mail z wykorzystaniem autoryzacji OAuth 2.0  Program musi mieć możliwość integracji ze sprzętową bramką GSM HW-SMS-GW 3 w celu wysyłania powiadomień SMS z wykorzystaniem protokołu netGSM (SOAP) oraz poprzez integrację z bramkami SMSEagle. |
| **Inwentaryzacja** | W zakresie inwentaryzacji program musi automatycznie gromadzić informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz:   1. Prezentować szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp. 2. Umożliwiać odczyt parametrów S.M.A.R.T. dysków twardych, dysków SSD, w tym NVMe. 3. Obejmować m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade. 4. Informować o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio ma umożliwiać audytowanie i weryfikację użytkowania licencji w organizacji. 5. Zbierać informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd. 6. Posiadać możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera. 7. Umożliwiać odczytanie numeru seryjnego (klucze licencyjne). 8. Umożliwiać automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych. 9. Umożliwiać przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp. 10. Umożliwiać 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. Umożliwiać wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji muszą być logowane.   Moduł inwentaryzacji zasobów musi umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania:   1. przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji, 2. przydzielania dostępu administratorów do zasobów na podstawie praw do oddziałów, 3. tworzenia powiązań między zasobami a urządzeniami, 4. tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych, 5. tworzenia relacji pomiędzy zasobami, 6. wskazania osób uprawnionych do użycia zasobów poprzez rozbudowane mechanizmy, 7. definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania musi istnieć 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, 8. określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów, 9. określenia atrybutów dodatkowych tylko dla wybranych typów zasobów, 10. masową edycję atrybutów zasobów, 11. definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie, 12. importu danych z zewnętrznego źródła (.CSV), 13. przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp., 14. tworzenia powiązań między zasobami a dokumentami w relacji 1:N, 15. oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp., 16. ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności, 17. generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania, 18. przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji, 19. konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca, 20. konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca, 21. archiwizacji i porównywania audytów zasobów, 22. tworzenia kodów kreskowych dla zasobów, 23. drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy, 24. 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, 25. możliwość zmiany portu komunikacyjnego wykorzystywanego przez aplikację mobilną dla systemu Android, 26. inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline), 27. 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 musi zapewniać 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 muszą posiadać możliwość filtrowania elementów per oddział. |
| **Obsługa użytkowników** | W zakresie obsługi użytkowników program musi umożliwiać monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie:   1. Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy), 2. Procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach, 3. 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, 4. Informacji o edytowanych przez użytkownika dokumentach, 5. Historii pracy (cykliczne zrzuty ekranowe), 6. Listy odwiedzanych stron WWW (tytuły, adresy, liczba i czas wizyt), 7. Transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika), 8. 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 musi mieć możliwość monitorowania kosztów wydruków, 9. Nagłówków przesyłanej w aplikacjach klienckich poczty e-mail.   Program ponadto musi posiadać możliwość:   1. wykrywania podejrzanej aktywności przez popularne „jigglery”, mającej na celu symulowanie faktycznej pracy. 2. zdefiniowania czasu (min. 15 minut) gdy wykrywana będzie symulowana aktywność wyłącznie przez ruch myszą bez kliknięcia lub wprowadzanie tego samego znaku z klawiatury. 3. wyszczególnienia podejrzanej aktywności w raportach. 4. wygenerowania alarmu i wykonania akcji po wykryciu podejrzanej aktywności. 5. automatycznego włączenia zapisywania zrzutów ekranowych po wykryciu podejrzanej aktywności. 6. 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. 7. integracji list stron w formie plików .TXT z dowolnego adresu zewnętrznego np. CERT. 8. skorzystania z wbudowanej listy stron sklasyfikowanych jako zagrożenia. 9. automatycznego odświeżania list stron zintegrowanych z adresów zewnętrznych. 10. blokowania ruchu na wskazanych portach TCP/IP, 11. blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem, 12. 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, 13. przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika), 14. 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 musi posiadać Grupy użytkowników oraz Grupy Inteligentne, które służą do lepszego zarządzania użytkownikami, polityką monitorowania oraz blokowania aplikacji i stron internetowych. |
| **Zdalna pomoc Użytkownikom** | Program musi umożliwiać 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 musi mieć możliwość wyboru dowolnego ekranu (monitora) oraz zablokowania działania myszy oraz klawiatury dla użytkownika. Funkcja zdalnego dostępu musi umożliwiać równoczesne podłączenie do tego samego komputera kilku administratorom.  W tym module musi znajdować 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 musi pozwalać na integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0. Moduł musi umożliwiać również przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o sygnalistach”) oraz zawierać 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 musi umożliwiać 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 musi pozwalać na:   1. zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej 2. rozmowy również między „zwykłymi” użytkownikami 3. osadzanie załączników w treści wiadomości, 4. osadzanie obrazków w treści wiadomości, 5. formatowanie tekstu, 6. tworzenie pokojów tematycznych, rozmów grupowych 7. oznaczanie kontaktów jako „ulubionych” na liście kontaktów 8. uruchomienie z poziomu ikony dostępowej Agenta oraz bezpośrednio w interfejsie WWW heldpesku 9. musi mieć możliwość wyświetlania w trybie jasnym lub ciemnym   W module musi być zawarta również baza wiedzy pomagająca użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy wraz z możliwością nadawania artykułom 1 z 3 statusów (opublikowany, wewnętrzny, szkic). Program musi umożliwiać 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 musi mieć możliwość przeglądnięcia historii odczytanych komunikatów bezpośrednio z poziomu ikony Agenta. Administrator musi mieć możliwość tworzenia szkiców i archiwizowania komunikatów.  Dostęp do systemu zgłoszeń oraz bazy wiedzy realizowany musi być przez dedykowany portal dostępny przez przeglądarkę internetową, który może być wyświetlany w trybie jasnym lub ciemnym.  Modułu musi umożliwiać 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 musi umożliwiać:   1. pobieranie listy użytkowników z Active Directory wraz z awatarami, 2. wyświetlanie w systemie zgłoszeń wizytówki użytkownika wraz z jego numerem telefonu, adresem e-mail oraz informacją o przełożonym, 3. zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont, 4. zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez rozbudowany system zarządzania regułami widoczności zgłoszeń, 5. zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii zgłoszeń, 6. zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii artykułów bazy wiedzy, 7. tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO, 8. automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników, 9. definiowanie ścieżek akceptacji zgłoszeń – procesu, w którym użytkownik uzyskuje akceptację na realizację zgłoszenia od wyznaczonych osób w organizacji, 10. przypisywanie ścieżek akceptacji zgłoszeń do określonych kategorii, 11. procesowanie zgłoszeń użytkowników z wiadomości e-mail, 12. dostęp do plików źródłowych wiadomości e-mail przetworzonych na zgłoszenia, 13. obsługę wielu adresów e-mail jednego użytkownika w celu przetwarzania jako zgłoszeń pochodzących od tej samej osoby, 14. eksportowania listy zgłoszeń do plików CSV i XLSX, 15. integrację ze wieloma skrzynkami e-mail w celu obsługi różnych kanałów zgłoszeń wraz z automatyzacjami, 16. integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0, 17. tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń, 18. wykonywanie operacji na wielu zgłoszeniach równocześnie, 19. dołączanie załączników do zgłoszeń, 20. usuwanie zamkniętych zgłoszeń, 21. rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy, 22. szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników, 23. wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia, 24. zrzuty ekranowe (podgląd pulpitu), 25. zdalną modyfikację rejestrów, 26. dystrybucję oprogramowania przez Agenty, 27. definiowanie aplikacji dozwolonych do samodzielnej instalacji przez użytkowników z pakietów MSI w postaci Kiosku z Aplikacjami, 28. przypisywanie dostępnych w Kiosku instalatorów do grup użytkowników, 29. dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI), 30. zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku, 31. możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu, 32. możliwość skonfigurowania automatyzacji dodających komentarze publiczne wraz z załącznikami i odnośnikami do artykułów w Bazie Wiedzy, 33. planowanie nieobecności pracowników helpdesk, 34. obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem, 35. generowanie raportów obsługi helpdesk, 36. zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu), 37. zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami), 38. wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików bez blokowania interfejsu programu podczas przesyłania plików. |
| **Ochrona danych przed wyciekiem** | 1. Blokowanie urządzeń i nośników danych.   Program musi mieć 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.   1. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek. 2. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA. 3. Blokownie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane. 4. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych. 5. Funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender. 6. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker. 7. Funkcje wspierające bezpieczeństwo systemu: zdalne szyfrowanie dysków za pomocą BitLocker. 8. Funkcje wspierające bezpieczeństwo systemu: zapisywanie klucza odzyskiwania do pliku oraz jako zasób w bazie danych programu. 9. Funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu. 10. Funkcje wspierające bezpieczeństwo systemu: odczytanie informacji o aktywnym oprogramowaniu antywirusowym firm trzecich, innym niż Windows Defender. 11. 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:   1. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych. 2. 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 musi umożliwiać prowadzenie rejestru naruszeń blokad podłączanych nośników. |
| **Gwarancja** | Do 31.12.2025r. |
| **Oprogramowanie do monitorowania infrastruktury informatycznej – warunki świadczenia usługi opieki serwisowej w okresie utrzymania projektu – 1 szt.** | |
| **Gwarancja** | 2 lata od 01.01.2026r. do 31.12.2027r. |
| **Oprogramowanie antywirusowe z funkcją EDR - licencja na 110 stanowisk – 1 komplet.** | |
| **Ogólne** | Z licencji będą korzystać dwie jednostki objęte projektem: Urząd Gminy Somonino (80 stanowisk) oraz Gminny Ośrodek Pomocy Społecznej Somonino (30 stanowisk). |
| **Administracja zdalna w chmurze** | 1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego. 2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW. 3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL. 4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. 5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. 6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM. 7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak. 9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta. 10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. 11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. 12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej. |
| **Ochrona stacji roboczych** | 1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). 2. Rozwiązanie musi wspierać architekturę ARM64. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. 5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. 9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku. 10. Rozwiązanie musi integrować się z Intel Threat Detection Technology. 11. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 13. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 14. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 15. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia. 16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:  * tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, * tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, * tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, * tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, * tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.  1. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. 2. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. 3. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. 4. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 5. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 6. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook. 7. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:  * tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące, * tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie, * tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora, * tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.  1. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki. 2. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika. 3. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki. 4. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych. 5. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii. 6. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. 7. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum. |
| **Ochrona serwera** | 1. Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux. 2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS. 5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji. 7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. 8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.   Dodatkowe wymagania dla ochrony serwerów Windows:   1. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. 2. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS). 3. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. 4. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 5. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 6. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 7. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 8. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. 9. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.   Dodatkowe wymagania dla ochrony serwerów Linux:   1. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. 2. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. 3. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon. 4. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu. |
| **Szyfrowanie** | 1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10 i Microsoft Windows 11. 2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault). 3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia. 4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI. |
| **Ochrona urządzeń mobilnych opartych o system Android** | 1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. 2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne. 3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). 4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM. 5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi: 6. usunięcie zawartości urządzenia, 7. przywrócenie urządzenie do ustawień fabrycznych, 8. zablokowania urządzenia, 9. uruchomienie sygnału dźwiękowego, 10. lokalizację GPS. 11. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. 12. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: 13. nazwę aplikacji, 14. nazwę pakietu, 15. kategorię sklepu Google Play, 16. uprawnienia aplikacji, 17. pochodzenie aplikacji z nieznanego źródła. |
| **Sandbox w chmurze** | 1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. 2. Rozwiązanie musi wykorzystywać do działania chmurę producenta. 3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi. 4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta. 5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek. 6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania. 7. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów. 8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy. 9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione. 10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych. 11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo. 12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem: 13. Czysty, 14. Podejrzany, 15. Bardzo podejrzany, 16. Szkodliwy. 17. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum. 18. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki. 19. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia. |
| **Moduł XDR** | 1. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW. 2. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta. 3. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL. 4. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa. 5. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”. 6. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia. 7. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika. 8. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta. 9. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej. 10. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku. 11. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania. 12. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny. 13. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej. 14. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych. 15. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich. 16. Konsola administracyjna musi mieć możliwość tagowania obiektów. 17. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell. |
| **Gwarancja oraz wsparcie** | System musi być objęty serwisem gwarancyjnym producenta do 31.12.2025r. |
| **Oprogramowanie antywirusowe z funkcją EDR - licencja na 110 stanowisk – warunki świadczenia usługi opieki serwisowej w okresie utrzymania projektu – 1 komplet.** | |
| **Gwarancja oraz wsparcie** | System musi być objęty serwisem gwarancyjnym producenta przez 2 lata od 01.01.2026r. do 31.12.2027r. |
| **Oprogramowanie Email Secure Gateway – 1 szt.** | |
| **Wymagania Ogólne** | System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware’ową bez limitu licencyjnego na ilość chronionych kont użytkowników.  Dopuszcza się aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.  Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń.  Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów:   1. Tryb Gateway. 2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej). |
| **Parametry fizyczne systemu antyspamowego** | 1. System musi być wyposażony w interfejsy:   4 porty Gigabit Ethernet RJ-45.   1. System musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 1 TB . 2. System musi posiadać wbudowany port konsoli szeregowej. 3. Zasilanie z sieci 230V/50Hz. |
| **Ogólne funkcje systemu ochrony poczty** | Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:   1. Wsparcie dla co najmniej 20 domen pocztowych. 2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 28 tyś wiadomości/godzinę. 3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all). 4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP. 5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości). 6. Możliwość ograniczenia ilości poczty wychodzącej do chronionych domen w oparciu o nie mniej niż: ilość jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie. 7. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej. 8. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów. 9. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP. 10. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika. 11. Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora. 12. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail. 13. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki. 14. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI. 15. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu. 16. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników. 17. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika. |
| **Kontrola antywirusowa i ochrona przed malware** | W tym zakresie dostarczony system ochrony poczty musi zapewniać:   1. Skanowanie antywirusowe wiadomości SMTP. 2. Kwarantannę dla zainfekowanych plików. 3. Skanowanie załączników skompresowanych. 4. Definiowanie komunikatów powiadomień w języku polskim. 5. Blokowanie załączników w oparciu o typ pliku. 6. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antywirusowej. 7. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu. 8. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora. 9. Ochronę typu wirus outbrake. 10. Ochronę przed zagrożeniami zawartymi wiadomościach pocztowych i w załącznikach (nie mniej niż: pliki MS Office, PDF, HTML, tekstowe) poprzez usuwanie treści będących zagrożeniem (makra, adresy URL zagnieżdżone w plikach, skrypty, ActiveX) i dostarczaniem oczyszczonych w ten sposób wiadomości. |
| **Kontrola antyspamowa** | System musi zapewniać poniższe funkcje i metody filtrowania spamu:   1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta. 2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania. 3. Szczegółowa kontrola nagłówka wiadomości. 4. Analiza Heurystyczna. 5. Współpraca z zewnętrznymi serwerami RBL, SURBL. 6. Filtrowanie w oparciu o filtry Bayes’a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen. 7. Możliwością dostrajania filtrów Bayes’a przez poszczególnych użytkowników. 8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF. 9. Kontrola w oparciu o Greylisting oraz SPF. 10. Filtrowanie treści wiadomości i załączników. 11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości. 12. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antyspamowej. 13. Ochrona typu outbrake. 14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking). 15. Możliwość skanowania linków znajdujących się w przesyłkach pocztowych, w momencie ich kliknięcia przez adresata. 16. Możliwość wykrywania i ochrony przed podszywaniem się (spoofing) pod wiadomości wysyłane przez osoby na stanowiskach kierowniczych (C-level) 17. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora. |
| **Ochrona przed atakami na usługę poczty** | System musi zapewniać poniższe funkcje i metody filtrowania:   1. Ochrona przed atakami na adres odbiorcy (m.in. email bombing). 2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu. 3. Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu. 4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing). 5. Weryfikacja poprawności adresu e-mail nadawcy. |
| **Funkcje logowania i raportowania** | W tym zakresie dostarczony system ochrony poczty musi zapewniać:   1. Logowanie do zewnętrznego serwera SYSLOG. 2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku. 3. Logowanie informacji na temat spamu oraz niedozwolonych załączników. 4. Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych. 5. Możliwość analizy przebiegu sesji SMTP. 6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych. 7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu. 8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu. |
| **Funkcje pracy w trybie wysokiej dostępności (HA)** | System ochrony poczty musi zapewniać poniższe funkcje:   1. Konfigurację HA w każdym z trybów: gateway, transparent. 2. Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP. 3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu. 4. Monitorowanie stanu pracy klastra. |
| **Aktualizacje sygnatur, dostęp do bazy spamu** | W tym zakresie dostarczony system ochrony poczty musi zapewniać:   1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym. 2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę. |
| **Zarządzanie** | System ochrony poczty musi zapewniać poniższe funkcje:   1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH. 2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy. 3. Powinna istnieć możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych. |
| **Serwisy i licencje** | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:  1. Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbrake, Sandbox w chmurze, ochrona typu Click Protect, Content Disarm & Reconstruction, Business Email Compromise przez cały okres gwarancji. |
| **Gwarancja oraz wsparcie** | System musi być objęty serwisem gwarancyjnym producenta lub autoryzowanego dystrybutora do 31.12.2025r. polega na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7 przez stronę internetową i telefonicznie.  Usługa serwisowa musi być realizowana zgodnie z systemem ISO 9001 lub równoważnym |
| **Rozszerzone wsparcie serwisowe** | System musi być 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 cały okres gwarancji.  Podmiot serwisujący musi posiadać certyfikat ISO 9001 lub równoważny w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. |
| **Oprogramowanie Email Secure Gateway – warunki świadczenia usługi opieki serwisowej w okresie utrzymania projektu – 1 szt.** | |
| **Serwisy i licencje** | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:  1. Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbrake, Sandbox w chmurze, ochrona typu Click Protect, Content Disarm & Reconstruction, Business Email Compromise przez 2 lata od 01.01.2026r. do 31.12.2027r. |
| **Gwarancja oraz wsparcie** | System musi być objęty serwisem gwarancyjnym producenta, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |
| **Rozszerzone wsparcie serwisowe** | System musi być 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 cały okres gwarancji.  Podmiot serwisujący musi posiadać certyfikat ISO 9001 lub równoważny w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. |
| **Software onetime password tokens (20 sztuk) – 1 komplet.** | |
| **Ogólne** | Przedmiotem zamówienia są tokeny programowe umożliwiające generowanie jednorazowych haseł dostępowych dla systemów zabezpieczeń informatycznych Zamawiającego. Oprogramowanie powinno wspierać mechanizmy dwuskładnikowego uwierzytelniania i być kompatybilne z istniejącą infrastrukturą informatyczną Zamawiającego oraz opisanym w OPZ UTM - Unified Threat Management. |
| **Wymagania funkcjonalne** | 1. Generowanie haseł jednorazowych:  * Obsługa algorytmów zgodnych ze standardami branżowymi.  1. Integracja z istniejącą infrastrukturą. 2. Dostępność aplikacji klienckich:  * Aplikacje mobilne dla systemów Android i iOS.  1. Zarządzanie:  * Możliwość centralnego zarządzania tokenami. * Wsparcie dla funkcji dodawania, usuwania i resetowania tokenów przez administratora.  1. Mechanizmy bezpieczeństwa:  * Wykrywanie i przeciwdziałanie próbom nieautoryzowanego dostępu. |
| **UTM - Unified Threat Management – 1 szt.** | |
| **Wymagania Ogólne** | System bezpieczeństwa musi realizować 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 musi realizować funkcję Firewall zapewniając pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.  System musi umożliwiać 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 5 administratorów do poszczególnych instancji systemu.  System musi wspierać 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 – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall musi zapewniać 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 musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto musi dawać możliwość tworzenia interfejsów redundantnych. |
| **Interfejsy, Dysk, Zasilanie** | 1. System realizujący funkcję Firewall musi dysponować co najmniej poniższą liczbą i rodzajem interfejsów: 5 portów Gigabit Ethernet RJ-45. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB. 3. System Firewall musi pozwalać skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q. 4. System musi być wyposażony w zasilanie AC. |
| **Parametry wydajnościowe** | 1. W zakresie Firewall’a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- min. 1 Gbps. 6. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus – min. 500 Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – min. 300 Mbps. |
| **Funkcje Systemu Bezpieczeństwa** | W ramach systemu ochrony muszą być 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 . 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. 10. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 11. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system. 12. Rozwiązanie musi posiadać 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 musi uwzględniać: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi realizować translację adresów NAT: źródłowego i docelowego, translację PAT oraz:  * Translację jeden do jeden oraz jeden do wielu. * Dedykowany ALG (Application Level Gateway) dla protokołu SIP.  1. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP. 3. Polityka firewall musi umożliwiać filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 4. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 5. Element systemu realizujący funkcję Firewall musi integrować 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 musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:  * Wsparcie dla IKE v1 oraz v2. * Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). * Obsługa protokołu Diffie-Hellman grup 19, 20. * Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. * Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. * Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. * Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. * Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. * Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. * Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. * Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. * Mechanizm „Split tunneling” dla połączeń Client-to-Site.  1. Producent rozwiązania musi posiadać 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 musi zapewniać obsługę:   1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego). 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 musi umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN musi wspierać zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec). |
| **Zarządzanie pasmem** | 1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System musi dawać możliwość określania pasma dla poszczególnych aplikacji. 3. System musi pozwalać zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. |
| **Ochrona przed malware** | 1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy musi zapewniać skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. W przypadku archiwów zagnieżdżonych musi istnieć możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum. 4. System musi umożliwiać blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System musi dysponować 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 musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. 8. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 9. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu. |
| **Ochrona przed atakami** | 1. Ochrona IPS musi opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System musi chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków musi zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać 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. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. 8. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie. |
| **Kontrola aplikacji** | 1. Funkcja Kontroli Aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji musi zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) muszą być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur musi zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. 6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 7. System musi dawać 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 musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra WWW muszą być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem np.: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW musi umożliwiać statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwalać definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW musi dawać 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 musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System musi pozwalać określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji. |
| **Uwierzytelnianie użytkowników w ramach sesji** | 1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:  * Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. * Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. * Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.  1. System musi dawać możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego. 2. System musi umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. 3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. |
| **Zarządzanie** | 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Musi istnieć możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System musi dawać możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall musi umożliwiać 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 muszą realizować 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 musi zapewniać przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto musi zapewniać możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 4. Możliwość włączenia logowania per reguła w polityce firewall. 5. System musi zapewniać możliwość logowania do serwera SYSLOG. 6. Przesyłanie SYSLOG do zewnętrznych systemów musi być możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS. |
| **Testy wydajnościowe oraz funkcjonalne** | Wszystkie funkcje i parametry wydajnościowe systemu muszą być możliwe do zweryfikowania w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych w terminie 3 dni od dnia zawarcia umowy( Testy muszą być wykonane przez producenta rozwiązania nie wcześniej niż 90 dni przed zawarciem Umowy). |
| **Serwisy i licencje** | 1. Dla poprawności działania systemu firewall Zamawiający wymaga dostarczenia licencji: 2. 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 przez cały okres gwarancji. |
| **Gwarancja oraz wsparcie** | 1. System musi być objęty serwisem gwarancyjnym producenta lub autoryzowanego dystrybutora do 31.12.2025r., polega 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. Obsługa zgłoszenia w tym zwrot uszkodzonego urządzenia do producenta, bez dodatkowych kosztów po stronie Zamawiającego, realizowana przez producenta lub autoryzowanego dystrybutora w języku polskim przez okres gwarancji. 2. Dostarczone rozwiązanie musi być objęte rozszerzonym wsparciem technicznym gwarantującym:   - w przypadku awarii - odbiór i zwrot urządzenia do producenta bez dodatkowych kosztów, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres wymaganej gwarancji;  -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 cały okres gwarancji   1. Wykonawca zapewni usługi wsparcia technicznego świadczone przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:   • obsługi procesu RMA u producenta,  • zdalnej pomocy w skonfigurowaniu urządzenia do współpracy z aktualnymi bazami funkcji ochronnych i serwisów producenta,  • jednorazowej podstawowej konfiguracji platformy realizowanej przez inżyniera z najwyższym dostępnym poziomem certyfikacji technicznej producenta,  • dostępie do szkolenia wideo prezentującego najlepsze praktyki współpracy z suportem producenta systemu realizującego funkcję Firewall.  Dostęp do usługi powinien być świadczony przez dedykowaną infolinię oraz przez dedykowany moduł internetowy.  Usługa gwarancyjna i wsparcia musi być świadczona przez podmiot posiadający certyfikat ISO 9001 lub równoważny w zakresie świadczenia usług serwisowych. |
| **UTM - Unified Threat Management – warunki świadczenia usługi opieki serwisowej w okresie utrzymania projektu – 1 szt.** | |
| **Serwisy i licencje** | 1. Dla poprawności działania systemu firewall Zamawiający wymaga dostarczenia licencji: 2. 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 przez 2 lata od 01.01.2026r. do 31.12.2027r. |
| **Gwarancja oraz wsparcie** | 1. System musi być objęty serwisem gwarancyjnym producenta lub autoryzowanego producenta, polega 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. Obsługa zgłoszenia w tym zwrot uszkodzonego urządzenia do producenta, bez dodatkowych kosztów po stronie Zamawiającego, realizowana przez producenta lub autoryzowanego dystrybutora w języku polskim przez okres gwarancji. 2. Dostarczone rozwiązanie musi być objęte rozszerzonym wsparciem technicznym gwarantującym:   - w przypadku awarii - odbiór i zwrot urządzenia do producenta bez dodatkowych kosztów, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres wymaganej gwarancji;  -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 cały okres gwarancji   1. Wykonawca zapewni usługi wsparcia technicznego świadczone przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:   • obsługi procesu RMA u producenta,  • zdalnej pomocy w skonfigurowaniu urządzenia do współpracy z aktualnymi bazami funkcji ochronnych i serwisów producenta,  • jednorazowej podstawowej konfiguracja platformy realizowanej przez inżyniera z najwyższym dostępnym poziomem certyfikacji technicznej producenta,  • dostępie do szkolenia wideo prezentującego najlepsze praktyki współpracy z suportem producenta systemu realizującego funkcję Firewall.  Dostęp do usługi powinien być świadczony przez dedykowaną infolinię oraz przez dedykowany moduł internetowy.  Usługa wsparcia musi być świadczona przez podmiot posiadający certyfikat ISO 9001 lub równoważny w zakresie świadczenia usług serwisowych. |
| **Oprogramowanie – 1 komplet (10 sztuk serwerowe oprogramowanie systemowe oraz 110 sztuk licencji dostępowych)** | |
| **Wymagania formalne** | 1. Dostarczone licencje na oprogramowanie muszą być bezterminowe. 2. Dostarczone licencje na oprogramowanie muszą objąć 10 sztuk licencji serwerowego oprogramowania systemowego oraz 110 sztuk licencji dostępowych. |
| **Serwerowe oprogramowanie systemowe** | Oprogramowanie powinno być w najnowszej stabilnej wersji na dzień składania ofert, kompatybilne z obecnymi standardami rynku i zapewniające długoterminowe wsparcie producenta.  Licencja na serwerowy system operacyjny musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowiskach serwerowego systemu operacyjnego niezależnie od liczby rdzeni w serwerze fizycznym.  Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy:   1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. 4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 9. Wbudowane wsparcie instalacji i pracy na wolumenach, które: - pozwalają na zmianę rozmiaru w czasie pracy systemu,   - umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,  - umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,  - umożliwiają zdefiniowanie list kontroli dostępu (ACL).   1. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 2. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 3. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 4. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 5. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 6. Dostępne dwa rodzaje graficznego interfejsu użytkownika:   - klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,  - dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.   1. W języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe. 2. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 3. Mechanizmy logowania w oparciu o:   - login i hasło,  - karty z certyfikatami (smartcard),  - wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).   1. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych. 2. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 3. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 4. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 5. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 6. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 7. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:   - Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,  - Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:   1. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, 2. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, 3. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. 4. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.   - Zdalna dystrybucja oprogramowania na stacje robocze.  - Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej  - Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego umożliwiająca:   1. Dystrybucję certyfikatów poprzez http, 2. Konsolidację CA dla wielu lasów domeny, 3. Automatyczne rejestrowanie certyfikatów pomiędzy różnymi lasami domen, 4. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.   - Szyfrowanie plików i folderów.  - Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).  - Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.  - Serwis udostępniania stron WWW.  - Wsparcie dla protokołu IP w wersji 6 (IPv6),  - Wsparcie dla algorytmów Suite B (RFC 4869),  - Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,  - Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:   1. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, 2. Obsługi ramek typu jumbo frames dla maszyn wirtualnych. 3. Obsługi 4-KB sektorów dysków 4. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra 5. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. 6. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) 7. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 8. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 9. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 10. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 11. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. |
| **Licencje dostępowe** | Licencje dostępowe w modelu użytkownika, które umożliwią indywidualnym użytkownikom korzystanie z zasobów serwera na poziomie infrastruktury informatycznej Zamawiającego.  Rodzaj licencji:  Typ licencji: przypisywana do użytkownika, umożliwiająca dostęp do zasobów serwera niezależnie od liczby i rodzaju urządzeń używanych przez daną osobę.  Zgodność z dostarczaną przez Wykonawcę wersją oprogramowania serwerowego.  Zakres funkcjonalny:  Umożliwienie użytkownikom dostępu do usług serwera, takich jak zarządzanie plikami, drukowanie, dostęp do baz danych, aplikacji i innych zasobów.  Obsługa urządzeń końcowych używanych przez licencjonowanego użytkownika, niezależnie od miejsca dostępu.  Obsługa wersji i zgodność:  Licencje muszą być kompatybilne z dostarczanym przez Wykonawcę oprogramowaniem serwerowym oraz muszą obejmować prawo do korzystania z poprawek i aktualizacji w okresie ważności.  Licencje muszą być dostarczone w formie elektronicznej.  Licencje muszą być licencjami bezterminowymi.  Oferowane licencje musza być nowe. |
| **Serwer RACK – TYP 1 – 3 szt.** | |
| **Obudowa** | Do instalacji w szafie RACK 19”, wysokość nie więcej niż 2U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych. Możliwość instalacji ramienia do zarządzania kablami. |
| **Procesor** | Architektura x86, maksymalny TDP dla procesora – maksymalnie 150W. Wymagana ilość rdzeni dla procesora – 16. Minimalna częstotliwość pracy procesora 2.0GHz. Minimalna ilość kanałów procesora – 8. Ilość kości pamięci na kanał – 2. Wynik wydajności procesora dla proponowanego serwera nie powinien być niższy niż 285 punkty base w teście SPECrate 2017 Integer, opublikowanym przez SPEC.org (www.spec.org) dla konfiguracji dwuprocesorowej. |
| **Liczba zainstalowanych procesorów** | 2 |
| **Płyta główna** | Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów wykonujących 64-bitowe instrukcje. |
| **Pamięć operacyjna** | Zainstalowane minimum 128GB pamięci RAM o częstotliwości 4800MHz. Pamięć zainstalowana w kościach mn. 32GB.  Minimum 32 sloty na pamięć. Możliwość rozbudowy do 8TB RAM. |
| **Zabezpieczenie pamięci** | Memory mirroring, ECC, SDDC, ADDDC |
| **Procesor Graficzny** | Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz. 1 port VGA na tylnym panelu. Możliwość zainstalowania drugiego portu VGA na przednim panelu serwera. |
| **Rozbudowa dysków** | W chwili dostawy serwer musi posiadać zainstalowane minimum:   * 8 sztuki dysków 3,5” SATA o pojemności minimum 8TB każdy   Wymagana możliwość instalacji minimum dysków M.2 zabezpieczonych sprzętowym RAID. Nie dopuszcza się rozwiązania, w którym dyski M.2 zajmują którykolwiek ze slotów PCIe.  Wymagany jest wewnętrzny slot na kartę Micro SD. |
| **Kontroler dyskowy** | Zainstalowany sprzętowy kontroler SAS 12Gb do obsługi min. 8 sztuk dysków wewnętrznych. Kontroler musi posiadać 2GB pamięci Flash. Kontroler musi obsługiwać poziomy RAID 0/1/10/5/50/6/60. |
| **Zasilacz** | Minimum dwa redundantne zasilacze o mocy minimum 750W z certyfikatem minimum Titanium. |
| **Interfejsy sieciowe** | Zainstalowana czteroportowa karta 1GB. Karta nie może zajmować żadnego ze slotów PCIe. |
| **Sloty I/O** | Serwer w momencie dostawy musi posiadać 3 sloty PCIe 4.0 z czego jeden x16. Serwer musi posiadać jeden slot OCP 3.0 na potrzeby instalacji karty sieciowej. |
| **Dodatkowe porty** | * z przodu obudowy: 1x USB 3.2, 1x USB 2.0 (z możliwością zarządzania serwerem), możliwość instalacji portu VGA * z tyłu obudowy: 3x USB 3.2, 1x VGA, 1x RJ-45 do zarządzania serwerem. Możliwość instalacji portu DB9. * wewnątrz obudowy: 1x USB 3.2   Wszystkie tylne porty USB, port RJ-45 służący do zarządzania, tylny port VGA, wewnętrzny port USB, wewnętrzny port na kartę Micro SD powinny być umieszczone na osobnej dedykowanej płytce I/O, którą łączy się bezpośrednio z płytą główną serwera. Możliwość instalacji dodatkowego redundantnego portu RJ45 służącego do zarządzania, w slocie OCP zamiast karty sieciowej. |
| **Chłodzenie** | Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1. |
| **Zarządzanie** | Wymagany wbudowany sprzętowy kontroler zdalnego zarządzania, który musi być umieszczony na osobnej dedykowanej płytce I/O (wspomnianej w sekcji Dodatkowe Porty). Płytka I/O musi posiadać swój własny min. 2 rdzeniowy procesor o taktowaniu min. 1.2GHz.   * Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna * Pozyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres IP karty zarządzającej, utylizacja CPU, utylizacja pamięci oraz komponentów I/O, lokalizacja * Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów. * Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń. * Wysyłanie określonych zdarzeń poprzez SMTP oraz SNMPv3 * Update systemowego firmware * Monitoring i możliwość ograniczenia poboru prądu * Zdalne włączanie/wyłączanie/restart * Zapis video zdalnych sesji * Podmontowanie lokalnych mediów z wykorzystaniem Java client * Przekierowanie konsoli szeregowej przez IPMI * Zrzut ekranu w momencie zawieszenia systemu * Możliwość przejęcia zdalnego ekranu * Możliwość zdalnej instalacji systemu operacyjnego * Alerty Syslog * Przekierowanie konsoli szeregowej przez SSH * Wyświetlanie danych aktualnych I historycznych dla użycia energii oraz temperatury serwera * Możliwość mapowania obrazów ISO z lokalnego dysku operatora * Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS * Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę * wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API * Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego. * Kontroler zarządzania musi posiadać 4Gb wewnętrznej pamięci (dopuszcza się zastosowanie karty Micro SD w celu uzyskania tej pojemności). Pamięć kontrolera zarządzania musi pełnić funkcję RDOC (Remote Disc on Card) oraz musi umożliwiać przechowywanie plików firmware. * Monitorowanie zmian sprzętowych w celu wykrycia nieoczekiwanych zmian. Po wykryciu zmiany zapis w logu serwera lub uniemożliwienie boot’u. * Możliwość synchronizacji konfiguracji i poziomów firmware pomiędzy serwerami. * Możliwość monitorowania i zarządzania grupą serwerów z poziomu kontrolera zarządzania pojedynczego serwera. Ilość serwerów możliwych do zarządzania – minimum 200.   Wraz z serwerem powinno zostać dostarczone dodatkowe oprogramowanie zarządzające umożliwiające:   * zarzadzanie infrastruktura serwerów i storage bez udziału dedykowanego agenta * przedstawianie graficznej reprezentacji zarządzanych urządzeń * możliwość skalowania do minimum 1000 urządzeń * obsługę szyfrowanej komunikacji z zarządzanymi urządzeniami, wsparcie dla NIST 800-131A oraz FIPS 140-2 * wsparcie dla certyfikatów SSL tzw. self-signed oraz zewnętrznych * udostępnianie szybkiego podgląd stanu środowiska * udostępnianie podsumowania stanu dla każdego urządzenia * tworzenie alertów przy zmianie stanu urządzenia * monitorowanie oraz tracking zużycia energii przez monitorowane urządzenie, możliwość ustalania granicy zużycia energii, * konsola zarzadzania oparta o HTML 5 * dostępność konsoli monitorującej na urządzeniach przenośnych ze wsparciem dla systemu Android oraz iOS, aplikacja musi umożliwiać włączenie wyłączenie oraz restart urządzenia, musi również mieć możliwość aktywowania diody lokacyjnej na urządzeniu, * automatyczne wykrywanie dołączanych systemów oraz szczegółowa inwentaryzacja * możliwość podnoszenia wersji oprogramowania dla komponentów zarządzanych serwerów w oparciu o repozytorium lokalne jak i zdalne dostępne na stronie producenta oferowanego rozwiązania * definiowanie polityk zgodności wersji firmware komponentów zarządzanych urządzań * definiowanie roli użytkowników oprogramowania * obsługa REST API oraz Windows PowerShell * obsługa SNMP, SYSLOG, Email Forwarding * autentykacja użytkowników: centralna (możliwość definiowania wymaganego poziomu skomplikowania danych autentykacyjnych) oraz integracja z MS AD oraz obsługa single sign on oraz SAML * obsługa tzw. Forward Secrecy w komunikacji z zarządzanymi urządzeniami * przedstawianie historycznych aktywności użytkowników * blokowanie możliwości podłączenia innego systemu zarzadzania do urządzeń zarządzanych * tworzenie dziennika zdarzeń ukończonych sukcesem lub bledem, oraz zdarzeń będących w trakcie. Możliwość definiowania filtrów wyświetlanych zdarzeń z dziennika. Możliwość eksportu dziennika zdarzeń do pliku csv * Obsługa NTP * przesyłanie alertów do konsoli firm trzecich * tworzenie wzorców konfiguracji zarządzanych urządzeń (definiowanie przez konsole albo kopiowanie konfiguracji z już zaimplementowanych urządzeń) * instalowanie systemów operacyjnych oraz wirtalizatorów Vmware i Hyper-V. Wymagana jest integracja konsoli zarządzania z konsolą wirtualizatora tak, aby zarządzanie środowiskiem sprzętowym mogło odbywać się z konsoli wirtualizatora. Wymaga się możliwości instalacji systemu na przynajmniej 20 nodach jednocześnie * możliwość automatycznego tworzenia zgłoszeń w centrum serwisowym producenta dla określonych zdarzeń wraz z przesyłem plików diagnostycznych,   Producent serwera ponadto powinien mieć w swojej ofercie narzędzia integrujące zarządzanie infrastrukturą z następującymi produktami:  VMware vCenter, Microsoft AdminCenter, Microsoft SystemCenter, RedHat CloudForms, Splunk. |
| **Funkcje zabezpieczeń** | Możliwość instalacji czujnika otwarcia obudowy zintegrowanego z modułem zarządzania serwerem, hasło włączania, hasło administratora, moduł RoT (umieszczony na dedykowanej płytce I/O wspomnianej w sekcji Dodatkowe porty) wspierający TPM2.0 oraz Platform Firmware Resiliency (PFR)., Możliwość zainstalowania przedniego panelu zamykanego na klucz. |
| **Urządzenia hot SWAP** | Dyski twarde, zasilacze, wentylatory. |
| **Diagnostyka** | Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID  Możliwość użycia aplikacji mobilnej na telefonie, do przeglądania awarii, konfiguracji i włączenia / wyłączenia serwera. |
| **Systemy operacyjne** | Wspierane systemy operacyjne:  Microsoft Windows Server 2019, 2022; Red Hat Enterprise Linux 8.6, 8.7, 9.0, 9.1, SUSE Linux Enterprise Server 15 SP4 oraz 15 Xen SP4; VMware vSphere (ESXi) 7.0 U3, ESXI 8.0; Ubuntu 22.04 LTS. |
| **Waga** | maximum: 38,8 kg |
| **Gwarancja** | 24 miesiące gwarancji producenta z czasem reakcji Next Business Day (Następny Dzień Roboczy). W przypadku braku funkcjonalności przewidywania awarii dla wszystkich komponentów wymienionych w punkcie Diagnostyka wymagane jest dostarczenie serwera nadmiarowego, mogącego zastąpić funkcjonalnie jak i wydajnościowo wymagane powyżej maszyny. Wszystkie komponenty serwera powinny być sygnowane i zoptymalizowane do użycia przez producenta serwera.  Serwis urządzeń musi być realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta zgodnie z systemem ISO 9001 lub równoważnym.  Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001 lub równoważnymi.  Serwer musi posiadać deklaracja CE - dokument należy dołączyć do oferty.  Możliwość wykupienia dodatkowego serwisu zapewniającego gwarantowany czas naprawy serwera w ciągu 6 godzin.  W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego |
| **Serwer RACK – TYP 2 – 2 szt.** | |
| **Obudowa** | Do instalacji w szafie RACK 19”, wysokość nie więcej niż 2U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych. Możliwość instalacji ramienia do zarządzania kablami. |
| **Procesor** | Architektura x86, maksymalny TDP dla procesora – maksymalnie 150W. Wymagana ilość rdzeni dla procesora – 16. Minimalna częstotliwość pracy procesora 2.0GHz. Minimalna ilość kanałów procesora – 8. Ilość kości pamięci na kanał – 2. Wynik wydajności procesora dla proponowanego serwera nie powinien być niższy niż 266 punkty base w teście SPECrate 2017 Integer, opublikowanym przez SPEC.org (www.spec.org) dla konfiguracji dwuprocesorowej. |
| **Liczba zainstalowanych procesorów** | 2 |
| **Płyta główna** | Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów wykonujących 64-bitowe instrukcje. |
| **Pamięć operacyjna** | Zainstalowane minimum 128GB pamięci RAM o częstotliwości 4800MHz. Pamięć zainstalowana w kościach mn. 32GB.  Minimum 32 sloty na pamięć. Możliwość rozbudowy do 8TB RAM. |
| **Zabezpieczenie pamięci** | Memory mirroring, ECC, SDDC, ADDDC |
| **Procesor Graficzny** | Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz. 1 port VGA na tylnym panelu. Możliwość zainstalowania drugiego portu VGA na przednim panelu serwera. |
| **Rozbudowa dysków** | W chwili dostawy serwer musi posiadać zainstalowane minimum:   * 8 sztuki dysków 3,5” SATA o pojemności minimum 8TB każdy   Wymagana możliwość instalacji minimum dysków M.2 zabezpieczonych sprzętowym RAID. Nie dopuszcza się rozwiązania, w którym dyski M.2 zajmują którykolwiek ze slotów PCIe.  Wymagany jest wewnętrzny slot na kartę Micro SD. |
| **Kontroler dyskowy** | Zainstalowany sprzętowy kontroler SAS 12Gb do obsługi min. 8 sztuk dysków wewnętrznych. Kontroler musi posiadać 2GB pamięci Flash. Kontroler musi obsługiwać poziomy RAID 0/1/10/5/50/6/60. |
| **Zasilacz** | Minimum dwa redundantne zasilacze o mocy minimum 750W z certyfikatem minimum Titanium. |
| **Interfejsy sieciowe** | Zainstalowana czteroportowa karta 1GB. Karta nie może zajmować żadnego ze slotów PCIe. |
| **Sloty I/O** | Serwer w momencie dostawy musi posiadać 3 sloty PCIe 4.0 z czego jeden x16. Serwer musi posiadać jeden slot OCP 3.0 na potrzeby instalacji karty sieciowej. |
| **Dodatkowe porty** | * z przodu obudowy: 1x USB 3.2, 1x USB 2.0 (z możliwością zarządzania serwerem), możliwość instalacji portu VGA * z tyłu obudowy: 3x USB 3.2, 1x VGA, 1x RJ-45 do zarządzania serwerem. Możliwość instalacji portu DB9. * wewnątrz obudowy: 1x USB 3.2   Wszystkie tylne porty USB, port RJ-45 służący do zarządzania, tylny port VGA, wewnętrzny port USB, wewnętrzny port na kartę Micro SD powinny być umieszczone na osobnej dedykowanej płytce I/O, którą łączy się bezpośrednio z płytą główną serwera. Możliwość instalacji dodatkowego redundantnego portu RJ45 służącego do zarządzania, w slocie OCP zamiast karty sieciowej. |
| **Chłodzenie** | Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1. |
| **Zarządzanie** | Wymagany wbudowany sprzętowy kontroler zdalnego zarządzania, który musi być umieszczony na osobnej dedykowanej płytce I/O (wspomnianej w sekcji Dodatkowe Porty). Płytka I/O musi posiadać swój własny min. 2 rdzeniowy procesor o taktowaniu min. 1.2GHz.   * Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna * Pozyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres IP karty zarządzającej, utylizacja CPU, utylizacja pamięci oraz komponentów I/O, lokalizacja * Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów. * Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń. * Wysyłanie określonych zdarzeń poprzez SMTP oraz SNMPv3 * Update systemowego firmware * Monitoring i możliwość ograniczenia poboru prądu * Zdalne włączanie/wyłączanie/restart * Zapis video zdalnych sesji * Podmontowanie lokalnych mediów z wykorzystaniem Java client * Przekierowanie konsoli szeregowej przez IPMI * Zrzut ekranu w momencie zawieszenia systemu * Możliwość przejęcia zdalnego ekranu * Możliwość zdalnej instalacji systemu operacyjnego * Alerty Syslog * Przekierowanie konsoli szeregowej przez SSH * Wyświetlanie danych aktualnych i historycznych dla użycia energii oraz temperatury serwera * Możliwość mapowania obrazów ISO z lokalnego dysku operatora * Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS * Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę * wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API * Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego. * Kontroler zarządzania musi posiadać 4Gb wewnętrznej pamięci (dopuszcza się zastosowanie karty Micro SD w celu uzyskania tej pojemności). Pamięć kontrolera zarządzania musi pełnić funkcję RDOC (Remote Disc on Card) oraz musi umożliwiać przechowywanie plików firmware. * Monitorowanie zmian sprzętowych w celu wykrycia nieoczekiwanych zmian. Po wykryciu zmiany zapis w logu serwera lub uniemożliwienie boot’u. * Możliwość synchronizacji konfiguracji i poziomów firmware pomiędzy serwerami. * Możliwość monitorowania i zarządzania grupą serwerów z poziomu kontrolera zarządzania pojedynczego serwera. Ilość serwerów możliwych do zarządzania – minimum 200.   Wraz z serwerem powinno zostać dostarczone dodatkowe oprogramowanie zarządzające umożliwiające:   * zarzadzanie infrastruktura serwerów i storage bez udziału dedykowanego agenta * przedstawianie graficznej reprezentacji zarządzanych urządzeń * możliwość skalowania do minimum 1000 urządzeń * obsługę szyfrowanej komunikacji z zarządzanymi urządzeniami, wsparcie dla NIST 800-131A oraz FIPS 140-2 * wsparcie dla certyfikatów SSL tzw. self-signed oraz zewnętrznych * udostępnianie szybkiego podgląd stanu środowiska * udostępnianie podsumowania stanu dla każdego urządzenia * tworzenie alertów przy zmianie stanu urządzenia * monitorowanie oraz tracking zużycia energii przez monitorowane urządzenie, możliwość ustalania granicy zużycia energii, * konsola zarzadzania oparta o HTML 5 * dostępność konsoli monitorującej na urządzeniach przenośnych ze wsparciem dla systemu Android oraz iOS, aplikacja musi umożliwiać włączenie wyłączenie oraz restart urządzenia, musi również mieć możliwość aktywowania diody lokacyjnej na urządzeniu, * automatyczne wykrywanie dołączanych systemów oraz szczegółowa inwentaryzacja * możliwość podnoszenia wersji oprogramowania dla komponentów zarządzanych serwerów w oparciu o repozytorium lokalne jak i zdalne dostępne na stronie producenta oferowanego rozwiązania * definiowanie polityk zgodności wersji firmware komponentów zarządzanych urządzań * definiowanie roli użytkowników oprogramowania * obsługa REST API oraz Windows PowerShell * obsługa SNMP, SYSLOG, Email Forwarding * autentykacja użytkowników: centralna (możliwość definiowania wymaganego poziomu skomplikowania danych autentykacyjnych) oraz integracja z MS AD oraz obsługa single sign on oraz SAML * obsługa tzw. Forward Secrecy w komunikacji z zarządzanymi urządzeniami * przedstawianie historycznych aktywności użytkowników * blokowanie możliwości podłączenia innego systemu zarzadzania do urządzeń zarządzanych * tworzenie dziennika zdarzeń ukończonych sukcesem lub bledem, oraz zdarzeń będących w trakcie. Możliwość definiowania filtrów wyświetlanych zdarzeń z dziennika. Możliwość eksportu dziennika zdarzeń do pliku csv * Obsługa NTP * przesyłanie alertów do konsoli firm trzecich * tworzenie wzorców konfiguracji zarządzanych urządzeń (definiowanie przez konsole albo kopiowanie konfiguracji z już zaimplementowanych urządzeń) * instalowanie systemów operacyjnych oraz wirtalizatorów Vmware i Hyper-V. Wymagana jest integracja konsoli zarządzania z konsolą wirtualizatora tak, aby zarządzanie środowiskiem sprzętowym mogło odbywać się z konsoli wirtualizatora. Wymaga się możliwości instalacji systemu na przynajmniej 20 nodach jednocześnie * możliwość automatycznego tworzenia zgłoszeń w centrum serwisowym producenta dla określonych zdarzeń wraz z przesyłem plików diagnostycznych,   Producent serwera ponadto powinien mieć w swojej ofercie narzędzia integrujące zarządzanie infrastrukturą z następującymi produktami:  VMware vCenter, Microsoft AdminCenter, Microsoft SystemCenter, RedHat CloudForms, Splunk. |
| **Funkcje zabezpieczeń** | Możliwość instalacji czujnika otwarcia obudowy zintegrowanego z modułem zarządzania serwerem, hasło włączania, hasło administratora, moduł RoT (umieszczony na dedykowanej płytce I/O wspomnianej w sekcji Dodatkowe porty) wspierający TPM2.0 oraz Platform Firmware Resiliency (PFR)., Możliwość zainstalowania przedniego panelu zamykanego na klucz. |
| **Urządzenia hot SWAP** | Dyski twarde, zasilacze, wentylatory. |
| **Diagnostyka** | Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID  Możliwość użycia aplikacji mobilnej na telefonie, do przeglądania awarii, konfiguracji i włączenia / wyłączenia serwera. |
| **Systemy operacyjne** | Wspierane systemy operacyjne:  Microsoft Windows Server 2019, 2022; Red Hat Enterprise Linux 8.6, 8.7, 9.0, 9.1, SUSE Linux Enterprise Server 15 SP4 oraz 15 Xen SP4; VMware vSphere (ESXi) 7.0 U3, ESXI 8.0; Ubuntu 22.04 LTS. |
| **Waga** | maximum: 38,8 kg |
| **Gwarancja** | 24 miesiące gwarancji producenta z czasem reakcji Next Business Day (Następny Dzień Roboczy). W przypadku braku funkcjonalności przewidywania awarii dla wszystkich komponentów wymienionych w punkcie Diagnostyka wymagane jest dostarczenie serwera nadmiarowego, mogącego zastąpić funkcjonalni jak i wydajnościowo wymagane powyżej maszyny. Wszystkie komponenty serwera powinny być sygnowane i zoptymalizowane do użycia przez producenta serwera.  Serwis urządzeń musi być realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta zgodnie z systemem ISO 9001 lub równoważnym.  Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001 lub równoważnymi.  Serwer musi posiadać deklaracja CE.  Możliwość wykupienia dodatkowego serwisu zapewniającego gwarantowany czas naprawy serwera w ciągu 6 godzin.  W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparcie technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego |
| **Urządzenia UPS dla dwóch jednostek – 1 komplet** | |
| Charakterystyka podstawowa | |
| **Technologia wykonania UPS** | Online podwójna konwersja |
| **Faza** | Jednofazowe |
| **Moc pozorna (VA)** | 3000 |
| **Moc rzeczywista (W)** | 2700 |
| **Kształt fali na wyjściu (praca na baterii)** | Czysta fala sinusoidalna |
| **Kompatybilność z zasilaczami z aktywnym PFC** | Wymagana |
| **Ochrona przed przeciążeniem** | Wymagana (min. bezpiecznik i wewnętrzny ogranicznik prądu) |
| **Filtr EMI/RFI** | Wymagany |
| **Układ przeciwprzepięciowy (Dżule)** | Wymagany, min. 388 |
| Charakterystyka wejścia/wyjścia | |
| **Nominalne napięcie wejściowe (V)** | 230 ± 10% |
| **Obsługiwany zakres napięcia wejściowego (V)** | 190 ~ 300 |
| **Częstotliwość wejściowa(Hz)** | 50 ± 10,  60 ± 10 |
| **Wykrywanie częstotliwości wejściowej** | Wymagane automatyczne |
| **Napięcie przy pracy na baterii (V)** | 208 +/-1% ; 220 +/-1%; 230 +/-1%; 240 +/-1% |
| **Częstotliwość przy pracy baterii (Hz)** | 50 ± 0.5%,  60 ± 0.5% |
| Charakterystyka gniazd | |
| **Rodzaj złącza wejściowego** | IEC C20 |
| **Gniazda** | IEC C19 x 2 / IEC C13 x 8 |
| Charakterystyka baterii | |
| **Typowy czas przełączenia na baterie (ms)** | 0 ms |
| **Bateria** | Wymagana praca z zewnętrznymi modułami baterii |
| **Ilość obsługiwanych modułów baterii** | Min. 3 |
| Zarządzanie | |
| **Sygnalizacja** | Wymagane alarmy dźwiękowe oraz wyświetlacz LCD |
| **Alarmy dźwiękowe** | Tryb baterii, Niski poziom baterii, Przeciążenie, Przeładowanie, Przegrzanie, Usterka UPS, Wymień baterię |
| **Port komunikacyjny USB** | Wymagany |
| **Port wyłącznika awaryjnego EPO** | Wymagany |
| **Dołączone oprogramowanie do zarządzania** | Wymagane, obsługa platform Windows, Linux, Vmware |
| **Zarządzanie przez sieć** | Wymagana możliwość rozbudowy o zarządzanie HTTP/SNMP, np. poprzez zamontowanie karty zarządzającej |
| Cechy fizyczne | |
| **Obudowa** | Wymagana możliwość instalacji w szafie RACK lub ustawienia jako Tower |
| **Konstrukcja obudowy** | Metalowa |
| **Szyny/uchwyty rack** | Wymagane |
| **Waga** | maksimum 26.7 kg (bez modułów bateryjnych) |
| Dane środowiskowe | |
| **Temperatura robocza (°C)** | 0 ~ 40 |
| **Względna wilgotność robocza (bez kondensacji) (%)** | 20 ~ 90 |
| Certyfikaty | |
| **Wymagane certyfikaty** | CE, EAC |
| Praca na baterii | |
| **Czas podtrzymania przy 50% obciążenia** | Min. 12 minut |
| **Czas podtrzymania przy 100% obciążenia** | Min. 4 minuty |
| **Gwarancja** | 24 miesiące gwarancji producenta |