Załącznik nr 1 do Zapytania Ofertowego

Opis Przedmiotu Zamówienia

Dostawa oprogramowania i urządzeń sieciowych

Katowice, grudzień 2025

# Informacje wstępne

Zamówienie niniejsze jest prowadzone w ramach projektu „Rozwój usług cyfrowych i poprawa cyberbezpieczeństwa w Szpitalu Zakonu Bonifratrów pw. Aniołów Stróżów w Katowicach. Nr wniosku KPOD.07.03-IP.10-0131/25” finansowanego ze środków Krajowego Planu Odbudowy i Zwiększania Odporności, Priorytet Efektywność, dostępność i jakość systemu ochrony zdrowia - część grantowa, Działanie D1.1.2. Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia, nr naboru: KPOD.07.03-IP.10-001/25

# Wymagania ogólne dla urządzeń i oprogramowania sieciowego.

* całość sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów;
* całość sprzętu musi być nowa (wyprodukowana nie wcześniej niż 6 miesięcy przed dostawą), nie używana wcześniej;
* Wykonawca zobowiązany jest zaoferować produkty (sprzęt i oprogramowanie), które w dniu dostawy będą w pełni zgodne z wymaganiami dostępności określonymi w Ustawie z dnia 26 kwietnia 2024 r. o zapewnianiu spełniania wymagań dostępności niektórych produktów i usług (Dz. U. z 2024 r. poz. 731)..
* Interfejs użytkownika oferowanego produktu musi spełniać co najmniej następujące wymagania, zgodne z Ustawą z dnia 26 kwietnia 2024 r.:
  + Informacje przekazywane za pomocą koloru muszą być również dostępne bez niego (np. za pomocą kształtu, etykiety tekstowej).
  + Interfejs musi zapewniać możliwość obsługi przy użyciu samej klawiatury.
  + Musi być zapewniona kompatybilność z najpopularniejszymi technologiami wspomagającymi (czytnikami ekranu) dla systemu operacyjnego, na którym produkt jest instalowany.
  + Instrukcja obsługi musi być dostarczona w formacie cyfrowym, umożliwiającym jej odczytanie przez oprogramowanie wspomagające (np. w formacie PDF z warstwą tekstową lub w formacie HTML).

# Wymagania gwarancyjne.

**Sprzęt**

* o ile wymagania szczegółowe nie specyfikują inaczej, na dostarczany sprzęt musi być udzielona gwarancja; serwis gwarancyjny świadczony ma być w miejscu instalacji sprzętu; czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć jednego dnia roboczego;
* Gwarantowany czas naprawy nie może być dłuższy niż 10 dni roboczych. W przypadku sprzętu, dla którego jest wymagany dłuższy czas na naprawę sprzętu, Zamawiający wymaga podstawienia na czas naprawy Sprzętu o nie gorszych parametrach funkcjonalnych. Naprawa w takim przypadku nie może przekroczyć 31 dni roboczych od momentu zgłoszenia usterki;
* Zamawiający otrzyma dostęp do pomocy technicznej (telefon, e-mail lub WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Wnioskodawcy;

**Oprogramowanie**

* oprogramowanie powinno posiadać min. 36-miesięczną gwarancję obejmującą swoim zakresem poprawność działania w zakresie wdrożonych funkcjonalności wg stanu na dzień podpisania stosownego protokołu odbioru (chyba że zapisy szczegółowe stanowią inaczej);

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

# Miejsce instalacji sprzętu i oprogramowania/systemu.

Dostarczony sprzęt i oprogramowanie powinny zostać zamontowane, zainstalowane i skonfigurowane zgodnie z wymaganiami opisanymi w dalszej części dokumentu, w miejscach wskazanych przez Zamawiającego, tj.:

1. Macierz do backupu (1 szt) – Data Center ul. Borowska 283B we Wrocławiu lub ul. Na Ostatnim Groszu 112 we Wrocławiu,
2. Firewall (UTM) (2 szt) - siedziba Szpitala Zakonu Bonifratrów pw. Aniołów Stróżów w Katowicach, przy ul. ks. Leopolda Markiefki 87,
3. System zbierania i analizy logów (1 szt.) – infrastruktura wirtualna Zamawiającego,
4. Przełącznik sieci LAN - CORE (2 szt.) - Data Center ul. Borowska 283B we Wrocławiu lub ul. Na Ostatnim Groszu 112 we Wrocławiu,
5. System do zarządzania i monitorowania dostępu do sieci (NAC) – infrastruktura wirtualna Zamawiającego.
6. Pozostałe oprogramowanie – infrastruktura wirtualna Zamawiającego.

# Wymagania w zakresie dostawy i instalacji

**Montaż i fizyczne uruchomienie systemu**

Zamawiający wymaga, aby Wykonawca zainstalował całości dostarczonego rozwiązania w pomieszczeniu serwerowni, jak i innych wskazanych miejscach co najmniej w zakresie:

1. Wniesienie, ustawienie i fizyczny montaż wszystkich dostarczonych urządzeń w szafach rack w pomieszczeniach (miejscach) wskazanych przez Zamawiającego z uwzględnieniem wszystkich lokalizacji.
2. Rozbudowa istniejących zasobów sprzętowych.
3. Urządzenia, które nie są montowane w szafach teleinformatycznych, powinny zostać zamontowane w miejscach wskazanych przez Zamawiającego, oraz skonfigurowane i dołączone do infrastruktury Zamawiającego.
4. Usunięcie opakowań i innych zbędnych pozostałości po procesie instalacji urządzeń.
5. Podłączenie całości rozwiązania do infrastruktury Zamawiającego.
6. Wykonanie procedury aktualizacji firmware dostarczonych elementów do najnowszej wersji oferowanej przez producenta sprzętu.
7. Dla urządzeń modularnych wymagany jest montaż i instalacja wszystkich podzespołów.
8. Wykonanie połączeń kablowych pomiędzy dostarczonymi urządzeniami w celu zapewnienia komunikacji – Wykonawca musi zapewnić niezbędne okablowanie (np.: patchordy miedziane min. kat. 6 UTP lub światłowodowe uwzględniające typ i model interfejsu w urządzeniu sieciowym).
9. Wykonawca musi zapewnić niezbędne okablowanie potrzebne do podłączenia urządzeń aktywnych do sieci elektrycznej (np.: listwy zasilające).
10. Wykonawca musi zapewnić niezbędne wkładki dla dostarczonych urządzeń np.: SFP, SFP+ między innymi celem:
    1. Stworzenia połączeń sieci LAN pomiędzy przełącznikami.
    2. Podłączenia urządzeń serwerowo-macierzowych do przełączników sieci LAN.
    3. Połączenia powinny być zrealizowane z zachowaniem redundancji i agregacji połączeń na poziomie co najmniej n+1.
    4. Połączenia musza wykorzystywać dostępną, największą przepustowość portu pomiędzy łączonymi urządzeniami.

**Instalacja i konfiguracja oprogramowania**

Wykonawca zobowiązany jest wykonać instalację dostarczonego oprogramowania na serwerach wskazanych przez Zamawiającego.

1. Wykonawca zobowiązany jest do wykreowania konta administratora oraz użytkowników zgodnie z listą przekazaną przez Zamawiającego.
2. Wykonawca zobowiązany jest do przeprowadzenia wstępnej konfiguracji oprogramowania pozwalającej na jego bezpieczne uruchomienie.
3. Systemy należy skonfigurować według zaproponowanych przez Wykonawcę wytycznych z uwzględnieniem wymagań Zamawiającego. Zakres konfiguracji musi zostać zaakceptowany i ustalony z administratorem.
4. Po przeprowadzanej aktualizacji wymagane jest przeszkolenie administratora z całości systemu ze szczególnym uwzględnieniem nowych funkcjonalności.

# Zakres zamówienia

Zamówienie niniejsze podzielone jest na 2 pakiety (części) zgodnie z poniższym zestawieniem

Część 1.

1. System do backupu danych MS Office 365
2. Oprogramowanie do backupu
3. Oprogramowanie do zarzadzania IT

Część 2

1. Macierz do backupu
2. Firewall (UTM)
3. System zbierania i analizy logów
4. Przełącznik sieci LAN -CORE
5. Zakup i wdrożenie systemu do zarządzania i monitorowania dostępu do sieci (NAC)

## Zestawienie zakresu dostaw i usług – część 1

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Lp.** | **Nazwa środka trwałego lub wartości niematerialnych i prawnych itp.** | **Wymagana minimalna długość gwarancji (m-ce)** | **Wymagana długość obowiązywania licencji na oprogramowanie (m-ce)** | **Typ/Rodzaj gwarancji** | **Ilość** | **Jednostka miary** |
|  | System do backupu danych MS Office 365 | 36 | 36 | Producenta | 50 | licencja |
|  | Oprogramowanie do backupu | 36 | 36 | Producenta | 1 | Licencja |
|  | Oprogramowanie do zarzadzania IT | 36 | 36 | producenta | 1 | Licencja |

## Opis przedmiotu zamówienia

### System do backupu danych MS Office 365

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **WYMAGANIA OGÓLNE DOTYCZĄCE ZAKRESU OCHRONY**  Oferowane rozwiązanie musi zapewniać kompletną i zintegrowaną ochronę danych w ramach jednej konsoli zarządzającej dla niżej wymienionych usług i środowisk.   1. **Ochrona usług Microsoft 365:** Wymagane jest zapewnienie natywnej ochrony dla:    1. **Exchange Online:** skrzynki pocztowe użytkowników, archiwa online, foldery publiczne.    2. **SharePoint Online:** kolekcje witryn, witryny, listy, biblioteki dokumentów wraz z metadanymi i uprawnieniami.    3. **OneDrive for Business:** konta użytkowników, pliki i foldery wraz z uprawnieniami.    4. **Microsoft Teams:** zespoły, kanały (w tym kanały **prywatne i udostępnione**), wpisy na kanałach, pliki, zakładki i ustawienia zespołów. 2. **Ochrona Microsoft Entra ID:** System musi posiadać dedykowaną funkcjonalność tworzenia kopii zapasowych i granularnego odzyskiwania obiektów oraz atrybutów usługi Microsoft Entra ID (dawniej Azure Active Directory). 3. **Ochrona środowisk hybrydowych:** System musi umożliwiać ochronę lokalnych wdrożeń **Microsoft Exchange Server** oraz **Microsoft SharePoint Server** z tej samej konsoli, która służy do zarządzania ochroną usług Microsoft 365.   **WYMAGANIA ARCHITEKTONICZNE I SKALOWALNOŚĆ**   1. **Architektura rozproszona:** Rozwiązanie musi posiadać architekturę komponentową, umożliwiającą instalację poszczególnych ról (serwer zarządzający, komponenty przetwarzające dane, baza danych) na oddzielnych serwerach wirtualnych lub fizycznych. 2. **Pula serwerów proxy:** System musi być wyposażony w mechanizm grupowania komponentów przetwarzających dane (serwerów proxy) w pule zasobów. Pula musi zapewniać automatyczne równoważenie obciążenia (load balancing) oraz wysoką dostępność (high availability) na wypadek awarii pojedynczego serwera proxy w puli. 3. **Wsparcie dla systemu Linux:** Wymagane jest, aby komponenty przetwarzające dane (serwery proxy) mogły być instalowane na serwerach z systemem operacyjnym Linux. 4. **Scentralizowana baza danych i pamięć podręczna:** Architektura systemu musi wykorzystywać scentralizowaną bazę danych opartą na silniku **PostgreSQL lub równoważnym**. Baza ta musi pełnić jednocześnie rolę bazy konfiguracyjnej oraz trwałej pamięci podręcznej (persistent cache) dla metadanych z repozytoriów zlokalizowanych w obiektowej pamięci masowej (object storage). Mechanizm ten musi minimalizować liczbę zapytań do chmury i przyspieszać operacje przeglądania kopii zapasowych.   **WYMAGANIA DOTYCZĄCE MAGAZYNU DANYCH**   1. **Elastyczność wyboru magazynu danych:** Rozwiązanie musi umożliwiać przechowywanie kopii zapasowych w co najmniej dwóch następujących typach lokalizacji:    1. **Lokalna pamięć masowa:** serwery plików z udostępnionymi zasobami sieciowymi (SMB).    2. **Chmurowa pamięć obiektowa (Cloud Object Storage):** wymagane jest natywne wsparcie dla platform zgodnych z API S3 oraz dla Microsoft Azure Blob. 2. **Niezmienność (Immutability) kopii zapasowych:** System musi zapewniać ochronę kopii zapasowych przed modyfikacją lub usunięciem (np. w wyniku ataku ransomware) poprzez natywną integrację z mechanizmami blokady obiektów. Wymagane jest wsparcie minimum dla:    1. **Amazon S3 Object Lock**.    2. Microsoft Azure Blob Immutability. 3. Funkcja niezmienności musi być dostępna zarówno dla podstawowych kopii zapasowych, jak i dla ich dodatkowych kopii (backup copies). 4. **Polityki retencji:** Okres przechowywania kopii zapasowych (retencja) musi być definiowany na poziomie konfiguracji magazynu danych (repozytorium), a nie na poziomie pojedynczego zadania backupu.   **WYMAGANIA FUNKCJONALNE: ODZYSKIWANIE DANYCH**   1. **Granularność odzyskiwania:** System musi zapewniać możliwość odzyskiwania pojedynczych elementów (np. jeden e-mail, plik, wpis na kanale Teams, pojedynczy atrybut obiektu Entra ID) bez konieczności odtwarzania całych kontenerów danych (np. całej skrzynki pocztowej czy witryny SharePoint). 2. **Elastyczność lokalizacji docelowej:** Dla każdego elementu z kopii zapasowej musi istnieć możliwość jego odzyskania do:    1. Oryginalnej lokalizacji.    2. Alternatywnej lokalizacji (np. do innego użytkownika, folderu, witryny).    3. Lokalnego systemu plików (np. eksport do pliku.PST,.MSG lub w formacie natywnym).    4. Wysłania jako załącznik wiadomości e-mail. 3. **Odzyskiwanie masowe:** System musi wspierać masowe odzyskiwanie danych dla wielu użytkowników, witryn lub kont OneDrive w ramach jednej operacji. 4. **Scenariusze odzyskiwania:** Oferent musi potwierdzić w ofercie realizację wszystkich scenariuszy odzyskiwania danych wyszczególnionych w poniższej tabeli.  |  |  |  | | --- | --- | --- | | **Usługa** | **Obiekt** | **Wymagana Akcja Odzyskiwania** | | Exchange Online | Cała skrzynka pocztowa | Przywrócenie do oryginalnej / innej skrzynki / on-premises | | Exchange Online | Pojedynczy e-mail/element | Przywrócenie do oryginalnego / innego folderu | | Exchange Online | Pojedynczy e-mail/element | Zapis jako plik.msg na dysku lokalnym | | Exchange Online | Skrzynka pocztowa/folder | Eksport do pliku.pst na dysku lokalnym | | SharePoint Online | Cała witryna (Site) | Przywrócenie do oryginalnej / innej lokalizacji / on-premises | | SharePoint Online | Lista / Biblioteka | Przywrócenie do oryginalnej / innej witryny | | SharePoint Online | Pojedynczy dokument/element | Przywrócenie do oryginalnej / innej biblioteki | | SharePoint Online | Pojedynczy dokument/element | Przywrócenie wyłącznie uprawnień do obiektu | | OneDrive for Business | Całe konto użytkownika | Przywrócenie do oryginalnego / innego konta | | OneDrive for Business | Plik / Folder | Przywrócenie do oryginalnego / innego folderu | | Microsoft Teams | Cały zespół (Team) | Przywrócenie do oryginalnej lokalizacji | | Microsoft Teams | Kanał (w tym prywatny) | Przywrócenie do oryginalnej lokalizacji | | Microsoft Teams | Wpis na kanale (Post) | Przywrócenie do oryginalnej lokalizacji lub eksport do pliku | | Entra ID | Użytkownik / Grupa | Przywrócenie obiektu wraz z atrybutami | | Entra ID | Atrybuty obiektu | Porównanie z kopią zapasową i przywrócenie wybranych atrybutów |   **WYMAGANIA DOTYCZĄCE BEZPIECZEŃSTWA I ZGODNOŚCI**   1. **Uwierzytelnianie i autoryzacja:** Dostęp do konsoli zarządzającej musi być zabezpieczony mechanizmem uwierzytelniania wieloskładnikowego (MFA). System musi również oferować kontrolę dostępu opartą na rolach (RBAC) w celu delegowania uprawnień. 2. **Szyfrowanie danych:** Dane w kopiach zapasowych muszą być szyfrowane zarówno podczas przesyłania (in-transit), jak i w miejscu ich przechowywania (at-rest) z wykorzystaniem algorytmu AES-256. 3. **Portal samoobsługowy:** Rozwiązanie musi zawierać portal internetowy, który umożliwia delegowanie uprawnień do odzyskiwania danych użytkownikom końcowym lub pracownikom działu wsparcia (helpdesk) bez konieczności udzielania im dostępu do głównej konsoli administracyjnej. 4. **Wyszukiwanie (eDiscovery):** System musi oferować zaawansowane funkcje wyszukiwania w treści kopii zapasowych z wykorzystaniem złożonych kryteriów (np. data, nadawca, słowa kluczowe) w celu wsparcia procesów audytowych i dochodzeniowych.   **WYMAGANIA DOTYCZĄCE ZARZĄDZANIA I AUTOMATYZACJI**   1. **RESTful API:** System musi udostępniać w pełni funkcjonalne i publicznie udokumentowane RESTful API, pozwalające na programistyczną kontrolę nad wszystkimi aspektami rozwiązania, w tym zarządzaniem zadaniami, repozytoriami i operacjami odzyskiwania. Autoryzacja do API musi być oparta o standard OAuth 2.0. 2. **Moduł PowerShell:** Równolegle do REST API, rozwiązanie musi dostarczać kompletny moduł PowerShell, oferujący funkcjonalność co najmniej równoważną z możliwościami konsoli graficznej i REST API.   **WYMAGANIA NIEFUNKCJONALNE**   1. **Model licencjonowania:** Licencjonowanie musi być oparte na liczbie chronionych użytkowników Microsoft 365. Licencja musi obejmować wszystkie komponenty i funkcjonalności bez dodatkowych kosztów zależnych od ilości przetwarzanych danych lub liczby komponentów infrastruktury (np. serwerów proxy). 2. **Wsparcie techniczne:** Wykonawca musi zapewnić wsparcie techniczne producenta oferowanego oprogramowania w trybie 24x7x365 dla zgłoszeń krytycznych. 3. Wymagane jest dostarczenie licencji dla 50 użytkowników na okres równy okresowi udzielonej gwarancji. |

### Oprogramowanie do backupu

|  |
| --- |
| **Wymagania ogólne**   * Zamawiający wymaga dostawy oprogramowania objętego licencją wieczystą z okresem wsparcia równym okresowi udzielonej gwarancji. * Minimalna ilość licencji musi obejmować min. 50 instancji (obciążeń/VUL). * Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5, 6.7, 7.0, 8.0 oraz Microsoft Hyper-V 2008R2SP1, 2012, 2012 R2, 2016, 2019, 2022 i 2025. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej. * Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami. * Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manager, klastrami hostów oraz pojedynczymi hostami. * Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.   **Całkowite koszty posiadania**   * Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej * Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków * Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-incremental) * Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji * Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu. * Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych. * Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania * Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota. * Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time) * Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji * Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji * Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania * Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX) * Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.   **Wymagania RPO**   * Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej * Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych. * Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych * Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora * Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware. * Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn * Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) * Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC. * Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC. * Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS. * Repozytoria oparte o XFS muszą pozwalać na niezmienność danych przez określoną ilość czasu (tzw Immutability) * Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji. * Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik * Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding) * Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)   **Wymagania RTO**   * Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych. * Dodatkowo dla środowiska vSphere i Hyper-V powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) * Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami * Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere * Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków * Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2. * Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików * Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V. * Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z następujących systemów plików: * Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs * BSD: UFS, UFS2 * Solaris: ZFS, UFS * Mac: HFS, HFS+ * Windows: NTFS, FAT, FAT32, ReFS * Novell OES: NSS * Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces. * Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej. * Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł. * Oprogramowanie musi wspierać granularne odtwarzanie dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA oraz elementów AD Sites. * Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"), * Oprogramowanie musi wspierać przywracanie danych Exchange do oryginalnego środowiska * Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowszych * Oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska * Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowszych * Oprogramowanie musi wspierać odtworzenia elementów, witryn, uprawnień dla witryn Sharepoint. * Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux. * Oprogramowanie musi pozwalać na zaprezentowanie oraz migrację online baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego * Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN   **Ograniczenie ryzyka**   * Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. * Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem * Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere * Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32. * Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.   **Monitoring**   * System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich * System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 5.5, 6.0, 6.5, 6.7, 7.0, 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie * System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016, 2019, 2022 oraz 2025 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. * System musi mieć status „VMware Ready” i być przetestowany i certyfikowany przez VMware * System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter * System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn * System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel * System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk * System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora * System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów * System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard) * System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna * System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego * System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta * System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych. * System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu. * System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware * System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji 9.x i 10.x   **Raportowanie**   * System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na VMware ESX/ESXi 5.5, 6.0, 6.5, 6.7, 7.0, 8.0, vCenter Server 5.x, 6.x oraz 7.x jak również Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016, 2019, 2022 oraz 2025 * System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów. * System musi być certyfikowany przez VMware i posiadać status „VMware Ready” * System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V * System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF * System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc * System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach * System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów * System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych * System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych * System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury * System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta * System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych. * System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’. * System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware * System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots) * System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie |

### Oprogramowanie do zarzadzania IT

|  |
| --- |
| Wymagania podstawowe:   * 1. Licencja wieczysta na korzystanie z oprogramowania, z okresem 36 miesięcy aktualizacji oprogramowania do najnowszej wersji oraz usługą wsparcia i pomocy technicznej.   2. System musi być fabrycznie nowy, pochodzić z legalnego kanału dystrybucji, a dostarczone licencje muszą być przeznaczone na rynek polski/europejski.   3. Licencja na nieograniczoną liczbę monitorowanych urządzeń sieciowych oraz 1000 stacji roboczych.   4. Oprogramowanie oraz pomoc techniczna (telefoniczna i mailowa) muszą być dostępne w języku polskim.   5. Oprogramowanie można zainstalować na następujących systemach operacyjnych:   - dla serwera zarządzającego: Windows Server 2012, 2012R2, 2016, 2019, 2022;  - dla konsoli zarządzającej: Windows Server 2012, 2012R2, 2016, 2019, 2022, Windows 10, 11;  - dla agenta: Windows 7, 8, 10, 11, Windows Serwer 2012, 2012R2, 2016, 2019, 2022;  Wymagania ogólne:   1. Modułowa budowa oprogramowania obejmująca: serwer zarządzający, konsolę zarządzającą oraz agentów, przy czym w ramach licencji możliwa jest instalacja dowolnej liczby konsoli zarządzających. 2. Moduły umożliwiają 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. 3. Instalator zabezpieczony jest aktualnym podpisem cyfrowym, który musi zostać zweryfikowany przez zaufany urząd certyfikacji (CA). 4. Komunikacja pomiędzy konsolami, agentami oraz serwerem odbywa się z wykorzystaniem protokołu TLS w wersji co najmniej 1.2. 5. Oprogramowanie od produkcyjnego uruchomienia nie wymaga zakupu dodatkowych licencji. M.in.: Zarówno serwer zarządzający, jak i agent, do działania wykorzystują bezpłatny silnik bazy danych open-source z publicznie dostępnym kodem źródłowym. 6. Integracja z usługą katalogową Active Directory, co umożliwia automatyczne pobieranie użytkowników, grup i struktury organizacyjnej. 7. Dostęp do konfiguracji agenta zabezpieczony jest hasłem - nawet użytkownik z prawami administratora stacji roboczej nie może ingerować w działanie agenta ani go usunąć bez podania hasła. 8. Globalna wyszukiwarka w konsoli zarządzającej umożliwia znalezienie dowolnego obiektu – np. zasobów, użytkowników czy urządzeń. 9. Administratorzy mogą mieć przydzielane różne poziomy dostępu i uprawnień do funkcji programu, użytkowników, a także grup urządzeń; główny Administrator zarządza prawami konfiguracyjnymi dla innych kont administracyjnych. 10. Wszelkie działania Administratorów podlegają rejestrowaniu w systemie. 11. Rejestrowane aktywności administratorów mogą być automatycznie kierowane do zewnętrznego kolektora Syslog. 12. Proces uwierzytelniania administracyjnych logowań do konsoli obejmuje mechanizmy weryfikacji dwuskładnikowej (MFA). 13. Synchronizacja kont użytkowników, w tym administratorów, odbywa się przez szyfrowane połączenie LDAPS z Active Directory, jednak możliwe jest także tworzenie lokalnych kont (z awatarami) w przypadku braku AD; liczba kont nie jest ograniczona ani licencjonowana. 14. Dane dotyczące aktywności pracownika (polityka internetowa, historia korzystania z aplikacji, dostęp do zewnętrznych nośników itp.) są odseparowane od danych technicznych stanowiska pracy, co umożliwia usuwanie danych pojedynczego użytkownika bez ingerencji w dane stacji roboczej. 15. System pozwala na kontrolowanie dostępu do danych osobowych oraz monitoringu przez wybranych Administratorów i przypisywanie kontom administracyjnym różnych uprawnień. 16. Rozbudowany system raportowania obejmuje nie mniej niż 130 raportów predefiniowanych oraz opcje tworzenia własnych raportów z pełną możliwością ich personalizacji. 17. Oprogramowanie dysponuje możliwością integracji z fizyczną bramką GSM.   Wymagane moduły funkcjonalne:  Moduł: Monitorowanie Sieci i Infrastruktury  Monitorowanie Infrastruktury (Bezagentowo) powinno zapewniać wsparcie dla minimum takich urządzeń jak serwery Windows, Linux, Mac, a także routery, przełączniki, urządzenia VoIP oraz firewalle, obejmując:   1. Skanowanie ping oraz arp-ping służące do wykrywania urządzeń w sieci. 2. Odczytywanie informacji z Active Directory, wraz z informacją o przynależności do jednostek organizacyjnych (OU), w celu identyfikacji urządzeń. 3. Graficzne mapy sieci wyświetlające stany urządzeń za pomocą ikon przypisanych do poszczególnych urządzeń. 4. Tworzenie spersonalizowanych map urządzeń przez wykorzystanie zaimportowanych obrazów, takich jak schemat rozmieszczenia pomieszczeń w budynku jako tła wizualizacji. 5. Zarówno ręczne, jak i automatyczne odwzorowanie połączeń między przełącznikami a urządzeniami, gdzie widoczne są linie oraz informacja, do którego portu przełącznika podłączono dane urządzenie. 6. Monitorowanie czasu odpowiedzi i procentu utraconych pakietów dla serwisów TCP/IP, HTTP, POP3, SMTP, FTP oraz innych, z możliwością definiowania własnych serwisów. 7. Testowanie serwerów pocztowych poprzez monitorowanie czasu logowania do serwisu odbierającego pocztę oraz czasu wysyłania wiadomości, informowanie o niedziałającym serwerze oraz wykonywanie operacji testowych. 8. Kontrolę serwisów WWW i monitorowanie określonych adresów URL. 9. Śledzenie czasu ładowania stron internetowych, wykrywanie zmian treści oraz monitorowanie statusu HTTPS. 10. Szyfrowanie SSL/TLS zastosowane w powiadomieniach e-mail. 11. Zarządzanie i monitorowanie urządzeń SNMP obsługujących wersje SNMP v1/2/3, zapewniających szyfrowanie oraz autoryzację – w tym przełączniki, routery, drukarki sieciowe, urządzenia VoIP – wraz z obsługą wartości po nazwach zmiennych oraz OID. 12. Ewidencjonowanie danych z odebranych komunikatów syslog oraz pułapek SNMP. 13. Weryfikację routerów i przełączników poprzez monitorowanie: zmian stanu interfejsów, natężenia ruchu, liczby podłączonych stacji roboczych oraz ruchu generowanego przez urządzenia podłączone do portów. 14. Monitorowanie serwisów Windows, które obejmuje generowanie alarmów, gdy wybrany serwis przestaje działać, jak również umożliwienie jego uruchomienia, zatrzymania lub restartu. 15. Prezentowanie statystyk przy każdym urządzeniu na mapie, takich jak czas odpowiedzi, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP i ewentualne ostrzeżenie o zdarzeniu. 16. Pozyskiwanie informacji o stanie maszyn wirtualnych VMware (działa, nie działa, wstrzymano). 17. Wysyłanie poleceń zarządzających do maszyn wirtualnych VMware umożliwiające ich uruchamianie, wstrzymywanie lub wyłączanie zasilania. 18. Kontrolę wydajności systemów Windows, tj. obciążenia CPU, pamięci, zajętości dysków oraz transferu sieciowego.   Program powinien automatycznie wykrywać w sieci urządzenia, takie jak stacje robocze, serwery, drukarki oraz urządzenia sieciowe – routery i przełączniki. Administrator może nakładać na wykryte urządzenia liczniki wydajności WMI oraz SNMP według przygotowanych szablonów i definiować alarmy bazujące na różnych typach zdarzeń obecnych w systemie. Do akcji wywoływanych w odpowiedzi na alarm można zaliczyć: wysłanie komunikatu pulpitowego, e-mail, SMS, wiadomości przez Microsoft Teams (z użyciem webhook i workflow), wiadomości przez Slack, uruchomienie programu, pułapkę SNMP, pakiet Wake-On-LAN, zatrzymanie lub restart wybranej usługi Windows, a także wyłączenie lub restart komputera.  Administrator samodzielnie wskazuje zdarzenia z dostępnej listy, które mogą inicjować alarmy oraz wybiera dowolną liczbę akcji do realizacji po wykryciu danego zdarzenia – wszystko w logice ciągu przyczynowo-skutkowego. Wykonywanie tych akcji można ustawić: automatycznie zaraz po wykryciu zdarzenia, z opóźnieniem, na zakończenie zdarzenia lub zdefiniować ich cykliczność. Możliwe jest przypisanie ograniczenia czasowego wybranym akcjom, np. wyłączenie ich w określonych godzinach.  Zdefiniowane alarmy mogą służyć do priorytetyzacji urządzeń, umożliwiając ich grupowanie według ważności i typu. Oprogramowanie obsługuje również zintegrowane alarmowanie przez skrzynki e-mail skonfigurowane z autoryzacją OAuth 2.0.  Moduł: Inwentaryzacja Sprzętu i Oprogramowania  Oprogramowanie automatycznie musi:   1. Gromadzić informacje o sprzęcie i oprogramowaniu na stacjach roboczych, 2. Prezentować szczegóły sprzętu, takie jak model, procesor, pamięć, płyta główna, napędy i karty, 3. Umożliwiać odczyt parametrów S.M.A.R.T. dysków twardych, SSD oraz NVME, 4. Przedstawiać zestawienie posiadanych konfiguracji sprzętowych, dostępnego miejsca na dyskach oraz średniego wykorzystania pamięci, 5. Informować o zainstalowanych aplikacjach i aktualizacjach Windows, pozwalając na audyt i weryfikację użytkowania licencji, 6. Zbierać dane o wszystkich zmianach dokonanych na wybranej stacji roboczej, takich jak instalacje i deinstalacje aplikacji czy zmiany adresu IP, 7. Posiadać możliwość wysyłania powiadomień (np. e-mail) w przypadku instalacji programu lub zmiany konfiguracji sprzętowej, 8. Umożliwiać odczytanie numerów seryjnych i kluczy licencyjnych, 9. Zarządzać automatycznie instalacją i deinstalacją oprogramowania poprzez definiowanie paczek aplikacji wymaganych i nieautoryzowanych, 10. Umożliwiać przegląd konfiguracji systemu, w tym komend startowych, zmiennych środowiskowych, kont lokalnych użytkowników oraz harmonogramu zadań, 11. Tworzyć listy plików użytkowników o określonych rozszerzeniach (np. avi) znalezionych na stacjach roboczych, wraz z możliwością ich zdalnego usuwania oraz wykrywaniem metadanych, takich jak wymiary obrazów, długość filmów i nagrań audio czy liczba plików i rozmiar w archiwach, 12. Umożliwiać wymianę plików do i ze stacją roboczą poprzez funkcję menedżera plików, przy czym działania administratorów wykonywane w tej funkcji są logowane.   Oprogramowanie musi umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i oprogramowania poprzez:   1. Przechowywanie wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz ich automatyczną aktualizację, 2. Przydzielanie dostępu administratorom do zasobów na podstawie praw do oddziałów, 3. Tworzenie powiązań między zasobami a urządzeniami, 4. Tworzenie powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory) oraz wskazywanie osób odpowiedzialnych, 5. Tworzenie relacji między zasobami, 6. Wskazywanie osób uprawnionych do użycia zasobów za pomocą rozbudowanych mechanizmów, 7. Definiowanie własnych typów zasobów i ich atrybutów wraz z możliwością dodawania dodatkowych informacji, takich jak numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (z funkcją automatycznego powiadamiania e-mailowego), nazwa firmy serwisującej lub komentarz, 8. Określanie atrybutów obowiązkowych dla wszystkich zasobów, 9. Określanie atrybutów dodatkowych tylko dla wybranych typów zasobów, 10. Masową edycję atrybutów zasobów, 11. Definiowanie własnych list jednokrotnego wyboru jako dodatkowych informacji o zasobie, 12. Import danych z zewnętrznych źródeł (np. Pliki .CSV), 13. Przechowywanie dowolnych dokumentów (np. .DOCX, .XLSX, .PDF) takich jak skany faktur, gwarancji czy innych dokumentów, 14. Tworzenie powiązań 1:N między zasobami a dokumentami, 15. Oznaczanie statusów zasobów, np. w użyciu, w naprawie, zutylizowany, 16. Ewidencjonowanie czynności wykonywanych na zasobach, jak aktualizacje, naprawy czy konserwacje wraz z możliwością określenia kosztów i czasu, 17. Generowanie zestawień wszystkich zasobów, w tym urządzeń i zainstalowanego oprogramowania, 18. Przygotowanie wielu szablonów dokumentów i protokołów przekazania zasobów z konfigurowalną sekcją zawierającą dane oraz logo organizacji, 19. Konfigurację stylu automatycznego numerowania zasobów według zdefiniowanych wzorców, 20. Konfigurację stylu automatycznego numerowania dokumentów i protokołów według wzorców, 21. Archiwizację i porównywanie audytów zasobów, 22. Tworzenie kodów kreskowych dla zasobów, 23. Drukowanie kodów kreskowych i dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów z numerem inwentarzowym, 24. Przeprowadzanie inwentaryzacji zasobów z kodami kreskowymi za pomocą aplikacji mobilnej na system Android, obejmującej wyszukiwanie, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych oraz drukowanie etykiet, 25. Przeprowadzanie inwentaryzacji stacji roboczych niepodłączonych do sieci (offline) poprzez manualne skany bez instalacji agenta, 26. Definiowanie alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu "data" w atrybutach zasobów lub licencji, np. Przypomnienie o wygasającej licencji lub gwarancji za 2 tygodnie.   Inwentaryzacja oprogramowania musi zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audytowaniu licencji poprzez:   1. Skanowanie plików wykonywalnych oraz multimedialnych na stacjach roboczych, w tym skanowanie archiwów ZIP, 2. Dostarczanie informacji o aplikacjach używanych w organizacji, 3. Umożliwianie tworzenia własnych wzorców aplikacji, 4. Pozwalanie na tworzenie dowolnych kategorii aplikacji, takich jak nowe, zabronione, 5. Zbieranie informacji o komputerach, na których wykryto daną aplikację, 6. Zarządzanie posiadanymi licencjami, 7. Wskazywanie osób odpowiedzialnych za konkretne licencje, 8. Identyfikowanie użytkowników licencji, 9. Tworzenie powiązań pomiędzy licencjami a dokumentami w relacji 1:N, 10. Oferowanie rozbudowanych i konfigurowalnych scenariuszy zarządzania licencjami, obejmujących przypisywanie licencji do użytkowników, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie według numerów seryjnych oraz wersji aplikacji na jednym urządzeniu, 11. Umożliwianie łatwego audytu legalności oprogramowania oraz wysyłanie powiadomień jedynie w przypadku przekroczenia liczby posiadanych licencji, z możliwością generowania aktualnych raportów audytowych w dowolnym momencie, 12. Generowanie raportów zgodności licencji, 13. Możliwość przypisywania do programów numerów seryjnych, wartości i innych atrybutów.   Moduł: Użytkownicy  Program pozwala na śledzenie aktywności osób pracujących na komputerach z systemem Windows poprzez monitorowanie:   1. Czasu faktycznej aktywności, obejmującego dokładny okres pracy wraz z godziną jej rozpoczęcia i zakończenia, 2. Procesów – każdy z nich posiada określony całkowity czas działania i czas aktywności użytkownika, a także informację, czy został uruchomiony z podwyższonymi uprawnieniami, 3. Rzeczywistego użycia programów, w tym procentowego wskaźnika wykorzystania aplikacji (pokazującego proporcję między czasem używania a czasem uruchomienia), wraz z informacją, na jakim komputerze dane działanie miało miejsce, 4. Dokumentów edytowanych przez użytkownika, 5. Historii pracy użytkownika w postaci cyklicznych zrzutów ekranu, 6. Odwiedzanych stron WWW, obejmujących ich tytuły, adresy, liczbę oraz czas wizyt, 7. Transferu sieciowego użytkownika, zarówno w obrębie sieci lokalnej, jak i w Internecie, 8. Wydruków – w tym informacji o dacie wydruku, wykorzystaniu drukarek, raportów dla każdego użytkownika (zawierających dane: kiedy, ile stron, w jakiej jakości, na której drukarce i jaki dokument drukowano), a także zestawień według stacji roboczej oraz możliwości grupowania drukarek przez ich identyfikację; program umożliwia też kontrolę kosztów wydruków, 9. Nagłówków wiadomości e-mail przesyłanych w aplikacjach klienckich. 10. System wykrywa podejrzaną aktywność generowaną przez powszechnie stosowane "jigglery"﻿, które symulują rzeczywistą pracę, 11. Definiuje minimalny czas (np. 15 minut), po którym wykrywana jest symulowana aktywność polegająca na ruchu myszy bez kliknięć lub na powtarzaniu tego samego znaku z klawiatury, 12. Podejrzana aktywność jest wyszczególniana w raportach monitorujących, 13. W przypadku wykrycia podejrzanej aktywności system generuje alarm oraz inicjuje przypisane działania, 14. Automatycznie uruchamiane jest zapisywanie zrzutów ekranowych po detekcji podejrzanej aktywności, 15. System blokuje dostęp do stron internetowych przez umożliwienie zezwolenia lub zablokowania całego ruchu WWW na stacji roboczej użytkownika, z opcją definiowania wyjątków — zarówno zezwalających, jak i zabraniających dostępu do określonych domen oraz ich subdomen, listy reguł są tworzone dla pojedynczych użytkowników lub grup, a także mogą być kopiowane i współdzielone między kontami i grupami, 16. Integruje listy domen w formacie plików ".TXT"﻿ pobieranych z dowolnych zewnętrznych źródeł, takich jak np. CERT 17. Umożliwia korzystanie z wbudowanych list stron sklasyfikowanych jako zagrożenia, 18. Zapewnia automatyczne odświeżanie list domen zintegrowanych z zewnętrznych adresów, 19. Blokuje ruch na wybranych portach "TCP/IP"﻿ 20. Blokuje pobieranie plików o określonych rozszerzeniach, 21. Prowadzi rejestr naruszeń blokad, 22. Wysyła powiadomienia, gdy użytkownik: odwiedza strony z określonej grupy domen, przesyła w ciągu dnia określoną ilość danych w sieci lokalnej lub "internecie"﻿, drukuje ustaloną liczbę stron dziennie lub narusza skonfigurowane blokady, 23. Generuje raporty zawierające metryki ustawień monitorowania użytkowników, które mogą być dołączane np. do akt pracowniczych, 24. Umożliwia definiowanie harmonogramów (godzin lub dni tygodnia) wyłączających monitorowanie użytkowników. 25. System umożliwia generowanie raportów dla użytkowników Active Directory﻿, niezależnie od komputerów, na których pracowali w danym okresie, 26. Wdrożony mechanizm blokowania uruchamiania aplikacji na podstawie maski nazwy pliku oraz lokalizacji, z regułami w formie list blokowanych plików lub ścieżek przypisanych do użytkowników lub grup użytkowników; reguły te można kopiować pomiędzy grupami lub kontami,   Moduł: Helpdesk i zdalna pomoc  W tym obszarze kontroli stacji użytkownika dostępny jest podgląd pulpitu z możliwością przejęcia nad nim kontroli oraz opcją określenia, czy użytkownik powinien być pytany o zgodę na połączenie oraz z możliwością jego odrzucenia. Podczas zdalnego dostępu zarówno administrator, jak i użytkownik widzą ten sam ekran. Dodatkowa funkcja musi pozwalać na zasłonięcie ekranu użytkownika, aby nie widział działań wykonywanych przez administratora. Administrator może w trakcie sesji zdalnej wybrać dowolny monitor oraz zablokować działanie myszy i klawiatury użytkownika. Połączenie zdalne możliwe jest także z komputerami bez ekranów (maszyny wirtualne, urządzenia bez podłączonego monitora lub laptopy z zamkniętym ekranem). System umożliwia podłączenie równocześnie kilku administratorów do jednego komputera.  W ramach tego modułu dostępna jest baza zgłoszeń umożliwiająca użytkownikom raportowanie problemów technicznych za pomocą dedykowanego portalu oraz obsługę wiadomości e-mail, które są automatycznie przetwarzane i przypisywane odpowiednim administratorom, którzy otrzymują powiadomienia. Oprogramowanie integruje się ze skrzynkami e-mail za pomocą klasycznej autoryzacji login/hasło oraz mechanizmu OAuth 2.0﻿. Moduł wspiera także tryb anonimowy zgłoszeń.  Korzystający mają możliwość monitorowania statusu rozwiązywania swoich zgłoszeń oraz komunikowania się z administratorami poprzez komentarze widoczne dla obu stron. System oferuje także pośredni status „zgłoszenie rozwiązane” przed ostatecznym zamknięciem zgłoszenia.  Moduł ten zawiera komunikator, który umożliwia prowadzenie rozmów w czasie rzeczywistym oraz archiwizację historii wiadomości pomiędzy zalogowanymi użytkownikami, pracownikami pomocy technicznej i administratorami. Komunikator wyposażony jest w wyszukiwarkę rozmów i wiadomości według słów kluczowych oraz funkcję automatycznego oczyszczania historii rozmów. Czat pozwala na zarządzanie dostępem w trzech poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej. Umożliwia prowadzenie rozmów również między użytkownikami oraz osadzanie załączników i obrazków w treści wiadomości. Funkcjonalność komunikatora obejmuje tworzenie pokojów tematycznych i rozmów grupowych oraz oznaczanie kontaktów jako ulubionych. Czat można uruchomić z poziomu ikony dostępowej Agenta lub bezpośrednio w interfejsie WWW﻿ helpdesku﻿.  W module znajduje się także baza wiedzy, która wspiera użytkowników w samodzielnym rozwiązywaniu najprostszych i powtarzających się problemów. Zawiera ona opcję nadawania artykułom jednego z trzech statusów: opublikowany, wewnętrzny lub szkic. Program umożliwia informowanie pracowników o zdarzeniach, takich jak planowane przerwy w dostępie do usług, za pomocą komunikatów z graficznym formatowaniem treści i odnośnikami do artykułów w bazie wiedzy. Użytkownik może przeglądać historię odczytanych komunikatów bezpośrednio z poziomu ikony Agenta. Administrator z kolei ma możliwość tworzenia szkiców i archiwizowania tych komunikatów.  Dostęp do systemu zgłoszeń i bazy wiedzy realizowany jest przez dedykowany portal dostępny za pośrednictwem przeglądarki internetowej, który może być wyświetlany w trybie jasnym lub ciemnym.  Moduł pomocy zdalnej umożliwia również:   1. Pobieranie awatarów oraz listy użytkowników z Active Directory﻿, 2. Wizytówkę użytkownika wraz z informacją o przełożonym, numerem telefonu i adresem e-mail wyświetlaną w systemie zgłoszeń, 3. Tworzenie, usuwanie, aktywację, edycję uprawnień, reset hasła i edycję kont lokalnych Windows, 4. Kontrolę dostępu pracowników helpdesku﻿ do zgłoszeń za pomocą rozbudowanego systemu reguł widoczności, 5. Kontrolę dostępu użytkowników końcowych do wybranych kategorii zgłoszeń, 6. Kontrolę dostępu użytkowników końcowych do wybranych kategorii artykułów bazy wiedzy, 7. Budowę własnego drzewa kategorii zgłoszeń z możliwością ich grupowania w folderach do 4 poziomów, 8. Automatyczne przypisywanie pracowników helpdesk﻿ do zgłoszeń z określonych kategorii lub pochodzących od wybranych grup użytkowników, 9. Definiowanie procesu akceptacji zgłoszeń, w którym użytkownik uzyskuje zgodę na realizację od wyznaczonych osób w organizacji, 10. Przypisywanie procesów akceptacji do konkretnych kategorii zgłoszeń, 11. Przetwarzanie zgłoszeń z wiadomości e-mail, 12. Dostęp do plików źródłowych przetworzonych wiadomości e-mail, 13. Obsługę wielu adresów e-mail jednego użytkownika celem przetwarzania zgłoszeń od tej samej osoby, 14. Eksportowanie list zgłoszeń do formatów CSV i XLSX, 15. Integrację z wieloma skrzynkami e-mail, obsługując różne kanały zgłoszeń z możliwością automatyzacji, 16. Integrację ze skrzynkami e-mail poprzez klasyczną autoryzację login/hasło oraz Oauth 2.0﻿ 17. Tworzenie formularzy z niestandardowymi polami dedykowanymi do wybranych kategorii, 18. Uwzględnianie wyników wyszukiwania w niestandardowych polach zgłoszeń, 19. Współdzielenie pól dodatkowych między wieloma kategoriami, 20. Dedykowane pola dodatkowe dostępne wyłącznie dla pracowników helpdesk﻿, administratorów i operatorów, 21. Wyświetlanie informacji z pól dodatkowych w kolumnach listy zgłoszeń, 22. Wykonywanie zbiorczych operacji na wielu zgłoszeniach, 23. Dołączanie załączników do zgłoszeń, 24. Usuwanie zamkniętych zgłoszeń, 25. Rozbudowane wyszukiwanie w zgłoszeniach i artykułach w bazie wiedzy, 26. Szybki dostęp do ostatnich zgłoszeń, artykułów i załączników, 27. Wprowadzanie komentarzy i informacji o poświęconym czasie na rozwiązanie przy zamykaniu zgłoszenia, 28. Wykonywanie zrzutów ekranowych (podgląd pulpitu), 29. Zdalną modyfikację rejestrów, 30. Dystrybucję oprogramowania przez agenty, 31. Definiowanie aplikacji do samodzielnej instalacji przez użytkowników 32. Dystrybucję i uruchamianie plików (w tym MSI) przez agenty, 33. Kolejkowanie zadań dystrybucji plików, gdy komputer jest wyłączony podczas zlecania operacji, 34. Konfigurowanie automatyzacji procesowania zgłoszeń z wysyłką powiadomień e-mail do przypisanych aktorów, 35. Konfigurację automatyzacji dodających komentarze publiczne wraz z załącznikami i odnośnikami do artykułów w bazie wiedzy, 36. Planowanie nieobecności pracowników helpdesk﻿ 37. Obsługę umów SLA z raportowaniem przekroczeń i podsumowaniem, 38. Generowanie raportów z obsługi helpdesk﻿ 39. Zdalne wykonywanie poleceń (np. Tworzenie lub edycja lokalnych kont użytkowników) poprzez agenty, 40. Zarządzanie procesami systemu Windows, w tym kończenie procesu i drzewa procesu oraz uruchamianie nowych procesów z parametrami w sesji użytkownika, 41. Wymianę plików z i na stacje robocze przez menedżera plików bez blokowania interfejsu programu podczas transferu.   Moduł: DLP (**ochrony przed wyciekiem danych)**  Program musi umożliwiać:   1. Zarządzanie 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, w zakresie blokowania urządzeń i nośników danych. 2. Blokowanie fizycznych urządzeń i interfejsów, takich jak USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD oraz stacje dyskietek. 3. Blokowanie interfejsów bezprzewodowych, w tym Wi-Fi, Bluetooth oraz IrDA. 4. Ograniczenie blokady wyłącznie do urządzeń służących do przenoszenia danych, przy jednoczesnym umożliwieniu podłączania innych urządzeń, takich jak drukarki, klawiatury czy myszy. 5. Generowanie alarmów o zdarzeniach podłączenia lub odłączenia urządzeń zewnętrznych, z opcją ograniczenia ich wyłącznie do nośników niezaufanych. 6. Integrację oraz zarządzanie ustawieniami Windows Defender﻿ jako element funkcji wspierających bezpieczeństwo systemu. 7. Monitorowanie stanu szyfrowania dysków przy użyciu BitLocker﻿ 8. Zdalne szyfrowanie dysków za pomocą BitLocker﻿ 9. Tworzenie list (map) komputerów, które zostały już zaszyfrowane lub nie zostały jeszcze zaszyfrowane. 10. Zapisywanie klucza odzyskiwania zarówno do pliku, jak i jako zasób w bazie danych programu. 11. Integrację z Windows Defender﻿ w zakresie odczytu stanu ochrony, włączania i wyłączania ochrony oraz tworzenia reguł ruchu sieciowego. 12. Odczyt informacji o aktywnym oprogramowaniu antywirusowym firm trzecich, różnym od Windows Defender﻿ 13. Monitorowanie stanu modułu TPM jako element wspierający bezpieczeństwo systemu. 14. Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika. 15. Monitorowanie operacji na plikach na udostępnionych zasobach sieciowych (udziałach) na urządzeniach nieobsługiwanych przez Agenta (np. macierze, NAS itp.) 16. Program umożliwia prowadzenie rejestru naruszeń blokad podłączanych nośników.   Program umożliwia zarządzanie prawami dostępu do urządzeń poprzez:   1. Definiowanie uprawnień dla użytkowników lub grup dotyczących odczytu, zapisu oraz wykonywania plików. 2. Autoryzowanie urządzeń firmowych, na przykład szyfrowanych pendrive’ów czy dysków, przy jednoczesnym blokowaniu urządzeń prywatnych. 3. Całkowite blokowanie określonych typów urządzeń dla wybranych użytkowników. 4. Centralne ustawianie reguł (polityk) konfiguracyjnych obowiązujących w całej sieci. 5. Usuwanie z listy znanych urządzeń nośników, które na przykład zostały zutylizowane.   Program realizuje audyt operacji na plikach na urządzeniach przenośnych poprzez:   1. Zapisywanie informacji dotyczących zmian w systemie plików na tych urządzeniach. 2. Rejestrowanie podłączenia oraz odłączenia urządzeń przenośnych. |
| Wdrożenie oprogramowania  W ramach realizacji zamówienia Wykonawca jest zobowiązany do kompleksowego wdrożenia **Oprogramowania do zarządzania IT**. Proces wdrożenia musi być wykonany zdalnie i obejmować wszystkie poniższe etapy, gwarantując pełną gotowość systemu do pracy w środowisku Zamawiającego.  **1. Instalacja i Konfiguracja Środowiska Serwerowego**   * **Instalacja komponentów:** Wykonawca zainstaluje i skonfiguruje wszystkie komponenty serwerowe oprogramowania (Serwer, Konsola administracyjna, Baza danych) na infrastrukturze wskazanej przez Zamawiającego, zgodnie z wymaganiami systemowymi określonymi w OPZ. * **Przygotowanie Agenta:** Wykonawca przygotuje i udostępni Zamawiającemu pakiety instalacyjne Agenta (w formacie .msi) gotowe do dystrybucji za pośrednictwem MS Active Directory oraz do instalacji manualnej. * **Aktualizacja:** Wykonawca zapewni, że wszystkie instalowane komponenty (Serwer, Baza Danych, Konsola, Agent) są w najnowszej stabilnej wersji oferowanej przez producenta w dniu instalacji.   **2. Integracja z Infrastrukturą Zamawiającego**   * **Synchronizacja z Active Directory:** Wymaga się skonfigurowania i przetestowania mechanizmu importu oraz cyklicznej aktualizacji danych o użytkownikach, komputerach i strukturze organizacyjnej z usługi MS Active Directory Zamawiającego. * **Uwierzytelnianie i autoryzacja:** Wykonawca skonfiguruje system tak, aby logowanie do konsoli administracyjnej odbywało się z wykorzystaniem mechanizmu jednokrotnego logowania (SSO) poprzez Active Directory. Należy również skonfigurować uprawnienia w systemie w oparciu o mechanizm RBAC zintegrowany z grupami AD.   **3. Konfiguracja Funkcjonalna i Uruchomienie**   * **Wdrożenie pilotażowe:** Wykonawca, we współpracy z Zamawiającym, wdroży Agenta na uzgodnionej grupie pilotażowej komputerów (minimum 10 stanowisk) w celu weryfikacji poprawności zbierania danych inwentaryzacyjnych. * **Konfiguracja bazowa:** Wykonawca przeprowadzi wstępną konfigurację (profilowanie) kluczowych modułów systemu, w tym:   + Inwentaryzacji sprzętu i oprogramowania w celu zapewnienia prawidłowego gromadzenia danych.   + Monitorowania uruchamianych aplikacji i odwiedzanych stron WWW.   + Zarządzania licencjami, w tym definicji podstawowych typów licencji używanych u Zamawiającego (np. OEM, Freeware). * **Powiadomienia i alerty:** Wymaga się skonfigurowania i przetestowania co najmniej trzech różnych powiadomień systemowych (np. o małej ilości miejsca na dysku, wykryciu nieautoryzowanego oprogramowania, zmianie w konfiguracji sprzętowej), aby zademonstrować działanie mechanizmu alertów. * **Panel Pracownika:** Wykonawca skonfiguruje domyślny schemat widoku dla Panelu pracownika, który będzie udostępniał podstawowe informacje o sprzęcie i oprogramowaniu przypisanym do użytkownika.   **4. Szkolenie i Dokumentacja**   * **Szkolenie:** Wykonawca jest zobowiązany do przeprowadzenia zdalnego szkolenia w wymiarze **minimum 2 godzin** dla administratorów Zamawiającego. Szkolenie musi obejmować obsługę konsoli, podstawową konfigurację, generowanie raportów oraz zarządzanie agentami. * **Certyfikaty:** Po zakończonym szkoleniu Wykonawca dostarczy imienne certyfikaty dla przeszkolonych administratorów. * **Dokumentacja:** Wykonawca przekaże Zamawiającemu dokumentację powdrożeniową w języku polskim, opisującą wykonaną instalację i konfigurację.   **5. Warunki Odbioru Wdrożenia**  Odbiór prac wdrożeniowych zostanie potwierdzony protokołem odbioru po łącznym spełnieniu przez Wykonawcę wszystkich poniższych warunków:   * Potwierdzenie poprawnej instalacji i działania wszystkich komponentów serwerowych. * Pozytywna weryfikacja synchronizacji danych z Active Directory. * Wykazanie poprawnego zbierania danych inwentaryzacyjnych z grupy pilotażowej komputerów. * Przeprowadzenie wymaganego szkolenia i dostarczenie certyfikatów. * Przekazanie kompletnej dokumentacji powdrożeniowej. |

## Zestawienie zakresu dostaw i usług – część 2

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Lp.** | **Nazwa środka trwałego lub wartości niematerialnych i prawnych itp.** | **Wymagana minimalna długość gwarancji (m-ce)** | **Wymagana długość obowiązywania licencji na oprogramowanie (m-ce)** | **Typ/Rodzaj gwarancji** | **Ilość** | **Jednostka miary** |
|  | Macierz do backupu | 36 | 36 | Producenta | 1 | Szt. |
|  | Firewall (UTM) | 36 | 36 | Producenta | 2 | Szt. |
|  | System zbierania i analizy logów | 36 | 36 | producenta | 1 | Szt. |
|  | Przełącznik sieci LAN -CORE | 36 | 36 | Producenta | 2 | Szt. |
|  | System do zarządzania i monitorowania dostępu do sieci (NAC) | 36 | 36 | Producenta | 1 | Licencja |

## Opis przedmiotu zamówienia

### Macierz do backupu

|  |  |  |
| --- | --- | --- |
| Lp. | Nazwa parametru | Minimalna wartość parametru |
|  | Obudowa | System musi być dostarczony ze wszystkimi komponentami do instalacji w szafie rack 19'' |
|  | Pojemność: | 1. System musi zostać dostarczony w konfiguracji zawierającej minimum 12 dysków 10TB NL-SAS oraz posiadać możliwość rozbudowy o kolejne dyski 2. System musi wspierać dyski:  * SAS: 1200GB do 1800GB * SATA/NL-SAS: od 4TB do 22TB * SSD lub NVME: 800GB do 15 300GB  1. Budowa systemu musi umożliwiać rozbudowę do modeli wyższych bez potrzeby kopiowania/migrowania danych. (Zamawiający przez model wyższy rozumie inny model macierzy danego producenta z większą pamięcią cache oraz mocniejszymi procesorami). 2. Zamawiający dopuszcza rozwiązanie, które nie pozwala na rozbudowę do wyższego modelu przy założeniu, że zostanie zaoferowany najwyższy model z rodziny z pamięcią Cache min. 1TB na kontroler. 3. System musi mieć możliwość rozbudowy do 500 dysków w obrębie pary kontrolerów lub w obrębie klastra wielu kontrolerów (scale-out) w zależności od sposobu realizacji rozbudowy dla oferowanego rozwiązania. 4. W przypadku klastrowania kontrolerów macierzy, system musi działać pod kontrolą jednego systemu operacyjnego od jednego producenta, nie dopuszczalne jest zestawienie systemu klastrowego poprzez wykorzystanie serwerów pośredniczących i oprogramowania dodatkowego. 5. Dla rozwiązań wykorzystujących klastrowanie (scale-out) musi być możliwość rozbudowy rozwiązania do co najmniej 12 kontrolerów w klastrze. 6. Rozwiązanie musi pozwalać na rozbudowę o dyski lub dodatkowe kontrolery (z zachowaniem obecnych) wykonane w technologii NVMe do min 1150 dysków w technologii NVME. Zamawiający dopuszcza zaoferowanie rozwiązania, które nie posiada takiej możliwości w przypadku, gdy całość zasobów zostanie dostarczona na dyskach flash/SSD. |
|  | Kontroler | 1. Dwa kontrolery wyposażone w przynajmniej 512GB cache każdy dla rozwiązania opartego o dyski SSD lub NVME 128GB Cache na kontroler. 2. Zamawiający dopuszcza alternatywnie rozwiązanie (dla konfiguracji z dyskami NL-SAS) posiadające co najmniej 64GB cache oparte o RAM na kontroler, jeżeli dodatkowo zostanie dostarczona z macierzą dodatkowa pamięć Flash minimum 1024GB pamięci na kontroler (wbudowana w kontroler lub formie dodatkowych dysków Flash skonfigurowanych w RAID 10) 3. System musi pozwalać na rozbudowę pamięci Cache opartej o RAM do 3072GB za pomocą dodatkowych modułów pamięci RAM lub poprzez rozbudowę o kolejne kontrolery. 4. Procesory macierzy powinny być wykonane w technologii wielordzeniowej z przynajmniej 8 rdzeniami na każdy kontroler dla procesorów AMD i Intel. Dla innych rodzajów procesorów min 64 rdzenie. 5. W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez minimum 72 godziny lub poprzez zrzut na pamięć nieulotną 6. Macierz musi pozwalać na poszerzenie pamięci Cache za pomocą dysków SSD do 6TB. |
|  | Interfejsy | Oferowana macierz musi posiadać minimum   * 4 porty 10Gbe SFP+ * 4 porty 32Gb FC * 4 porty 1GbE * 6 portów 12Gb SAS, |
|  | RAID | System RAID musi zapewniać taki poziom zabezpieczania danych, aby był możliwy do nich dostęp w sytuacji awarii minimum dwóch dysków w grupie RAID |
|  | Kopie Migawkowe | Macierz musi być wyposażona w system kopii migawkowych, dostępny dla wszystkich rodzajów danych przechowywanych na macierzy. System kopii migawkowych nie może powodować spadku wydajności macierzy +/-5%  Zamawiający dopuszcza rozwiązanie, które ma wpływ na wydajność przy stosowaniu kopii migawkowych przy zapisie, przy założeniu zaoferowania całej pojemności na dyskach SSD/Flash/NVME. |
|  | Obsługiwane protokoły | Macierz musi obsługiwać jednocześnie protokoły FC, iSCSi, CIFS i NFS, S3 (macierz obiektowa) - jeśli wymagane są licencje zamawiający wymaga dostarczenia ich wraz z macierzą. |
|  | Inne wymagania | 1. Macierz musi posiadać wsparcie dla wielościeżkowości dla systemów Win 2019 i nowsze, Linux, Vmware, Unix 2. Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie 3. Macierz musi posiadać funkcjonalność priorytetyzacji zadań. 4. Macierz musi posiadać funkcjonalność kompresji danych w trybie in-line oraz off-line na każdym rodzaju danych. 5. Macierz musi posiadać funkcjonalność eliminacji (deduplikacji) identycznych bloków danych którą można stosować na macierzy/danych produkcyjnej dla wszystkich rodzajów danych. Macierz powinna mieć możliwość czynności odwrotnej tzn. Cofnięcia procesu deduplikacji na zdeduplikowanym wolumenie. Jeżeli oferowane rozwiązanie nie posiada funkcjonalności deduplikacji danych, zamawiający wymaga dostarczenia 4-krotności przestrzeni wyspecyfikowanej. 6. System musi posiadać specjalny moduł do zabezpieczenia przez atakiem Ransomware w szczególności:   - musi informować administratora w przypadku niestandardowego zachowania systemu oraz danych  - wykonywać prewencyjną kopię migawkową „snapshot” w przypadku zagrożenia atakiem ransomware  - monitorować niestandardowe zachowanie użytkowników serwera plików  - moduł musi działać także dla zasobów SAN   1. Macierz musi posiadać zaimplementowaną funkcjonalność WORM. Jeżeli rozwiązanie wymaga do tego licencji zamawiający wymaga jej dostarczenia. 2. W celach bezpieczeństwa macierz musi posiadać funkcjonalność wieloetapowej akceptacji wybranych operacji tj. operacje takie jak: Skasowanie LUN/Wolumeny, skasowanie Snapshotu, wyłączenie replikacji. System musi pozwalać by wykonanie w/w operacji było akceptowane przez przynajmniej dwóch administratorów w celu zwiększenia bezpieczeństwa i uniknięcia błędów ludzkich. 3. Macierz musi posiadać możliwość automatycznego informowania przez macierz i przesyłania przez pocztę elektroniczną raportów o konfiguracji, utworzonych dyskach logicznych i woluminach oraz ich zajętości wraz z podziałem na rzeczywiste dane, kopie migawkowe oraz dane wewnętrzne macierzy. 4. Macierz musi posiadać funkcjonalność wykonania wirtualnych klonów, które nie wymagają kopiowania bloków danych. 5. Z macierzą zamawiający wymaga dostarczenia oprogramowania, które pozwala na:   - monitoring wykorzystania przestrzeni na macierzy  - monitoring grup RAIDowych  - monitoring wykonywanych backupów/replikacji danych między macierzami  - monitoring wydajności macierzy  - analizę i diagnozę spadku wydajności   1. Zamawiający dopuszcza zastosowanie oprogramowania zewnętrznego, na pełną max pojemność macierzy. 2. Wszystkie funkcjonalności muszą być dostarczone na maksymalną pojemność macierzy 3. Producent musi dostarczyć usługę w postaci portalu WWW lub dodatkowego oprogramowania umożliwiającą następujące funkcjonalności:   - Narzędzie do tworzenia procedury aktualizacji oprogramowania macierzowego.  a) procedura musi opierać się na aktualnych danych pochodzących z macierzy oraz najlepszych praktykach producenta.  b) procedura musi uwzględniać systemy zależne np. macierze replikujące  c) procedura musi umożliwiać generowanie planu cofnięcia aktualizacji.  - Wyświetlanie statystyk dotyczących wydajności, utylizacji, oszczędności uzyskanych dzięki funkcjonalnościom macierzy.  - Wyświetlanie konfiguracji macierzy oraz porównywanie jej z najlepszymi praktykami producenta w celu usunięcia błędów konfiguracji.   1. Portal lub oprogramowanie może pochodzić od innego producenta niż producent macierzy z tym, że zostanie dostarczona odpowiednia licencja do maksymalnej pojemności macierzy. 2. Zamawiający wymaga by wszystkie funkcjonalności działały wspólnie tj. włączenie jednej funkcjonalności nie eliminowało innej. |
|  | Gwarancja i serwis | 1. 3 lata serwisu producenta z 2 godzinnym czasem odpowiedzi na awarie krytyczne i wymianą onsite elementów w na następny dzień roboczy 2. Dostarczony system musi posiadać również 3 lata subskrypcji dla dostarczonego wraz z macierzą oprogramowania, dostęp do portalu serwisowego producenta, dostęp do wiedzy i informacji technicznych dotyczących oferowanego urządzenia. 3. Zepsute nośniki pozostają u Zamawiającego |
|  | Inne | 1. Oferowane urządzenie (macierz dyskowa/serwer) musi spełniać wymogi Rozporządzenia Komisji (UE) 2019/424 z dnia 15 marca 2019 r. ustanawiającego wymogi dotyczące ekoprojektu dla serwerów i produktów do przechowywania danych (tzw. Lot 9). 2. Urządzenie musi być zgodne z Dyrektywą Parlamentu Europejskiego i Rady 2011/65/UE (Dyrektywa RoHS) w sprawie ograniczenia stosowania niektórych niebezpiecznych substancji w sprzęcie elektrycznym i elektronicznym oraz nie może zawierać substancji z listy kandydackiej SVHC w stężeniu powyżej 0,1% wag., zgodnie z rozporządzeniem REACH (WE) nr 1907/2006. |

### Firewall (UTM)

|  |
| --- |
| **Wymagania Ogólne**   1. System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. 2. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. 3. System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacjisubskrypcje 4. Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu. 5. System wspiera protokoły IPv4 oraz IPv6 w zakresie:    1. Firewall.    2. Ochrony w warstwie aplikacji.    3. Protokołów routingu dynamicznego.   **Redundancja, monitoring i wykrywanie awarii**   1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych. 5. System ma pracować w postaci redundantnego klastra.   **Interfejsy, Dysk, Zasilanie:**   1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:  * 10 portami Gigabit Ethernet RJ-45. * 8 gniazdami SFP 1 Gbps. * 4 gniazdami SFP+ 10 Gbps.  1. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB. 2. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q. 3. System jest wyposażony w zasilanie AC.   **Parametry wydajnościowe:**   1. W zakresie Firewall’a obsługa nie mniej niż 3 mln jednoczesnych połączeń oraz 130 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 38 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6.5 Gbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 33 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) - minimum 5 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 - minimum 2.5 Gbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 3 Gbps.   **Funkcje Systemu Bezpieczeństwa:**  W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:   1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN. 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. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 12. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system. 13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).   **Polityki, Firewall**   1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:  * Translację jeden do jeden oraz jeden do wielu. * Dedykowany ALG (Application Level Gateway) dla protokołu SIP.  1. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP. 3. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 4. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 5. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.  * Amazon Web Services (AWS). * Microsoft Azure. * Cisco ACI. * Google Cloud Platform (GCP). * OpenStack. * VMware NSX. * Kubernetes.   **Połączenia VPN**   1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:  * Wsparcie dla IKE v1 oraz v2. * Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). * Obsługa protokołu Diffie-Hellman grup 19, 20. * Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. * Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. * Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. * Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. * Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. * Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. * Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. * Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. * Mechanizm „Split tunneling” dla połączeń Client-to-Site.  1. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.   **Routing i obsługa łączy WAN**  W zakresie routingu rozwiązanie zapewnia obsługę:   1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.   **Funkcje SD-WAN**   1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).   **Zarządzanie pasmem**   1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System daje możliwość określania pasma dla poszczególnych aplikacji. 3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.   **Ochrona przed malware**   1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. W przypadku archiwów zagnieżdżonych istnieje 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 umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej. 8. System wstrzymuje dostarczenie pliku, dla którego jest realizowana analiza z wykorzystaniem systemu Sandbox, do czasu otrzymania werdyktu z systemu Sandbox. 9. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 10. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 11. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.   **Ochrona przed atakami**   1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookiesdla protokołu http. 8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. 9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.   **Kontrola aplikacji**   1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. 6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).   **Kontrola WWW**   1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. 4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.   **Uwierzytelnianie użytkowników w ramach sesji**   1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:  * Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. * Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. * Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.  1. System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego. 2. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. 3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.   **Zarządzanie**   1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. 3. Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego. 4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). 9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.   **Logowanie**   1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 4. Możliwość włączenia logowania per reguła w polityce firewall. 5. System zapewnia możliwość logowania do serwera SYSLOG. 6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.   **Testy wydajnościowe oraz funkcjonalne**   1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni.   **Serwisy i licencje**  Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:   * 1. Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android),   2. Analiza typu Sandbox realizowana inline, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen,   3. Weryfikacja zgodności konfiguracji z dobrymi praktykami producenta (audyt konfiguracji i polityk urządzenia) na okres 36 miesięcy.   **Gwarancja oraz wsparcie**  System jest objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania i wsparcie techniczne w trybie 24x7 przez dedykowany moduł internetowy oraz infolinię.  **Pozostałe wymagania**   1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. 2. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań. 3. Urządzenie musi być zgodne z Dyrektywą 2011/65/UE (RoHS) w zakresie ograniczenia stosowania ołowiu, rtęci, kadmu i innych substancji niebezpiecznych oraz zgodne z rozporządzeniem REACH (WE) nr 1907/2006. 4. Producent urządzenia musi gwarantować dostępność aktualizacji oprogramowania układowego (firmware) oraz sygnatur bezpieczeństwa przez okres minimum **5 lat** od daty zakupu, co zapobiega przedwczesnemu wykluczeniu urządzenia z użytku (starzenie techniczne). |

### System zbierania i analizy logów

|  |
| --- |
| **Wymagania Ogólne**  W ramach pozycji wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.  Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi werje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016, 2019, 2022, 2025; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).  **Interfejsy, Dysk:**   1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 10 TB.   **Parametry wydajnościowe:**   1. System musi być w stanie przyjmować minimum 20 GB logów na dzień. 2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.   W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:  **Logowanie**   1. Podgląd logowanych zdarzeń w czasie rzeczywistym. 2. Możliwość przeglądania logów historycznych z funkcją filtrowania. 3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:    1. Listę najczęściej wykrywanych ataków.    2. Listę najbardziej aktywnych użytkowników.    3. Listę najczęściej wykorzystywanych aplikacji.    4. Listę najczęściej odwiedzanych stron www.    5. Listę krajów, do których nawiązywane są połączenia.    6. Listę najczęściej wykorzystywanych polityk Firewall.    7. Informacje o realizowanych połączeniach IPSec. 4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów. 5. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514. 6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.   **Raportowanie**  W zakresie raportowania system musi zapewniać:   1. Generowanie raportów co najmniej w formatach: PDF, CSV. 2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników. 3. Funkcję definiowania własnych raportów. 4. Możliwość spolszczenia raportów. 5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.   **Korelacja logów**  W zakresie korelacji zdarzeń system musi zapewniać:   1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany. 2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. 3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:  * Malware. * Aplikacje sieciowe. * Email. * IPS. * Traffic. * Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.  1. Funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach, w celu wykrycia potencjalnych stacji - narażonych na zagrożenie w ostatnim czasie. 2. Funkcję zarządzania zdarzeniami z automatyzacją zadań, która może być konfigurowalna za pomocą playbooków składających się z reakcji i sekwencji zautomatyzowanych działań. 3. Funkcję, która umożliwia administratorom wyświetlanie alertów typu Outbreak i automatyczne pobieranie powiązanych zdarzeń oraz raportów od producenta rozwiązania.   **Zarządzanie**   1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów. 2. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI. 3. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.   **Serwisy i licencje**   1. Wsparcie: System musi być objęty licencją wieczystą wraz z serwisem producenta przez okres 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.   **Pozostałe wymagania**   1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. 2. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań. |

### Przełącznik sieci LAN -CORE

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **I. Wymagania Ogólne**   1. Przedmiotem zamówienia jest dostawa fabrycznie nowego, nieużywanego i nieregenerowanego przełącznika sieciowego. 2. Oferowane urządzenie musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na rynek polski. 3. Urządzenie musi być kompletne, sprawne technicznie i gotowe do pracy bez konieczności dokonywania dodatkowych zakupów. 4. Wszystkie oferowane funkcjonalności muszą być dostępne w ramach dostarczonej licencji, bez dodatkowych opłat. 5. Urządzenie musi w pełni wspierać obsługę protokołu IPv6. 6. Urządzenie musi spełniać wymogi dyrektywy RoHS (2011/65/UE) oraz być wolne od substancji z listy SVHC (REACH).   **II. Minimalne Wymagania Techniczne**   |  |  | | --- | --- | | **Parametr** | **Wymagana wartość / funkcjonalność** | | **Parametry Konstrukcyjne i Fizyczne** | | | Rodzaj urządzenia | Przełącznik zarządzalny warstwy L3. | | Obudowa | Standard RACK 19", wysokość nie większa niż 1U. | | Porty światłowodowe | Co najmniej 24 porty SFP+ pracujące z przepustowością 10 Gb/s. | | Porty uniwersalne | Co najmniej 4 porty uniwersalne (combo) 10 Gb/s, każdy umożliwiający pracę jako port SFP+ lub port miedziany RJ-45. | | Porty do zarządzania | Wymagany co najmniej jeden fizyczny port konsolowy (np. RJ-45 lub USB-C). | | Zasilanie | Wbudowany zasilacz AC z zakresem napięcia wejściowego 100-240V, 50/60Hz. | | **Wydajność** | | | Przepustowość matrycy | Nie mniejsza niż 480 Gb/s. | | Szybkość przekazywania | Nie mniejsza niż 350 Mpps (dla pakietów 64-bajtowych). | | Pamięć RAM | 1 GB. | | Pamięć Flash | 512 MB. | | Rozmiar bufora pakietów | 1,5 MB. | | **Funkcjonalność Warstwy 2** | | | Tablica adresów MAC | Pojemność co najmniej 16 000 wpisów. | | Ramki Jumbo | Obsługa ramek o rozmiarze co najmniej 9000 bajtów. | | Sieci VLAN | Obsługa co najmniej 4000 aktywnych sieci VLAN zgodnie z IEEE 802.1Q. Wymagana obsługa VLAN-ów prywatnych (Private VLAN) oraz gościnnych (Guest VLAN). | | Agregacja portów | Wsparcie dla standardu IEEE 802.3ad (LACP). Możliwość konfiguracji co najmniej 8 grup agregacyjnych. | | Protokoły Spanning Tree | Wsparcie dla standardów IEEE 802.1D (STP), IEEE 802.1w (RSTP), IEEE 802.1s (MSTP). | | **Funkcjonalność Warstwy 3** | | | Routing statyczny | Wsparcie dla routingu statycznego IPv4 oraz IPv6. Możliwość zdefiniowania co najmniej 990 tras statycznych IPv4. | | Interfejsy IP | Możliwość konfiguracji co najmniej 128 interfejsów wirtualnych (SVI). | | Routing dynamiczny | Wsparcie dla protokołu RIPv2. | | Routing zaawansowany | Wsparcie dla routingu opartego na regułach (Policy-Based Routing, PBR). | | **Bezpieczeństwo** | | | Kontrola dostępu do sieci | Wsparcie dla uwierzytelniania na portach zgodnie ze standardem IEEE 802.1X. | | Centralne uwierzytelnianie | Wsparcie dla protokołów RADIUS oraz TACACS+. | | Listy kontroli dostępu (ACL) | Możliwość definiowania list ACL w oparciu o adresy MAC, IP (warstwa 3) oraz porty TCP/UDP (warstwa 4). Wymagana obsługa co najmniej 1000 reguł. | | Ochrona przed atakami | Wbudowane mechanizmy ochrony: DHCP Snooping, Dynamic ARP Inspection (DAI), IP Source Guard. | | Kontrola ruchu | Mechanizmy kontroli natężenia ruchu rozgłoszeniowego, multicast i unicast (Storm Control). | | Bezpieczeństwo portów | Mechanizm Port Security umożliwiający ograniczenie liczby i/lub typów adresów MAC na porcie. | | **Jakość Usługi (QoS)** | | | Kolejkowanie | Obsługa co najmniej 8 kolejek priorytetów na port. | | Klasyfikacja ruchu | Możliwość klasyfikacji ruchu na podstawie pól CoS (IEEE 802.1p) oraz DSCP/ToS (IP Precedence). | | Algorytmy kolejkowania | Wsparcie dla algorytmu WRR (Weighted Round Robin). | | **Zarządzanie** |  | | Interfejsy zarządzania | Zarządzanie poprzez interfejs wiersza poleceń (CLI), graficzny interfejs webowy (GUI) oraz protokół SNMP v2c i v3. | | Bezpieczne zarządzanie | Wymagane wsparcie dla protokołów SSH, HTTPS oraz SNMPv3 w celu zapewnienia szyfrowanej komunikacji. | | Monitorowanie i logowanie | Wsparcie dla RMON, a także możliwość wysyłania logów systemowych do zewnętrznego serwera Syslog. | | **Warunki Środowiskowe i Niezawodność** | | | Temperatura pracy | Zakres od -5°C do +50°C. | | Wilgotność pracy | Zakres od 10% do 90% (bez kondensacji). | | MTBF (średni czas bezawaryjnej pracy) | Nie krótszy niż 2 000 000 godzin. |   **III. Wymagania Gwarancyjne i Serwisowe**   1. Wymagana jest gwarancja producenta typu "ograniczona dożywotnia" (limited lifetime). 2. Wykonawca musi zapewnić dostęp do wsparcia technicznego producenta przez okres co najmniej 36 miesięcy od daty dostawy.   **IV. Wymagania Dodatkowe**   1. Wraz z urządzeniem należy dostarczyć komplet akcesoriów niezbędnych do jego montażu w szafie RACK 19" (np. uchwyty montażowe, śruby). 2. Należy dostarczyć komplet niezbędnego okablowania (kabel zasilający, kabel konsolowy). 3. Wraz z każdym z dwóch (2) dostarczonych przełączników, Wykonawca jest zobowiązany dostarczyć    1. 12 szt. fabrycznie nowych kable typu Direct Attach Copper (DAC) zgodne ze standardem SFP+ (10 Gb/s).    2. 12 kompletów połączeniowych składających się z każdy z 2 wkladek SFP+ oraz patchcorda światłowodowego.   Długość każdego kabla nie może być mniejsza niż 2 metry, a dostarczone kable muszą być w pełni kompatybilne z oferowanym modelem przełącznika. |

### System do zarządzania i monitorowania dostępu do sieci (NAC)

|  |
| --- |
| **Wymagania ogólne**   1. Przedmiotem jest dostarczenie centralnego systemu kontroli i zarządzania dostępem do sieci LAN oraz WLAN współpracującego z posiadaną przez Zamawiającego infrastrukturą dostępową. 2. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu NAC były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia w środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy wirtualne wraz z odpowiednio zabezpieczonym systemem operacyjnym. Platformy wirtualne muszą wspierać następujące rodzaje hypervisorów: Vmware vSphere, KVM oraz Microsoft Hyper-V. 3. W ramach pozycji muszą zostać dostarczone wszystkie elementy fizyczne lub wirtualne niezbędne do monitorowania i zarządzania kontrolą dostępu   **Architektura**   1. System musi umożliwiać instalację rozproszoną na wielu serwerach fizycznych lub wirtualnych w celu zapewnienia wysokiej niezawodności i możliwości stopniowego zwiększania wydajności systemu (skalowanie). 2. Elementy Systemu muszą umożliwiać klastrowanie active-passive. 3. System NAC musi pracować w trybie out-of-band, tj. realizować wszystkie wymagane funkcje bez konieczności analizy ruchu sieciowego (na porcie SPAN, inline). 4. Wszystkie elementy Sytemu powinny być zarządzane centralnie. 5. System i jego wszystkie funkcje muszą w pełni współpracować z urządzeniami Zamawiającego (tj. można na nich wydawać polecenia konfiguracyjne z poziomu systemu kontroli i zarządzania dostępem do sieci):   **Funkcje Systemu**   1. System musi umożliwiać uwierzytelnienie użytkowników i urządzeń podłączanych do sieci lokalnej LAN i sieci bezprzewodowej WLAN z wykorzystaniem:    * standardu 802.1X    * adresu MAC urządzenia    * formularza webowego (captive portal) z wykorzystaniem LDAP lub przy pomocy loginu i hasła z lokalnej bazy danych użytkowników w Systemie. 2. System musi obsługiwać uwierzytelnianie w oparciu o: wbudowany serwer RADIUS, zewnętrzny serwer Radius, protokół LDAP, jak również w oparciu o wewnętrzną bazę użytkowników i urządzeń. 3. System musi obsługiwać autoryzację w oparciu o adresy MAC definiowane w wewnętrznej bazie z wykorzystaniem protokołu RADIUS. 4. System musi obsługiwać „machine authentication” w oparciu o grupy urządzeń pochodzące z serwerów Windows AD. 5. System musi obsługiwać środowiska EduRoam w celu utworzenia procesu uwierzytelniania dla gości z różnych instytucji. 6. System musi obsługiwać obsługę RADIUS Change of Authorization (CoA) z niestandardowymi atrybutami (AVPairs). 7. System musi obsługiwać następujące metody uwierzytelnienia: TLS (w tym TLS 1.3), TTLS, PEAP, MD5, GTC, MSCHAPV2, FAST, TEAP. 8. System musi zapewniać automatyczne wykrywanie urządzeń końcowych i śledzenie ich położenia poprzez identyfikowanie nowych adresów MAC i IP, nowych sesji uwierzytelniających (802.1X, wykorzystujące przeglądarkę internetową, LDAP) lub żądania RADIUS pochodzących z przełączników dostępowych. W ramach postępowania muszą zostać dostarczone wszystkie niezbędne elementy, które umożliwią realizację powyższej funkcji we wszystkich lokalizacjach i segmentach sieci. 9. System powinien logować i przetrzymywać we własnej bazie danych co najmniej następujące informacje:    * adresy MAC przełączników, urządzeń końcowych i dostępowych,    * adresy IP ww. urządzeń    * identyfikatory i nazwy portów przełączników określające porty na przełącznikach i urządzeniach dostępowych do których podłączane są urządzenia końcowe    * stan skanowania - wyniki skanowania urządzenia końcowego i jego ocena. w oparciu skanowanie przeprowadzone przy pomocy dostępnych w rozwiązaniu agentów    * informacje o użytkownikach    * nazwa użytkownika, do którego przypisany jest urządzenie końcowe    * nazwa zalogowanego użytkownika na urządzeniu końcowym, jeśli wykonywana jest na nim autoryzacja    * profil/rola jak została przydzielona urządzeniowi końcowemu przez System    * data zarejestrowania urządzenia końcowego w Systemie    * data ostatniego logowania urządzenia końcowego w sieci lub/i podłączenia 10. System musi umożliwiać tworzenie reguł autoryzacji (kontroli dostępu) opartych o złożone i wielowarunkowe polityki bezpieczeństwa. Powinny one obejmować co najmniej: lokalizacja urządzenia w sieci, przynależność do grupy administracyjnej, parametr opisujący urządzenie lub użytkownika. 11. System musi aktywnie zapobiegać przed dostępem do sieci nieautoryzowanych użytkowników, zagrożonych urządzeń końcowych i innych niechronionych urządzeń. Dla tak zdefiniowanych urządzeń końcowych muszą być zapewnione mechanizmy automatycznej kwarantanny oraz blokowania. 12. System musi zapewniać możliwość powiadamiania poprzez SYSLOG oraz pocztę elektroniczną o sytuacjach krytycznych np. związanych z próbą nieautoryzowanego dostępu do sieci lub awarii wewnętrznych usług Systemu NAC. 13. System musi posiadać wewnętrzną bazę urządzeń. Baza musi umożliwiać wprowadzanie danych poprzez import danych, wprowadzanie danych z poziomu Systemu lub z wykorzystaniem API. 14. System musi wykorzystywać informacje zawarte w bazie urządzeń końcowych dla potrzeb procesów wykrywania, oceniania, kwarantanny, korygowania oraz autoryzacji. 15. System musi posiadać bazę minimum 30 kategorii urządzeń końcowych. 16. System musi mieć możliwość klasyfikacji jednorazowej przy wstępnym uwierzytelnianiu/rejestracji bądź klasyfikacji wielokrotnej. Klasyfikacja urządzeń i użytkowników musi bazować na harmonogramie z częstotliwością w przedziale od kilku minut do kilku tygodni. 17. System musi umożliwiać wykonywanie na urządzeniach sieciowych skryptów CLI, które są elementem polityk bezpieczeństwa. 18. System musi obsługiwać telefony IP wraz z możliwością podłączenia do nich stacji końcowych (przez wbudowany przełącznik w telefonie) przypisując każdemu z urządzeń dedykowane polityki bezpieczeństwa. 19. System musi podejmować decyzję o przyłączeniu urządzeń końcowych do sieci poprzez ocenę ich zgodności ze zdefiniowanymi wymaganiami. Ocena zgodności musi być realizowana zarówno bez dedykowanego agenta instalowanego na stacji końcowej (za pomocą metod takich jak: WinRM, WMI) jak i z użyciem agenta. Ocena stanu stacji końcowych musi być możliwa zarówno w trybie „pre-connect” przed udzieleniem dostępu do sieci, jak i w trybie „post-connect – po udzieleniu dostępu do sieci. 20. Klasyfikacja urządzeń końcowych z użyciem agenta dedykowanego dla komputerów z systemem Windows i MAC OS X musi umożliwiać przeprowadzenie następujących testów:     1. Sprawdzenie wersji agenta     2. Sprawdzenie wersji systemu operacyjnego,     3. Sprawdzenie obecności i stanu oprogramowania antywirusowego (niezainstalowany/zainstalowany, uruchomiona ochrona, zaktualizowany),     4. test zapory (włączona/wyłączona),     5. test poprawek do systemów Windows (sprawdzanie czy poprawka jest zainstalowana bądź nie),     6. test usługi Windows Update z opcją automatycznego naprawienia niezgodności     7. test obecności/niewystępowania pliku o określonej nazwie     8. test obecności procesu (uruchomiony/nieuruchomiony)     9. test rejestru dla systemów Windows (obecność klucza o zdefiniowanej nazwie, typie wartości i wartości, równy bądź różny zadanemu)     10. test stanu usługi (uruchomiona/nieuruchomiona)     11. test obecności aplikacji (sprawdzenie czy aplikacja zdefiniowanej nazwie jest zainstalowana) 21. Wykorzystywany przez system Agent nie może wprowadzać zmian w działaniu aplikacji lub procesów systemu operacyjnego. 22. System musi mieć możliwość przeprowadzania różnych metod testowania w zależności od lokalizacji urządzenia w sieci, przynależności do grupy administracyjnej, parametru opisującego urządzenie lub użytkownika. 23. Podczas oceniania urządzenia końcowego musi być możliwość określenia alternatywnej polityki dostępu do zasobów w przypadku braku zgodności. 24. System musi mieć możliwość przeniesienia urządzenia do kwarantanny w przypadku braku komunikacji z agentem. 25. Na urządzeniu podlegającym kwarantannie musi zostać wyświetlona informacja o fakcie przeniesienia urządzenia do kwarantanny oraz informacja z wytycznymi o działaniach jakie użytkownik urządzenia musi podjąć w celu usunięcia niezgodności. 26. Administrator musi mieć możliwość określenia poziomu niezgodności z politykami, po którym będzie następowało przeniesienia stacji do kwarantanny. 27. System musi zapewniać integrację z rozwiązaniami bezpieczeństwa (platformy Firewall, systemy SIEM, systemy Antymalware, systemy MDM) na potrzeby oceny stanu urządzeń końcowych oraz określenia ich zgodności z polityką bezpieczeństwa NAC. Ocena stanu stacji końcowych musi być możliwa zarówno w trybie „pre-connect” przed udzieleniem dostępu do sieci, jak i w trybie „post-connect – po udzieleniu dostępu do sieci. 28. System musi zapewniać integrację z platformami typu Firewall w ramach której: 29. możliwy jest import stanu sesji urządzeń końcowych z platformy Firewall i wykorzystanie tych informacji jako danych wejściowych w konfiguracji metod profilowania urządzeń końcowych. 30. możliwe jest wykorzystanie funkcji rozpoznawania urządzeń końcowych przez platformę Firewall jako daną wejściową w konfiguracji metod profilowania urządzeń końcowych. 31. System musi zapewniać integrację z serwerem wdrażania, zarządzania, rejestrowania i monitorowania urządzeń końcowych w ramach której: 32. System NAC może gromadzić dane o urządzeniach końcowych (nazwa urządzenia końcowego, typ, system operacyjny, użytkownik, zgodność z polityką bezpieczeństwa) 33. System NAC może wykorzystać zgromadzone dane do rejestracji urządzenia końcowego.   **Profilowanie urządzeń**   1. System musi umożliwiać rozpoznawanie rodzaju urządzeń podłączonych do sieci lokalnej LAN i sieci bezprzewodowej WLAN poprzez analizę informacji pochodzących z co najmniej następujących źródeł: DHCP, Network Scan (NMAP), HTTP/HTTPS, SNMP, SSH, TCP, Telnet, UDP, ONVIF, WMI, OUI producenta, WinRM, WMI, Location, Agent, IP Range, Network Traffic. 2. System musi posiadać funkcję automatycznego profilowania urządzeń nieposiadających agenta 802.1x (suplikanta) na podstawie: DHCP, Network Scan (NMAP), HTTP/HTTPS, SNMP, SSH, TCP, Telnet, UDP, ONVIF, WMI, OUI producenta, WinRM, WMI, Location, Agent, IP Range, Network Traffic i przyznawania dostępu do sieci na podstawie zdefiniowanych polityk dostępu do sieci. 3. System musi umożliwiać dodawania rozpoznanych urządzeń do grup systemowych. 4. System na podstawie rodzaju rozpoznanego urządzenia musi umożliwiać różnicowanie poziomu dostępu. 5. System musi rozpoznawać co najmniej następujące rodzaje urządzeń:    * urządzenia z systemem Android,    * urządzenia Apple (iPad, iPhone, iPod)    * drukarki sieciowe,    * telefony IP,    * stacje robocza z systemem Microsoft Windows,    * stacje robocza z systemem MAC OS,    * stacje robocza z systemem Linux. 6. System musi posiadać funkcję wykrywanie nieautoryzowanych serwerów DHCP. 7. System musi posiadać funkcję wykrywania procesu NAT na urządzeniach końcowych.   **Logowanie, Raportowanie i Alarmowanie**   1. System musi zapewniać dane dla potrzeb audytu (dziennik zdarzeń). 2. System musi mieć możliwość generowania szczegółowego wykazu urządzeń podłączonych do sieci, zorganizowanego według typu urządzenia końcowego. 3. System musi rejestrować dane o atrybutach urządzeń końcowych i raportować zmiany w atrybutach np. przydział do VLAN-u, przyznany adres IP, klasyfikacja urządzenia w Systemie. 4. System musi zapewniać dane historyczne o zmianach stanu konfiguracji portów dostępowych. 5. System musi posiadać centralną bazę, zawierającą historyczne dane związane z operacjami zarządzania i procesem podłączanych urządzeń. Dane muszą być przechowywane i dostępne do analizy przez co najmniej 12 miesięcy. 6. System musi oferować możliwość tworzenia własnych szablonów raportów. 7. System musi umożliwiać logowanie do zewnętrznych serwerów logowania z wykorzystaniem Syslog. 8. System musi umożliwiać konfigurację generowanych alarmów i zautomatyzowanych akcji w oparciu o zdarzenia wewnętrzne np. w przypadku stwierdzenia zagrożenia na stacji, zablokowanie jej i powiadomienie administratora. 9. System musi umożliwiać przekazywanie informacji do systemów zewnętrznych poprzez mechanizm np. ODBC. 10. System NAC musi zapewniać integrację z modułem analizy i raportowania pochodzącym od tego samego producenta, w którym możliwe jest – oprócz logowania i raportowania – tworzenie reguł korelujących i alarmujących.   **Zarządzanie systemem**   1. System musi posiadać graficzny interfejs zarządzania – zarządzanie poprzez przeglądarkę internetową w wersji oferowanej przez producenta przeglądarki lub dedykowaną aplikację. 2. System musi umożliwiać uwierzytelnienie i autoryzację dostępu do interfejsu zarządzania w oparciu o wewnętrzną bazę użytkowników lub zewnętrzne repozytorium użytkowników (LDAP lub Radius). 3. System musi umożliwiać definiowanie zróżnicowanego poziomu dostępu do interfejsu zarządzania - RBA. 4. System musi umożliwiać zdefiniowanie co najmniej 3 administratorów z możliwością określenia praw dostępu do poszczególnych elementów systemu. 5. System musi umożliwiać personalizację wyglądu interfejsu zarządzania, w tym co najmniej zmianę koloru tła i czcionek, treści, grafiki. 6. System musi posiadać panel administracyjny, przedstawiający szczegółowy obraz stanu zabezpieczeń podłączonych lub próbujących się podłączyć urządzeń końcowych. 7. System musi posiadać możliwość tworzenia kopii zapasowej z wykorzystaniem SFTP.   **Zarządzanie dostępem gościnnym**   1. System musi umożliwiać przyznawanie dostępu gościnnego do sieci lokalnej LAN i sieci bezprzewodowej WLAN poprzez wypełnienie formularza w portalu rejestracyjnym. 2. System musi umożliwiać realizację usług BYOD dla urządzeń prywatnych pracowników. 3. Funkcja portalu rejestracyjnego powinna działać bez udziału lub przy minimalnym udziale pracowników IT. System powinien posiadać możliwość delegowania uprawnień do akceptowania kont gości przez pracowników nieposiadających uprawnień administracyjnych w Systemie. 4. Wsparcie dla linków akceptacyjnych generowanych z portalu sponsorskiego. 5. Rejestracja gości powinna umożliwiać powiązanie z bramką SMS celem wysyłania PIN-ów weryfikacyjnych. Wymagana jest obsługa PIN-ów składających się ze znaków alfanumerycznych i znaków specjalnych. 6. System musi umożliwiać przyznanie dostępu czasowego dla gości. 7. System musi umożliwiać dopasowanie wyglądu portalu logowania gościnnego, w tym co najmniej zmianę logo strony logowania, zmianę koloru tła i czcionek, treści, grafiki.   **Licencje i serwisy**   1. W ramach postępowania koniecznym jest dostarczenie 3000 licencji umożliwiających uruchomienie wszystkich wyżej wymienionych funkcji z zastosowaniem agenta na stacjach końcowych, z założeniem, że są one równocześnie podłączone do sieci lokalnej LAN i sieci bezprzewodowej WLAN. 2. Licencje w ramach rozwiązania powinny być dostarczone w modelu permanentnym. Zamawiający nie dopuszcza licencji bazujących na subskrypcji. 3. Dostarczony System NAC musi zawierać wszystkie niezbędne komponenty sprzętowe oraz programowe, na których możliwa będzie licencyjna rozbudowa do min. 5000 urządzeń równocześnie podłączonych do sieci lokalnej LAN i sieci bezprzewodowej WLAN, z uwzględnieniem instalacji agentowej. 4. Wsparcie: System musi być objęty serwisem producenta przez okres 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7. 5. System musi być dostarczony w modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.   **Opisy do wymagań ogólnych**   1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. 2. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.   **Rozszerzenie wymagań funkcjonalnych systemu NAC:**   1. W celu zapewnienia pełnej funkcjonalności oraz centralnego nadzoru nad środowiskiem kontroli dostępu w wielu lokalizacjach, konieczne jest uwzględnienie w ramach oferty dodatkowego komponentu umożliwiającego centralne zarządzanie systemem w architekturze rozproszonej, obejmującym do 50 serwerów odpowiedzialnych za kontrolę dostępu (tzw. serwery typu CA). Komponent ten musi pochodzić od tego samego producenta co pozostałe elementy oferowanego systemu NAC, być dostarczony jako zwirtualizowana platforma zgodna z wymaganiami dotyczącymi wspieranych hypervisorów (min. VMware vSphere, KVM, Microsoft Hyper-V) oraz umożliwiać integrację i centralne zarządzanie urządzeniami wskazanymi w opisie przedmiotu zamówienia 2. System jest objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania i wsparcie techniczne w trybie 24x7 przez dedykowany moduł internetowy oraz infolinię.   **Wdrożenie systemu**  W ramach realizacji zamówienia Wykonawca jest zobowiązany do kompleksowego wdrożenia **Systemu do zarządzania i monitorowania dostępu do sieci (NAC)**. Proces wdrożenia musi obejmować wszystkie poniższe etapy i czynności, zapewniając pełną funkcjonalność rozwiązania w infrastrukturze Zamawiającego.  **1. Instalacja i konfiguracja wstępna**   * **Instalacja platform wirtualnych:** Wymaga się instalacji i uruchomienia wszystkich komponentów Systemu NAC na serwerach wskazanych przez Zamawiającego, w posiadanym przez niego środowisku wirtualizacyjnym (VMware vSphere, KVM lub Microsoft Hyper-V). * **Aktualizacja oprogramowania:** Przed rozpoczęciem konfiguracji, Wykonawca musi zaktualizować oprogramowanie Systemu NAC do najnowszej, stabilnej wersji rekomendowanej przez producenta. * **Integracja z infrastrukturą:** Należy podłączyć i skonfigurować System NAC w celu zapewnienia pełnej i poprawnej komunikacji z infrastrukturą sieciową Zamawiającego (przełączniki LAN, sieć bezprzewodowa WLAN).   **2. Konfiguracja funkcjonalna i polityki bezpieczeństwa**  Wdrożenie musi objąć konfigurację wszystkich wymaganych funkcjonalności Systemu NAC, w szczególności:   * **Metody uwierzytelniania:** Konfiguracja mechanizmów uwierzytelniania urządzeń i użytkowników w oparciu o standard **802.1X**, **adres MAC** oraz **portal webowy (captive portal)**. * **Integracja z usługami katalogowymi:** Pełna integracja Systemu NAC z usługami **LDAP/Active Directory** oraz serwerami **RADIUS** Zamawiającego w celu autoryzacji. * **Profilowanie urządzeń:** Uruchomienie i dostrojenie mechanizmów automatycznego wykrywania i klasyfikacji urządzeń podłączanych do sieci (np. komputery, drukarki, telefony IP, urządzenia mobilne) na podstawie informacji z DHCP, SNMP, NMAP oraz analizy ruchu HTTP. * **Polityki dostępu:** Stworzenie w porozumieniu z Zamawiającym reguł i polityk bezpieczeństwa, które będą dynamicznie zarządzać dostępem do sieci, w tym m.in. przypisywać urządzenia do odpowiednich sieci VLAN lub izolować je w strefie kwarantanny. * **Ocena zgodności:** Skonfigurowanie weryfikacji stanu technicznego stacji końcowych (zarówno z użyciem agenta, jak i bezagentowo) pod kątem zgodności z polityką bezpieczeństwa (np. status oprogramowania antywirusowego, zapory systemowej, aktualizacji OS). * **Dostęp gościnny i BYOD:** Wdrożenie i personalizacja (logo, treść) portalu dla gości oraz przygotowanie polityk dostępu dla urządzeń prywatnych pracowników. * **Akceptacja konfiguracji:** Ostateczny zakres konfiguracji oraz zdefiniowane polityki muszą zostać zaakceptowane przez wyznaczonego administratora ze strony Zamawiającego.   **3. Szkolenie i dokumentacja**   * **Szkolenie administratorów:** Po zakończeniu prac wdrożeniowych Wykonawca jest zobowiązany przeprowadzić dedykowane szkolenie techniczne dla co najmniej dwóch administratorów Zamawiającego. Zakres szkolenia musi obejmować architekturę, administrację, konfigurację polityk, monitorowanie oraz generowanie raportów wdrożonego systemu. * **Dokumentacja powdrożeniowa:** Wykonawca ma obowiązek dostarczyć kompletną dokumentację techniczną wdrożonego rozwiązania w języku polskim. Dokumentacja musi szczegółowo opisywać architekturę systemu, wykonaną konfigurację oraz zaimplementowane polityki bezpieczeństwa.   **4. Warunki odbioru wdrożenia**  Odbiór prac wdrożeniowych zostanie potwierdzony protokołem odbioru po spełnieniu przez Wykonawcę wszystkich poniższych warunków:   * Zakończenie instalacji i konfiguracji wszystkich komponentów Systemu NAC. * Pozytywna weryfikacja przez Zamawiającego działania wszystkich wymaganych funkcjonalności. * Przeprowadzenie szkolenia dla administratorów. * Przekazanie kompletnej dokumentacji powdrożeniowej. |