Załącznik nr 5b do SWZ

RIR.271.1.2026

I. Przedmiot zamówienia

Podniesienie poziomu bezpieczeństwa cyfrowego Urzędu Miejskiego w Zabłudowie i Miejskiego Ośrodka Pomocy Społecznej w Zabłudowie poprzez wykonanie klastra serwerów i macierzy, segmentację sieci LAN, systemu backupu i archiwizacji, wdrożenie systemu ochrony sieci, komputerów i serwerów, wdrożenie zapasowych systemów zasilania w postaci zasilaczy UPS, zakup usług eksperckich i szkoleń realizowanych w ramach programu grantowego „Cyberbezpieczny Samorząd".

II. Ogólny zakres przedmiotu zamówienia

Przedmiot zamówienia obejmuje:

1. Zakup urządzeń i licencji oraz wdrożenie systemu ochrony sieci oraz ochrony komputerów i serwerów na potrzeby Urzędu Miejskiego w Zabłudowie (UM) oraz Gminnego Ośrodka Pomocy Społecznej w Zabłudowie (GOPS).
2. Podniesienie bezpieczeństwa zasobów i systemów informatycznych poprzez zakup, konfigurację i instalację klastra serwerów i macierzy wraz z dedykowanym serwerowym systemem operacyjnym oraz licencjami dostępowymi użytkowników do zasobów serwerowych.
3. Zakup, instalację i konfigurację przełączników sieciowych do segmentacji sieci LAN/SAN w UM i GOPS.
4. Wykonanie systemu do tworzenia kopii bezpieczeństwa danych IT poprzez zakup serwerów plików NAS i oprogramowania do tworzenia kopii zapasowych oraz archiwizacji.
5. Zakup systemu zasilania zapasowego w postaci zasilaczy UPS.
6. Zakup specjalistycznych usług eksperckich w zakresie instalacji, uruchomienia i konfiguracji oraz wsparcia powdrożeniowego zakupionych urządzeń i oprogramowania oraz wykonania dokumentacji technicznej opisującej parametry konfiguracji.
7. Szkolenia specjalistyczne dla informatyków w zakresie wdrożonych systemów przez osobę z doświadczeniem w zakresie szkoleń w zakresie przedmiotu zamówienia, doświadczenie w zakresie szkoleń w dziedzinie przedmiotu zamówienia co najmniej 2 lata.

III. Szczegółowe wymagania w zakresie realizacji przedmiotu zamówienia

W ramach realizacji przedmiotu zamówienia Zamawiający wymaga realizacji poniższych dostaw i usług:

1. **Zakup urządzeń i licencji oraz wdrożenie systemu ochrony sieci oraz ochrony komputerów i serwerów na potrzeby Urzędu Miejskiego w Zabłudowie (UM) oraz Gminnego Ośrodka Pomocy Społecznej w Zabłudowie (MOPS).**

W ramach realizacji przedmiotu zamówienia Zamawiający wymaga dostarczenie i uruchomienia kompleksowego systemu zapewniającego ochronę sieci lokalnych UM oraz MOPS przed zagrożeniami ze strony Internetu, stworzenie bezpiecznego dostępu do sieci lokalnych jednostek w oparciu o technologię VPN, a także dostawę licencji i

wdrożenie systemu klasy XDR do ochrony urządzeń końcowych (komputerów i serwerów).

Zakres wdrożenia powinien obejmować:

a. Opracowanie założeń ochrony sieci od strony Internetu i bezpiecznego połączenia sieci lokalnych UM i MOPS na potrzeby wymiany danych informatycznych i uruchomienia systemu backup oraz archiwizacji.
b. Dostawę, instalację i konfigurację klastra urządzeń UTM do ochrony sieci w budynku UM
c. Dostawę, instalację i konfigurację wyniesionego urządzenia UTM do ochrony sieci w MOPS.
d. Konfigurację bezpiecznego połączenia sieciowego przez Internet z wykorzystaniem dostarczonych urządzeń w celu połączenia sieci lokalnej UM z siecią MOPS na potrzeby wymiany danych systemów informatycznych i uruchomienia systemu backup oraz archiwizacji.
e. Konfigurację dostępu VPN do zasobów sieci UM i sieci MOPS na potrzeby administratorów oraz co najmniej 5 użytkowników.
f. Dostawę licencji oraz konfigurację systemu ochrony typu XDR do ochrony 70 urządzeń końcowych (komputery w sieci UM i MOPS) na okres co najmniej 36 miesięcy, jednak nie krótszy niż okres trwania subskrypcji ochrony zadeklarowany w formularzu oferty.
g. Dostawę licencji oraz konfigurację systemu ochrony typu XDR do ochrony 10 serwerów (maszyn fizycznych lub wirtualnych) na okres co najmniej 36 miesięcy, jednak nie krótszy niż okres trwania subskrypcji ochrony zadeklarowany w formularzu ofertowym.
h. Przeprowadzenie szkoleń administratorów w zakresie zarządzania i administrowania wdrożonych systemów.
i. W ramach świadczonych usług instalacyjnych i konfiguracyjnych zapewnienie wsparcia wdrożeniowego i powdrożeniowego w opisanym zakresie.

Wraz z urządzeniami Wykonawca powinien dostarczyć wymagane okablowanie połączeniowe.
Zamawiający zapewni miejsce do instalacji urządzeń UTM w szafach rack 19” w serwerowni UM oraz MOPS. Wszystkie ww. dostarczane i wdrażane urządzenia (klaster UTM, wyniesione urządzeni UTM) oraz systemy ochrony typu XDR do urządzeń końcowych i serwerów powinny być zarządzane z jednej centralnej konsoli chmurowej oferowanej przez producenta. Dostarczone systemy ochrony powinny współpracować w zakresie ochrony sieci i aktywnej reakcji na zagrożenia.
Dostarczone wraz z urządzeniami i systemami licencje powinny zapewniać korzystanie ze wszystkich zaoferowanych funkcjonalności, w tym możliwość zarządzania i konfigurowania z centralnej konsoli wszystkich dostarczonych produktów przez okres trwania subskrypcji ochrony zadeklarowany w formularzu ofertowym, bez potrzeby zakupu dodatkowych licencji np. dostępu do konsoli, aktywacji poszczególnych funkcjonalności, współpracy w zakresie ochrony sieci i aktywnej reakcji na zagrożenia itp.
Zamawiający nie dopuszcza dostawy niezależnych i niezależnie zarządzanych produktów UTM i systemu XDR.

Szczegółowe wymagania minimalne dla urządzenia UTM do ochrony sieci w budynku UM określone zostały w tabeli nr 1

Szczegółowe wymagania minimalne dla urządzenia wyniesionego UTM do ochrony sieci w MOPS określone zostały w tabeli nr 2.
Dostarczone licencje systemu XDR do ochrony urządzeń końcowych i serwerów powinny spełniać wymagania minimalne określone w tabeli nr 3.

2. Podniesienie bezpieczeństwa zasobów i systemów informatycznych poprzez zakup, konfigurację i instalację klastra serwerów i macierzy wraz z dedykowanym serwerowym systemem operacyjnym oraz licencjami dostępowymi użytkowników do zasobów serwerowych.

Aktualnie w serwerowniach w budynku UM i MOPS Zamawiający posiada serwery fizyczne, na których zainstalowane są systemy informatyczne.

W ramach realizacji przedmiotu zamówienia Zamawiający wymaga:

a. Opracowanie założeń rekonfiguracyjnych sieci urzędu z wydzieleniem dedykowanych podsieci opartych na VLAN (podsieć SAN, podsieć zarządzania, podsieć dostępowa) na potrzeby podłączenia dostarczanych urządzeń i systemów.
b. Dostawy, instalacji, uruchomienia i konfiguracji 2 nowych serwerów przeznaczonych do pracy w klastrze wysokiej dostępności (HA) z macierzą dyskową dwukontrolerową, połączonych przez dedykowaną siec SAN iSCSI 10 GB Ethernet.
c. Dostawy i instalacji na nowych serwerach serwerowego systemu operacyjnego wraz z licencjami umożliwiającymi korzystanie użytkowników z zasobów informacyjnych lub usług udostępnianych przez te serwery.
d. Dostawa licencji serwerowego systemu operacyjnego do aktualizacji istniejącego systemu operacyjnego.
e. Uruchomienie i konfiguracje systemu wirtualizacji na dostarczonym klastrze serwerów wraz z instalacją i uruchomieniem na maszynach wirtualnych dostarczanych w ramach przedmiotu zamówienia systemów.
f. Wykonanie instalacji serwerowego systemu operacyjnego i konfiguracji kontrolera domenowego Active Directory na serwerze udostępnionym przez Zamawiającego.
g. W ramach świadczonych usług instalacyjnych i konfiguracyjnych zapewnienie wsparcia wdrożeniowego i powdrożeniowego w opisanym zakresie.

Wraz z serwerami i macierzą Wykonawca powinien dostarczyć:

- 4 komplety modułów połączeniowych SFP+ 10 GbE (elektryczne lub optyczne wraz z przewodami połączeniowymi lub kable DAC kompatybilne z dostarczanymi urządzeniami), niezbędne do podłączenia portów LAN serwerów do przełączników dostępowych w sieci LAN urzędu;
- 4 komplety modułów połączeniowych SFP+ 10 GbE (elektryczne lub optyczne wraz z przewodami połączeniowymi lub kable DAC kompatybilne z dostarczanymi urządzeniami), niezbędne do wykonania podłączeń SAN serwerów i macierzy.
- niezbędne kable Ethernet i zasilające do podłączenia dostarczanych urządzeń.

Wykonawca wykona instalację i konfigurację nowego środowiska klastra serwerów, macierzy i sieci SAN.
Zamawiający zapewni miejsce do instalacji urządzeń w szafach rack 19” w serwerowni.

Szczegółowe wymagania minimalne dla serwerów w trybie HA określone zostały w tabeli nr 4.
Szczegółowe wymagania minimalne dla serwerowego systemu operacyjnego określone zostały w tabeli nr 5.
Szczegółowe wymagania minimalne dla macierzy sieciowej określone zostały w tabeli nr 6.

3. Zakup, instalację i konfigurację przełącznika sieciowego do segmentacji sieci LAN MOPS

W ramach realizacji przedmiotu zamówienia wykonawca:
a. Dostarczy, zainstaluje i skonfiguruje 1 zarządzalny przełącznik sieciowy do MOPS.
b. W ramach świadczonych usług instalacyjnych i konfiguracyjnych zapewnienie wsparcia wdrożeniowego i powdrożeniowego w opisanym zakresie.

Zamawiający zapewni miejsce do instalacji urządzeń w szafach rack 19” w MOPS.
Wykonawca powinien skonfigurować dostarczone przełączniki w celu utworzenia wydzielonych podsieci z sieci LAN (w ty, podsieci biurowej,wi-fi, zarządzania, itp.).
Szczegółowe wymagania minimalne dla przełącznika sieciowego do segmentacji sieci LAN w MOPS określone zostały w tabeli nr 7.

4. Zakup, instalację i konfigurację przełączników sieciowych do segmentacji sieci SAN w urzędzie

W ramach realizacji przedmiotu zamówienia wykonawca:
a. Dostarczy, zainstaluje i skonfiguruje 2 zarządzalny przełączniki sieciowe do serwerowni urzędu w celu utworzenia wydzielonej sieci SAN do podłączenia nowego klastra serwerów i macierzy.
b. W ramach świadczonych usług instalacyjnych i konfiguracyjnych zapewnienie wsparcia wdrożeniowego i powdrożeniowego w opisanym zakresie.

Zamawiający zapewni miejsce do instalacji urządzeń w szafach rack 19”.
Wykonawca powinien skonfigurować dostarczone przełączniki w celu utworzenia wydzielonych podsieci z sieci LAN (w ty, podsieci biurowej, WI-FI, zarządzania, itp.).
Szczegółowe wymagania minimalne dla przełączników sieciowych do segmentacji sieci AAN w urzędzie określone zostały w tabeli nr 8.

5. Wykonanie systemu do tworzenia kopii bezpieczeństwa danych IT poprzez zakup serwerów plików NAS, biblioteki taśmowej i oprogramowania do tworzenia kopii zapasowych

W ramach realizacji przedmiotu zamówienia Wykonawca powinien:
a. Opracowanie założeń i konfiguracji systemu kopii bezpieczeństwa danych w sieci UM i MOPS na potrzeby wymiany danych i uruchomienia systemu backup, z

wykorzystaniem dostarczanych w ramach przedmiotu zamówienia urządzeń i oprogramowania.

b. Dostawę, instalację i konfigurację serwera plików NAS do serwerowni urzędu.
c. Dostawę, instalację i konfigurację biblioteki taśmowej wraz z kartą SAS i kablem SAS do podłączenia biblioteki.
d. Dostawę licencji oprogramowania do backup maszyn wirtualnych z dostarczonego klastra serwerów w trybie HA oraz **70 komputerów**.
e. Przygotowanie procedury wykonania kopii zapasowych na serwerze plików NAS wykonanie procedury przywracania danych i systemów z kopii zapasowych.
f. Przygotowanie procedury wykonania archiwizacji na bibliotece taśmowej wykonanie procedury przywracania danych i systemów z kopii.
g. W ramach świadczonych usług instalacyjnych i konfiguracyjnych zapewnienie wsparcia wdrożeniowego i powdrożeniowego w opisanym zakresie.

Szczegółowe wymagania minimalne dla serwerów plików NAS do urzędu określone zostały w tabeli nr 9 .
Szczegółowe wymagania minimalne dla oprogramowania do backup określone zostały w tabeli nr 10.
Szczegółowe wymagania minimalne dla biblioteki taśmowej określone zostały w tabeli nr 11.

6. Zakup systemu zasilania zapasowego w postaci zasilaczy UPS

W ramach realizacji przedmiotu zamówienia Wykonawca powinien:

a. Dostarczyć zainstalować i skonfigurować zasilacz awaryjny UPS z dodatkowym dedykowanym modułem bateryjnym do serwerowni urzędu.
b. Dostarczyć zainstalować i skonfigurować zasilacz awaryjny UPS z dodatkowym dedykowanym modułem bateryjnym do serwerowni MOPS.

Szczegółowe wymagania minimalne dla zasilacza awaryjnego UPS określone zostały w tabeli nr 12.

7. Dostawa licencji i wdrożenie systemu do monitorowania infrastruktury teleinformatycznej

Wykonawca powinien dostarczyć licencje oraz zainstalować na maszynach wirtualnych na dostarczonym klastrze serwerów i skonfigurować system inwentaryzacji i monitorowania zasobów teleinformatycznych w sieci LAN urzędu.

Dostarczone oprogramowanie powinno posiadać bezterminową licencję na użytkowanie oraz co najmniej 36 -miesieczne wsparcie producenta dla dostarczonego oprogramowania.
Szczegółowe wymagania minimalne dla systemu inwentaryzacji i monitorowania zasobów teleinformatycznych określone zostały w tabeli nr 13.

8. Zakup specjalistycznych usług eksperckich w zakresie instalacji, uruchomienia i konfiguracji i wsparcia powdrożeniowego zakupionych urządzeń i oprogramowania

Wraz z dostarczonymi urządzeniami i systemami Wykonawca powinien wykonać specjalistyczne usługi eksperckie w zakresie:

a. Instalacji i konfiguracji centralnej konsoli oraz systemów ochrony sieci UTM i ochrony urządzeń końcowych i serwerów zgodnie z wymaganiami opisanymi w pkt. 1.
b. Wykonania instalacji dostarczanych klastrów serwerów i macierzy oraz konfigurację środowiska domenowego Active Directory zgodnie z wymaganiami opisanymi w pkt. 2.
c. Instalacji i konfiguracji dostarczonych przełączników LAN i SAN zgodnie z wymaganiami opisanymi w pkt. 3 i 4.
d. Wdrożenia systemu kopii bezpieczeństwa poprzez instalację i konfigurację serwera plików NAS, biblioteki taśmowej oraz oprogramowania do systemu kopi bezpieczeństwa serwerów i komputerów zgodnie z wymaganiami opisanymi w pkt. 5.
e. Wdrożenie systemu do monitorowania infrastruktury teleinformatycznej zgodnie z wymaganiami opisanymi w pkt. 7.
f. Montaż zasilaczy UPS.

Zakres usług wsparcia powdrożeniowego powinien obejmować **co najmniej 32 roboczogodzin**, przy czym usługi te świadczone będą na potrzeby poszczególnych systemów i rozliczane łącznie w ramach puli roboczogodzin przewidzianej na wsparcie powdrożeniowe.
Usługi eksperckie wsparcia powdrożeniowego realizowane powinny być wg następujących wymagań:

1) Zakres realizacji usług wsparcia powdrożeniowego powinien obejmować usługi eksperckie IT w zakresie konfiguracji, zmian i modyfikacji konfiguracji, instalacji systemów operacyjnych i konfiguracji maszyn wirtualnych, zmian konfiguracji dostarczonych urządzeń (UTM, przełączniki sieciowe, serwery, macierz, NAS), systemów ochrony, systemów backu.
2) Usługi wsparcia powdrożeniowego dla każdego z ww. elementów/systemów realizowane będą w okresie od zakończenia wdrożenia danego elementu/systemu, potwierdzonego protokołem odbioru częściowego do dnia 15.09.2026 r.
3) Zamawiający uprawniony będzie do zgłaszania Wykonawcy potrzeb wykonania usług w dni robocze w godzinach 8 – 16.
4) Wykonawca każdorazowo rozpocznie świadczenie usług wsparcia powdrożeniowego z zachowaniem czasu reakcji wsparcia, określonego jako okres, od momentu zgłoszenia przez przedstawiciela Zamawiającego potrzeby i zakresu wykonania usługi wsparcia powdrożeniowego, do momentu przeprowadzenia przez Wykonawcę pierwszej czynności w ramach zgłoszonego wsparcia powdrożeniowego, nie mniej niż 32 godz. robocze.
5) Zakres i tryb świadczenia usług wsparcia powdrożeniowego nie obejmuje świadczenia usług obsługi zgłoszeń i napraw gwarancyjnych.

9. Przeprowadzenie szkoleń specjalistycznych w zakresie wdrożonych systemów

Wraz z dostarczonymi urządzeniami i systemami Wykonawca powinien przeprowadzić szkolenia administratorów Zamawiającego, tj.:

a. Szkolenie z zakresu konfiguracji i administracji urządzeń UTM i konsoli do zarządzania – co najmniej 24-godzinne szkolenie obejmujące część teoretyczną i warsztatową.
b. Szkolenie z zakresu konfiguracji i administrowania systemu XDR ochrony urządzeń końcowych i konsoli do zarządzania – co najmniej 24-godzinne szkolenie obejmujące część teoretyczną i warsztatową.
c. Szkolenie z zakresu konfiguracji i administrowania systemu do monitorowania infrastruktury teleinformatycznej – co najmniej 8-godzinne szkolenie obejmujące część teoretyczną i warsztatową.

Zamawiający dopuszcza możliwość przeprowadzania części warsztatowych szkoleń z wykorzystaniem dostarczonych i zainstalowanych systemów.

Wszystkie szkolenia prowadzone powinny być w języku polski. W szkoleniach uczestniczyć będą administratorzy systemów IT Zamawiającego.

Szkolenia z systemów ochrony ruchu sieciowego UTM, ochrony urządzeń końcowych XDR powinno być realizowane wg. programów autoryzowanych przez producenta oferowanych systemów oraz powinny być przeprowadzone przez producenta lub autoryzowany ośrodek szkoleniowy producenta w Polsce. Trener prowadzący szkolenie powinien posiadać wymagane przez producenta autoryzacje i certyfikacje do prowadzenia szkoleń w wymaganym zakresie.
Zamawiający nie dopuszcza przeprowadzenia ww. szkoleń przez osoby nie posiadające wymaganych autoryzacji i certyfikatów producenta.

10. Dokumentacja

Do dnia zgłoszenia do odbioru częściowego każdego z elementów przedmiotu zamówienia Wykonawca zobowiązany jest dostarczyć Zamawiającemu dokumentację powykonawczą obejmującą odpowiednio:

a. Opis, miejsce instalacji i parametry konfiguracji, schematy sieciowe wdrożonych systemów.
b. Opis miejsce instalacji i parametry konfiguracji dostarczonych urządzeń.
c. Deklarację zgodności UE (lub dokument równoważny) dostarczonych urządzeń.

Deklaracja powinna obejmować spełnienie wymaganych dyrektyw i norm zharmonizowanych zgodnie z:

- Dyrektywą kompatybilności elektromagnetycznej EMC 2014/30/EU z dnia 26 lutego 2014 roku.
- Dyrektywą w sprawie ograniczenia stosowania niektórych niebezpiecznych substancji w sprzęcie elektrycznym i elektronicznym 2011/65/EU z dnia 8 czerwca 2011 roku.
- Dyrektywą Niskiego Napięcia 2014/35/UE z dnia 26 lutego 2014 roku.
-

IV. Szczegółowe wymagania w zakresie minimalnych parametrów technicznych dostarczonych urządzeń, systemów i oprogramowania

Zaoferowany urządzenia, systemy i oprogramowanie powinny spełniać wymagania minimalne określone w poniższych tabelach.

Tabela nr 1.
Szczegółowe wymagania minimalne dla urządzeń UTM skonfigurowanych w klastrze do ochrony sieci w budynku Urzędu Miejskiego w Zabłudowie

Urządzenia UM do ochrony sieci – 1 kpl. **Miejsce instalacji: infrastruktura serwerowni UM**	
Nazwa parametru	**Minimalne wymagania**
Typ i ilość	Dwa niezależne urządzenia fizyczne UTM skonfigurowane w klastrze wysokiej dostępności do pracy w trybie Active-Passive. Zamawiający nie dopuszcza stosowania UTM zainstalowanych w postaci maszyn wirtualnych (VM).
Zastosowanie	Ochrona na brzegu sieci LAN
Wymagania licencyjne i czas trwania subskrypcji ochrony i zarządzania	Zamawiający wymaga dostarczenia licencji ochrony w modelu subskrypcyjnym. Licencje ochrony powinny umożliwiać korzystanie ze wszystkich wymagane w niniejszej tabeli funkcjonalność, tj. w zakresie zarządzania, zapory sieciowej, koncentratora VPN, zapobiegania włamaniom i zaawansowana ochrona przed zagrożeniami, ochrony i kontroli ruchu WEB, ochrony przed nieznanymi zagrożeniami, integracji z rozwiązaniami XDR, ochrony DNS, logowania i raportowania. Wraz z urządzeniami powinny być dostarczone licencje zapewniające możliwość konfiguracji i zarządzania dostarczonymi urządzeniami UTM z centralnej konsoli chmurowej producenta z możliwością retencji analizy logów z urządzeń UTM przez okres co najmniej 12 miesięcy wstecz. Okres trwania subskrypcji licencji ochrony do urządzeń UTM powinien wynosić co najmniej 36 miesięcy, jednak powinien być nie krótszy niż okres trwania subskrypcji ochrony zadeklarowany w formularzu oferty. W okresie trwania subskrypcji powinna być: - możliwość kontaktu ze wsparciem producenta w trybie 24/7 przez różne kanały (co najmniej telefonicznie, zgłoszenia przez portal web, chat) w celu uzyskania wsparcia producenta w zakresie rozwiązywania problemów działaniem systemu; - możliwość aktualizacji oprogramowania układowego i pobierania poprawek; - wymiany uszkodzonego urządzenia.
Liczba i typ interfejsów fizycznych w pojedynczym UTM	Co najmniej: 4 x 1GbE 2 x 2.5 GbE 2 x 10 GbE SFP+ 2 x USB 3.0 1 x USB 2.0
Interfejsy zarządzania	1 x RJ45 COM 1 x COM Micro-USB Diody LED na przednim panelu z podstawowymi informacjami statusowymi i konfiguracyjnymi.
Parametry wydajnościowe klastra Active-Passive	Co najmniej: - Minimalna liczba i typ interfejsów wirtualnych: 100 (IEEE 802.1Q) - Minimalna liczba nowych połączeń na sekundę: 100 000 - Minimalna liczba jednoczesnych połączeń 6 500 000

	- Minimalna przepustowość Firewall: 19 Gbps - Przepustowość firewall IMIX: 10 Gbps - Minimalna przepustowość IPS: 5 Gbps - Minimalna przepustowość Threat Protection: 4 Gbps - Minimalna przepustowość VPN IPsec: 6 Gbps - Minimalna liczba jednoczesnych tuneli SSL VPN: 1 500 - Minimalna przepustowość SSL/TLS Inspection: 1 700 Mbps - Minimalna liczba jednoczesnych połączeń SSL/TLS 18 000 - Ilość użytkowników nielimitowana - Zintegrowany podwójny dysk SSD do przechowywania oprogramowania, logowania i raportowania o pojemności nie mniejszej niż 64GB.
Wymagania systemu zarządzania	Rozwiązanie powinno mieć możliwość administrowania: - z poziomu centralnej konsoli chmurowej, która oprócz UTM zapewnia możliwość zarządzania pozostałymi zaoferowanymi komponentami systemów bezpieczeństwa, co najmniej takimi jak zaawansowana ochrona urządzeń końcowych XDR, ochrona serwerów oraz dodanie do zarządzania systemów tj. ochrony urządzeń mobilnych, ochrony poczty e-mail, itp. - za pośrednictwem nowoczesnego, graficznego interfejsu webowego (Web GUI), który działa w trybie rzeczywistym, umożliwiając bieżące zarządzanie i natychmiastowe reagowanie na zmiany w systemie, rozwiązanie powinno oferować narzędzia diagnostyczne takie jak co najmniej: ping, traceroute, name lookup, route lookup. Interfejs graficzny powinien zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych, wyświetlania tablicy ARP/NDP. Webowy graficzny interfejs administratora powinien być zabezpieczony za pomocą protokołu HTTPS, wykorzystując domyślnie certyfikat typu self-signed, z opcją jego zastąpienia certyfikatem wydanym i podpisanym przez renomowanego, zewnętrznego wystawcę zaufania (External Trusted CA). Urządzenie UTM powinno oferować możliwość konfiguracji przez wiersz poleceń dostępny z poziomu interfejsu graficznego urządzenia, portu konsolowego oraz za pośrednictwem bezpiecznego protokołu SSH. System powinien wdrażać zaawansowany mechanizm dwuskładnikowego uwierzytelniania, oparty na tokenach sprzętowych lub programowych, zgodnych ze standardem RFC6238 (Time-Based One-Time Password Algorithm), zapewniając tym samym wysoki poziom ochrony zarówno dla dostępu do interfejsu Web GUI, jak i połączeń VPN. Rozwiązanie powinno oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych urządzenia na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. System UTM powinien oferować intuicyjny, samoobsługowy portal dla użytkowników końcowych, który odciąża administratorów poprzez redukcję liczby rutynowych zadań, przy czym dostęp do portalu powinien być chroniony dwuskładnikowym uwierzytelnianiem zgodnym ze standardem RFC6238 (Time-Based One-Time Password Algorithm). System powinien oferować opcję automatycznego wylogowania administratora po zdefiniowanym czasie bezczynności. System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła.

	System powinien być wyposażony w funkcjonalność rejestrowania i śledzenia wszystkich zmian w konfiguracji (tzw. changelog), co umożliwia pełną kontrolę nad historią modyfikacji i ułatwia audytowanie działań administracyjnych System powinien oferować mechanizm blokady kolejnych połączeń w przypadku prób nieautoryzowanego dostępu do interfejsu do zarządzania. Liczba takich prób oraz czas blokady powinny być swobodnie definiowane przez administratora. Rozwiązanie powinno zapewniać elastyczne i granularne zarządzanie dostępem do usług administracyjnych w zależności od stref zapory sieciowej, co pozwala na precyzyjne dostosowanie uprawnień do specyfiki danej infrastruktury sieciowej. System powinien oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników, klient, serwer z możliwością wykorzystania ich do budowy polityk bezpieczeństwa. Dodawanie tego typu obiektów powinno być możliwe bezpośrednio podczas tworzenia dowolnej polisy bezpieczeństwa. System powinien oferować mechanizm pozwalający na śledzenie zmian w konfiguracji. Rozwiązanie powinno zapewniać elastyczne zarządzanie dostępem do usług administracyjnych na poziomie stref zapory sieciowej. System powinien dysponować mechanizmem automatycznego wysyłania powiadomień za pośrednictwem bezpiecznego protokołu SMTPS (z obsługą STARTTLS lub SSL/TLS). Rozwiązanie powinno wspierać kompleksowe monitorowanie stanu pracy w oparciu o protokoły SNMP w wersjach v1, v2c oraz v3. System powinien zapewniać monitorowanie w czasie rzeczywistym stanu urządzenia (użycie CPU, RAM, HDD, obciążenie interfejsów sieciowych). System powinien oferować możliwość integracji z centralnym systemem do zarządzania. Wymagane jest, aby rozwiązanie oferowało wbudowany mechanizm do tworzenia kopii zapasowych konfiguracji z zapisem do pliku lokalnego lub via email. Rozwiązanie powinno oferować mechanizm pozwalający na automatyczne tworzenie kopii zapasowych w odstępach czasowych: codziennie, raz w tygodniu lub raz w miesiącu. Rozwiązanie powinno zapewnić możliwość uruchomienia zdalnego dostępu dla pracowników wsparcia technicznego bez konieczności tworzenia czy modyfikowania polis zapory sieciowej. Zarządzanie licencjami i subskrypcjami powinno odbywać się za pośrednictwem centralnej konsoli administracyjnej. Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware). System ochrony powinien pracować w klastrze złożonym z dwóch urządzeń w celu zapewnienia wysokiej dostępności w trybie Active-Passive oraz posiadać możliwość rozbudowy do klastra Active-Active przez zakup licencji.
Wymagania Zapory sieciowej	Niezbędne jest, aby zapora sieciowa funkcjonowała w oparciu o zaawansowany mechanizm Stateful Packet Inspection.

	System musi zapewniać możliwość tworzenia całkowicie odrębnych, autonomicznych zestawów reguł dedykowanych dla protokołów IPv4 oraz IPv6, bez jakichkolwiek zależności między nimi. Rozwiązanie powinno umożliwiać budowanie polis w oparciu o takie obiekty jak sieć, usługa, użytkownik, grupa użytkowników lub czas. System powinien umożliwiać budowanie polis bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe. Polisy zapory powinny umożliwiać egzekwowanie ruchu dla poszczególnych stref, sieci lub usług. Rozwiązanie powinno zapewniać możliwość tworzenia polis w oparciu o relacje między strefami zapory sieciowej. Konieczne jest, aby system oferował opcję tymczasowego wyłączania wybranych reguł zapory sieciowej, przy jednoczesnym zachowaniu ich w konfiguracji, bez potrzeby trwałego usuwania. System powinien wspierać kompleksowe grupowanie reguł zapory, z dodaną funkcją automatycznego przypisywania nowo tworzonych reguł do odpowiednich grup na podstawie zdefiniowanych cech opisujących te grupy. Rozwiązanie musi gwarantować możliwość opracowywania polityk w oparciu o dynamiczne relacje między różnymi strefami zapory sieciowej, odzwierciedlając ich wzajemne zależności. System ochrony powinien być wyposażony w fabrycznie zdefiniowane strefy zapory, takie jak LAN, WAN, DMZ czy VPN. Rozwiązanie ma oferować pełną elastyczność w definiowaniu niestandardowych, autorskich stref zapory sieciowej, dostosowanych do specyficznych potrzeb użytkownika. System musi umożliwiać blokowanie ruchu sieciowego w oparciu o geolokalizację IP, precyzyjnie określając kraj pochodzenia i stosując odpowiednie restrykcje. Rozwiązanie powinno dostarczać zaawansowane narzędzie do przeprowadzania symulacji działania reguł zapory, uwzględniając kryteria zdefiniowane przez administratora, takie jak adres IP, strefa zapory, użytkownik, dzień czy godzina. System powinien pozwalać na dynamiczne filtrowanie widoku zestawu reguł, umożliwiając ich selekcję na podstawie dowolnego elementu składowego, zgodnie z potrzebami administratora.
Wymagania Koncentratora VPN	System ma obsługiwać połączenia IPsec zabezpieczone szyfrowaniem AES256 w połączeniu z funkcją skrótu SHA512, wykorzystując przy tym grupy kluczy Diffie-Hellman o najwyższej sile, takie jak 19 (ecp256), 21 (ecp521) czy 31 (curve25519) Urządzenie musi oferować mechanizmy Full Tunnel oraz Split Tunnel dla połączeń IPsec client-to-site VPN jak i SSL client-to-site VPN. Rozwiązanie musi oferować mechanizmy IPsec VPN Failover i Failback. System powinien być wyposażony w zaawansowane mechanizmy ciągłego monitorowania i podtrzymywania aktywności tuneli IPsec site-to-site VPN, zapewniając ich niezawodność i stabilność w czasie rzeczywistym. Rozwiązanie musi dostarczać mechanizmy przełączania awaryjnego (Failover) oraz powrotu do stanu pierwotnego (Failback) dla tuneli IPsec VPN, minimalizując ryzyko przerw w łączności. Producent powinien udostępniać bezpłatne, w pełni funkcjonalne oprogramowanie klienckie VPN, umożliwiające realizację połączeń zarówno IPsec client-to-site VPN, jak i SSL client-to-site VPN, bez dodatkowych kosztów dla użytkownika.

	System musi umożliwiać konfigurację połączeń typu IPsec site-to-site VPN dla IKE v1 oraz IKE v2.
Logowanie i raportowanie	System musi umożliwiać monitorowanie logów ruchu w czasie rzeczywistym. System powinien umożliwiać składowanie oraz archiwizację logów bezpośrednio w urządzeniu oraz z poziomu centralnej konsoli chmurowej. Okres przechowywania logów i raportowania z centralnej konsoli chmurowej powinien wynosić **co najmniej 12 miesięcy**. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. Rozwiązanie musi zapewniać narzędzie do graficznej analizy logów. Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa. System powinien zapewniać monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników np. klasyfikując ryzyko wg. skali. System powinien zapewniać przeglądanie logów przy zastosowaniu funkcji filtrujących. Rozwiązanie powinno umożliwiać wysyłanie raportów via email. Rozwiązanie powinno umożliwiać eksport raportów do plików PDF, HTML i CSV. Rozwiązanie powinno oferować możliwość wysyłania logów systemowych do co najmniej 3 serwerów syslog. System powinien zapewniać podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym lub rocznym dla wszystkich lub indywidualnego łącza. System powinien zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP lub aplikację. Rozwiązanie powinno oferować możliwość zanonimizowania danych w raportach. System powinien umożliwiać automatyczne tworzenie raportów według kryteriów i harmonogramów określonych przez administratora.
System zapobiegania włamaniom i zaawansowana ochrona przed zagrożeniami	Ochrona IPS musi opierać się co najmniej na analizie protokołów i bazie minimum 5000 sygnatur. Wymagane jest, aby system automatycznie aktualizował sygnatury zagrożeń. Rozwiązanie powinno umożliwiać tworzenie własnych sygnatur IPS. Rozwiązanie powinno umożliwiać selektywne wskazywanie sygnatur i/lub grup sygnatur dla tworzonych przez administratora polis IPS. System ochrony powinien zapewniać wykrywanie, blokowanie i raportowanie prób połączeń z serwerami Command & Control / Botnet.
Ochrona i kontrola web	Rozwiązanie powinno działać jako Transparent Web Proxy zapewniając ochronę przed niebezpiecznymi treściami i szkodliwym oprogramowaniem dystrybuowanym przez HTTP, HTTPS i FTP. Rozwiązanie powinno wykorzystywać silnik antywirusowy pochodzący bezpośrednio od producenta rozwiązania. Dodatkowo rozwiązanie powinno umożliwiać uruchomienie silnika antywirusowego firmy trzeciej. Wymagane jest, aby system automatycznie aktualizował sygnatury zagrożeń. System powinien filtrować pliki na podstawie tak rozszerzeń jak i nagłówków MIME. Rozwiązanie musi zapewniać filtrowanie aktywnych treści takich jak ActiveX, apletów Java czy ciasteczek. Rozwiązanie musi przeprowadzać emulację skryptów Java. Rozwiązanie powinno przeprowadzać tzw. live-lookups tj.. w trybie rzeczywistym weryfikować bazę zagrożeń producenta. Rozwiązanie powinno umożliwiać blokowanie potencjalnie niechcianych aplikacji (tzw. Potentially Unwanted

	Applications - PUAs) System powinien umożliwiać ręczną aktualizację przez pobraną wcześniej bazę sygnatur (Air Gap Pattern Updates)
Ochrona przed nieznanymi zagrożeniami	Rozwiązanie klasy Sandbox do ochrony przez zagrożeniami typu Zero-Day. Rozwiązanie oferujące statyczną i dynamiczną analizę kodu przesyłanego w ramach ruchu web czy email. Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików wykonywalnych w tym .exe, .com, .dll. Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików dokumentów w tym .doc, .docx, .docm, .rtf. Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików .pdf. Rozwiązanie umożliwiające dodatkową inspekcję i detoancję archiwów w tym .zip, .bzip, .gzip, .rar, .tar, .lha, .lhz, .7z, .cab. System zapewniający agresywną analizę behawioralna kodu uruchamianego w środowiskach testowych Windows i MacOS. System zapewniający analizę pamięci, ruchu sieciowego, operacji na dysku, operacji w rejestrze systemowym po detonacji kodu. System zapewniający analizę struktury kodu w tym analizę przeprowadzaną przez mechanizmy głębokiego uczenia maszynowego. System zapewniający ochronę przed exploitami i złośliwym kodem ransomware. System badający reputację pliku w zewnętrznych bazach takich jak np. Virustotal. System powinien oferować szczegółowe raporty dowodzące przeprowadzenia analizy w/w mechanizmów. Urządzenie powinno mieć możliwość realizacji funkcji ZTNA Gateway.
Integracja z rozwiązaniami XDR	Urządzenia UTM powinny zapewniać integrację z systemem do ochrony urządzeń końcowych XDR producenta w zakresie zbierania danych i poszukiwania zagrożeń, usuwania zagrożeń i analityki. Funkcjonalność aktywnej reakcji na zagrożenia powinna zapewniać automatyczna identyfikację, blokowanie lub izolowanie aktywnych zagrożeń na poziomie sieci. Zbierane i raportowane powinny być informacje o zagrożeniach, użytkownikach oraz procesach i zagrożonych urządzeniach.
Ochrona DNS	Usługa umożliwiająca: - rozpoznawania nazw domen, - blokowanie złośliwych adresów URL podczas wyszukiwania DNS, - kontrola zgodności i blokowanie niechcianych witryn wg ustalonych kategorii.
Dodatkowe funkcjonalności ochrony	Urządzenie powinno umożliwiać realizacje funkcji ochrony Web Application Firewall. Zamawiający nie wymaga dostarczenia licencji do uruchomienia funkcjonalności ochrony Web Application Firewall.
Wymagania pozostałe	Urządzenie powinno być fabrycznie nowe i być zakupione w oficjalnym kanale dystrybucyjnym producenta oraz być objęte gwarancją producenta, co najmniej przez czas trwania dostarczanych subskrypcji ochrony. W zestawie dostarczone elementy wymagane do zainstalowania w szafie rack 19” oraz redundantne zasilacze.

Tabela nr 2. Szczegółowe wymagania minimalne dla urządzenia wyniesionego UTM do ochrony sieci w MOPS

Wyniesione urządzenia UTM do ochrony sieci – 1 szt. **Miejsce instalacji: MOPS**	
Nazwa parametru	**Minimalne wymagania**
Typ i ilość	Niezależne urządzenie fizyczne w pełni zintegrowane z klastrem UTM zainstalowanym w UM w trybie SD-WAN/VPN, połączone poprzez bezpieczny szyfrowany tunel. Zamawiający nie dopuszcza instalacji w postaci maszyn wirtualnych (VM).

Zastosowanie	Ochrona na brzegu sieci LAN
Wymagania licencyjne i czas trwania subskrypcji ochrony	Dostarczone licencje ochrony i wsparcia do klastra UTM powinny zapewniać korzystanie ze wszystkich funkcjonalności ochrony ruchu przez urządzenie wyniesione. Licencje ochrony dla klastra UTM powinny umożliwiać korzystanie ze wszystkich wymaganych funkcjonalność przez urządzenie wyniesione, tj. w zakresie zarządzania, zapory sieciowej, koncentratora VPN, zapobiegania włamaniom i zaawansowana ochrona przed zagrożeniami, ochrony i kontroli ruchu WEB, ochrony przed nieznanymi zagrożeniami, integracji z rozwiązaniami XDR, ochrony DNS, logowania i raportowania. Okres trwania subskrypcji licencji ochrony do urządzeń UTM powinien wynosić co najmniej 36 miesięcy, jednak nie powinien być krótszy niż okres trwania subskrypcji ochrony zadeklarowany w formularzu oferty. W okresie trwania subskrypcji powinna być: - możliwość kontaktu ze wsparciem producenta w trybie 24/7 przez różne kanały (co najmniej telefonicznie, zgłoszenia przez portal web, chat) w celu uzyskania wsparcia producenta w zakresie rozwiązywania problemów działaniem systemu; - możliwość aktualizacji oprogramowania układowego i pobierania poprawek; - wymiany uszkodzonego urządzenia w trybie AHB.
Liczba i typ interfejsów fizycznych	Co najmniej: 4 x 1 GbE (LAN) 1 x 1 GbE (WAN) 1 x 1GbE/SFP (WAN) 1 x USB 3.0
Interfejsy zarządzania	Diody LED na przednim panelu z podstawowymi informacjami statusowymi i konfiguracyjnymi
Parametry wydajnościowe	Przepustowość tunelu szyfrowanego do klastra UTM co najmniej: 800 Mbps
Wymagania systemu zarządzania	Urządzenie w pełni zarządzalne z poziomu interfejsów zarządzania klastra UTM.
Wymagania sieciowe	Dwa łącza WAN umożliwiające zestawienia dwóch połączeń poprzez bezpieczne szyfrowane tunele do klastra UTM z możliwością ustawienia trybów pracy tj. Fail-Over lub Load-Balancing. Obsługa funkcjonalności VLAN na portach LAN, w tym VLAN-per Port, trunk.
Wymagania pozostałe	Urządzenie powinno być fabrycznie nowe i być zakupione w oficjalnym kanale dystrybucyjnym producenta oraz być objęte gwarancją producenta co najmniej przez czas trwania dostarczanych subskrypcji ochrony. Możliwość podłączenia dodatkowego zasilacza redundantnego.

Tabela nr 3. Szczegółowe wymagania minimalne dla systemu XDR do ochrony urządzeń końcowych i serwerów

Wymagania minimalne dla systemu XDR do ochrony urządzeń końcowych i serwerów	
Nazwa parametru	**Minimalne wymagania**
Wymagania licencyjne i czas trwania subskrypcji ochrony	Zamawiający wymaga dostarczenia następujących licencji: – do ochrony komputerów z systemami Windows, Mac i Linux – **70** urządzeń końcowych (komputerów), – do ochrony serwerów z systemami Windows, Linux – **10** serwerów.

	Okres trwania subskrypcji na systemy ochrony XDR powinien wynosić, co najmniej 36 miesięcy, jednak nie powinien być krótszy niż okres trwania subskrypcji ochrony zadeklarowany w formularzu oferty. W okresie trwania subskrypcji powinna być możliwość kontaktu ze wsparciem producenta np. poprzez system zgłoszeń w celu uzyskania wsparcia producenta w zakresie rozwiązywania problemów działaniem systemu.
Zintegrowane zarządzanie z poziomu centralnej konsoli	- Oprogramowanie powinno posiadać centralną ujednoliconą konsolę chmurową do zarządzania wieloma komponentami, co najmniej takimi jak zaawansowana ochrona urządzeń końcowych XDR, ochrona serwerów, ochrona urządzeń mobilnych, ochrona poczty e-mail, zarządzania UTM, itp. - Wszystkie ustawienia zarządzanych i monitorowania ww. komponentów powinny mieć możliwość konfiguracji z centralnej graficznej konsoli nawigacyjnej bez konieczności uzyskiwania dostępu do dodatkowych konsol. - Konsola powinna obsługiwać wszystkie urządzenia końcowe i serwery niezależnie od systemu operacyjnego (Windows, Mac, Linux). - Automatyczna prezentacji stanu ochrony - konsola administratora powinna umożliwiać prezentację kondycji konta (ocena na podstawie użycia wszystkich funkcji ochrony zawartych w licencji, wskazanie czy urządzenia lub zasady używają zalecanych, bezpiecznych ustawień, itp.).
Klasyfikacja rozwiązania wg. Gartner Magic Quadrant	Proponowane rozwiązanie powinno być w kategorii „Lidera” w raporcie Gartner Magic Quadrant for Endpoint Protection Platforms (EPP) na rok 2023, 2024.
	Dostawca powinien być „Liderem” w raportach Gartner Magic Quadrant for Endpoint Protection Platforms (EPP) przez 1co najmniej 10 kolejnych edycji.
	Ocena wg MITRE ATT&CK
	Proponowane rozwiązanie powinno uczestniczyć w ocenie MITRE Engenuity ATT&CK.
	Test ochrony SE Labs
	Dostawca powinien uzyskać wysoką liczbę punktów w raporcie SE Labs dotyczącym ochrony punktów końcowych.
	Certyfikacja AV-Test
	Produkt posiadać certyfikat „Top Product” w teście AV-TEST dla urządzeń z systemem Windows.
Zarządzanie zużyciem przepustowości	- Oprogramowania do ochrony powinno mieć możliwość ustawienia wstępnie skonfigurowanej dostępnej przepustowości używanej zarówno do aktualizacji oprogramowania, jak i aktualizacji definicji zagrożeń (np. 64, 128, 256 Kb / s itp.). - Opcja skonfigurowania lokalnego serwera aktualizacji jako pamięci podręcznej w lokalnym środowisku sieciowym, aby zminimalizować duże obciążenie aktualizacja silnika oprogramowania. Polityko zarządzania aktualizacjami, która zawiera konfigurację harmonogramów aktualizacji na zarządzanych punktach końcowych.
Opcje wdrażania	Wdrażanie agenta ochrony urządzeń powinno obsługiwać następujące metodologie: 1) Link do konfiguracji poprzez e-mail 2) za pomocą skryptu AD Startup/Shutdown 3) Skrypt logowania AD 4) poprzez SCCM 5) bezpośrednią instalację agenta z pliku instalacyjnego
	Integracja z SIEM
	System powinien mieć możliwość wyodrębniania informacji o zdarzeniach i alertach z konsoli do lokalnego SIEM.
	Interfejs API do zarządzania ochroną urządzeń

	Interfejsy API oferujące zarządzanie punktami końcowymi jako RESTful HTTP przez publiczny Internet. Interfejsy API muszą mieć możliwość wykonywania zapytań do dzierżawców, wyliczania punktów końcowych i serwerów oraz zarządzania nimi, a także możliwość przeszukiwania alertów i zarządzania nimi programowo. Interfejs API powinien umożliwiać zapytania OSquery do punków końcowych podłączonych do konsoli administracyjnej oraz zapytań XDR do danych zgromadzonych w Data Lake.
	Zarządzanie rolami w systemie
	- Możliwość zezwolenia na rozdzielenie zarządzania od różnych loginów administratora. - Musi zapewniać administratorom możliwość przypisywania wstępnie zdefiniowanych ról administracyjnych użytkownikom, którzy potrzebują dostępu do konsoli administracyjnej. - Możliwość tworzenia ról niestandardowych i przypisywania do nich potrzebnych produktów i dostępu.
	Synchronizacja usługi Microsoft AD
	- Możliwość zezwalania tylko na synchronizację użytkowników/grup z lokalnych serwerów Active Directory do centralnej konsoli systemu w celu zarządzania zasadami. - Zarządzanie grupami urządzeń - możliwość porównania urządzeń, na których zainstalowano agentów ochrony punktu końcowego z urządzeniami zsynchronizowanymi z usługą Active Directory i sporządzenia listy niezarządzanych urządzeń.
	Uwierzytelnianie usługi Microsoft Azure AD / Entra ID
	- Możliwość zalogowania się do pulpitu administracyjnego i portalu samoobsługowego przy użyciu logowania do usługi Azure AD. - Możliwość automatycznego logowania się do pulpitu nawigacyjnego administratora/portalu samoobsługowego, jeśli jest już uwierzytelniony w przeglądarce internetowej przy użyciu logowania do usługi Azure AD / Entra ID z innej aplikacji/usługi
	Zasady przypisywania polityk ochrony
	- Wybrane polityki powinny mieć możliwość zastosowania do użytkowników lub urządzeń. - Polityki muszą mieć możliwość automatycznego wyłączania na podstawie zaplanowanej godziny i daty.
	Ulepszona ochrona przed manipulacją (Enhanced Tamper Protection)
	- Możliwość uniemożliwienia lokalnym użytkownikom administracyjnym lub złośliwym procesom wyłączenia ochrony punktów końcowych. - Możliwość zapobiegania następującym działaniom na oprogramowaniu zainstalowanych na urządzeniach końcowych: 1) Zatrzymywanie usług z interfejsu usług 2) Zabijaniu usługi z interfejsu Menedżera Zadań 3) Zmiany konfiguracji usługi z interfejsu Użytkownika Usług 4) Zatrzymaniu usługi/edycji konfiguracji usługi z wiersza poleceń 5) Odinstalowanie aplikacji 6) Ponowna instalacja aplikacji 7) Zabijania procesu z interfejsu Menedżera Zadań (żądane) 8) Usuwania lub zmodyfikowania chronionych plików lub folderów 9) Usuwania lub modyfikowania chronionych kluczy rejestru - Musi mieć możliwość eksportowania haseł Tamper Protection w formacie CSV lub PDF - Możliwość eksportowania haseł Tamper Protection w formacie CSV lub PDF.

Ochrona przed zagrożeniami (Threat Protection)	- Powinna chronić przed wieloma zagrożeniami, zarówno znanymi, jak i nieznanymi, oraz zapewniać zaufane i zintegrowane podejście do zarządzania zagrożeniami w punkcie końcowym. - Powinna chronić systemy punktów końcowych przed wirusami, programami szpiegującymi, trojanami, rootkitami i robakami na stacjach roboczych i laptopach, niezależnie od ich charakteru lub zastosowanych mechanizmów ukrywania. - Powinna chronić przed zagrożeniami związanymi z plikami wykonywalnymi, a także plikami dokumentów zawierającymi aktywne elementy, takie jak makra lub skrypty. Musi chronić przed exploitami wynikającymi z wykrycia (opublikowanych lub nie) luk w zabezpieczeniach systemów lub oprogramowania. - Powinna mieć możliwość 'lookup' plików w czasie rzeczywistym, aby sprawdzić, czy są złośliwe. Ta funkcja sprawdza podejrzane pliki pod kątem najnowszego złośliwego oprogramowania w bazie danych Threat Intelligence producenta w chmurze. - Powinna mieć możliwość skanowania w czasie rzeczywistym plików lokalnych i udziałów sieciowych w momencie, gdy użytkownik próbuje uzyskać do nich dostęp. Dostęp musi zostać odrzucony, chyba, że plik jest w dobrej kondycji. - Powinna mieć możliwość skanowania w czasie rzeczywistym dostępu do Internetu przez użytkowników końcowych. Powinna monitorować i klasyfikować strony internetowe zgodnie z ich poziomem ryzyka i udostępniać tę technologię systemom operacyjnym komputera. Witryna, o której wiadomo, że zawiera złośliwy kod lub witryny wyłudzające informacje, musi być proaktywnie blokowana przez rozwiązanie, aby zapobiec ryzyku infekcji lub ataku na lukę używanej przeglądarki. Rozwiązanie musi przeprowadzać kontrole w bazie danych zainfekowanych stron internetowych, która to baza jest stale aktualizowana o nowe witryny identyfikowane każdego dnia. - Powinna chronić zarządzane systemy przed złośliwymi witrynami internetowymi w czasie rzeczywistym, niezależnie od tego, czy użytkownicy końcowi pracują w firmie, czy poza bezpieczną siecią firmy - w domu lub za pośrednictwem publicznej sieci Wi-Fi. Wszystkie przeglądarki dostępne na rynku muszą być obsługiwane (Internet Explorer, Firefox, Safari, Opera, Chrome itp.).
Wykrywanie rootkitów	System powinien zidentyfikować rootkita podczas przeglądania elementu bez przeciążania systemu operacyjnego końcówki. Rootkity muszą być proaktywnie wykrywane.
Wykrywanie podejrzanych zachowań (Suspicious Behavior Detection)	- System powinien chronić się przed niezidentyfikowanymi wirusami i podejrzanym zachowaniem. - Powinien mieć zarówno analizę zachowania przed wykonaniem, jak i analizę zachowania w czasie wykonywania. - System powinien zidentyfikować i zablokować złośliwe programy przed wykonaniem. - System powinien dynamicznie analizować zachowanie programów uruchomionych w systemie, a następnie wykrywać i blokować aktywność, która wydaje się być złośliwa. Może to obejmować zmiany w rejestrze, które mogą umożliwić automatyczne uruchamianie wirusa po ponownym uruchomieniu komputera. - Powinien zapewniać ochronę przed atakami przepełnienia bufora.
Skanowanie	- Powinno zapewnić możliwość zaplanowanego uruchomienia skaner w zależności od wybranej częstotliwości lub przez ręczne wyzwalanie za pomocą Eksploratora Windows w celu skanowania określonych katalogów (lokalnych, zdalnych lub wymiennych), z użytymi parametrami analizy, które mogą różnić się od tych wybranych do ochrony w czasie rzeczywistym. - Powinno mieć możliwość skanowania archiwów, takich jak zip, cab itp., które można włączyć za pomocą ustawień polityki.
Zaawansowany mechanizm	- System musi być skanowany z prędkością światła; w ciągu 20 milisekund model jest w stanie wyodrębnić miliony cech z pliku, przeprowadzić głęboką analizę i określić, czy plik jest poprawny czy złośliwy. Cały ten proces odbywa się przed wykonaniem pliku.

głębokiego uczenia (Deep Learning)	- Powinien być w stanie zapobiec zarówno znanemu, jak i nigdy wcześniej nie widzianemu złośliwemu oprogramowaniu, a także musi być w stanie zablokować złośliwe oprogramowanie przed jego wykonaniem. - Powinien chronić system nawet w trybie offline i nie będzie polegać na sygnaturach. - Powinien klasyfikować pliki jako złośliwe, potencjalnie niechciane aplikacje (PUA) lub nieszkodliwe. Deep Learning musi również koncentrować się na przenośnych plikach wykonywalnych systemu Windows. - Możliwość wykonywania nowego skanowania zagrożeń Zero Days w trybie offline (bez Internetu). - Powinien być w stanie przetwarzać dane przez wiele warstw analizy, z których każda sprawia, że model jest znacznie potężniejszy. - Musi być skalowalny - powinien być w stanie przetworzyć znacznie więcej danych wejściowych, może dokładnie przewidzieć zagrożenia, jednocześnie pozostając na bieżąco. - Przestrzeń zajmowana przez model powinna być mniejsza niż 20 MB na punkcie końcowym, z prawie zerowym wpływem na wydajność. - Model głębokiego uczenia się będzie śledził i oceniał modele end-to-end przy użyciu zaawansowanych pakietów opracowanych zdalnie, takich jak Keras, Tensorflow i Scikit-learn.
Funkcjonalność zapobiegania/ograniczania zagrożeń (Exploit Prevention/Mitigation) powinna wykrywać i zatrzymywać następujące znane ataki	1) Egzekwowanie ochrony wykonania danych (DEP). 2) Zapobiega nadużywaniu przepełnienia bufora 3) Obowiązkowa randomizacja układu przestrzeni adresowej (ASLR) 4) Zapobiega przewidywalnym lokalizacjom kodu 5) Bottom-up ASLR 6) Ulepszona randomizacja lokalizacji kodu. 1) 4) Null Page (Null Dereference Protection) 2) Zatrzymuje exploity, które przeskakują przez stronę 0. 3) Heap Spray Allocation 4) Zarezerwowanie lub wstępne alokowanie powszechnie używanych adresów pamięci, więc nie można ich używać do przechowywania ładunków. 5) Dynamiczne ataki Heap Spray 6) Zatrzymuje ataki które rozpylają podejrzane sekwencje na stercie 7) Stack Pivot 8) Zatrzymanie nadużywania wskaźnika stosu. 9) Stack Exec (MemProt) 10) Zatrzymuje kod atakującego na stosie. 11) Stack-based ROP Mitigations (Caller) 12) Zatrzymuje standardowe ataki Return-Oriented Programming . 13) Branch-based ROP Mitigations (Hardware Augmented) 14) Zatrzymuje zaawansowane ataki Return-Oriented Programming. 15) Structured Exception Handler Overwrite Protection (SEHOP) 16) Zatrzymuje nadużywanie mechanizmu obsługi wyjątków 17) Import Address Table Access Filtering (IAF) (Hardware Augmented) 18) Zatrzymuje osoby atakujące, które wyszukują adresy API w IAT. 19) LoadLibrary API calls 20) Zapobiega ładowaniu bibliotek ze ścieżek UNC. 21) Reflective DLL Injection 22) Zapobiega ładowaniu biblioteki z pamięci do procesu hosta 23) Shellcode monitoring 24) Wykrywanie wrogich shellcode obejmuje wiele technik rozwiązywania problemów, takich jak fragmentaryczny kod powłoki, zaszyfrowane ładunki i kodowanie bez wartości null.

	25) VBScript God Mode 26) Ma możliwość wykrywania manipulowania flagą trybu awaryjnego w VBScript w przeglądarce internetowej. 27) WoW64 28) Musi mieć możliwość zabronienia kodowi programu bezpośredniego przełączania się z trybu 32-bitowego na 64-bitowy (np. za pomocą ROP), jednocześnie umożliwiając warstwie WoW64 wykonanie tego przejścia. 29) Syscall 30) Zatrzymuje osoby atakujące, które próbują ominąć haki bezpieczeństwa. 31) Hollow Process Protection 32) Zatrzymuje ataki wykorzystujące legalne procesy do ukrywania wrogiego kodu. 33) DLL Hijacking 34) Daje priorytet do dostępu do bibliotek systemowych dla pobranych aplikacji. 35) Application Lockdown 36) Automatycznie zakończy chronioną aplikację na podstawie jej zachowania; na przykład, gdy aplikacja pakietu Office jest wykorzystywana do uruchamiania programu PowerShell, uzyskiwania dostępu do usługi WMI, uruchamiania makra w celu zainstalowania dowolnego kodu lub manipulowania krytycznymi obszarami systemu; rozwiązanie musi blokować złośliwe działanie nawet jeśli atak nie powoduje powstania procesu potomnego. 37) Java Lockdown 38) Zapobiega atakom, które nadużywają Javy do uruchamiania plików wykonywalnych systemu Windows. 39) Squiblydoo AppLocker Bypass 40) Zapobiega regsvr32 przed uruchamianiem zdalnych skryptów i kodu. 41) CVE-2013-5331 i CVE-2014-4113 via Metasploit 42) In-memory payloads: Meterpreter & Mimikatz. 43) EFS Guard 44) Ochrona plików zaszyfrowanych za pomocą EFS przed atakami Encrypting File System. 45) CTF Guard 46) Zapobieganie nadużyciom podsystemu CTF 47) ApiSetGuard 48) Pomoc w zapobieganiu bocznemu ładowaniu przez aplikację złośliwej biblioteki DLL podszywającej się pod bibliotekę DLL ApiSet Stub.
Zaawansowane ograniczanie zagrożeń (Advanced Exploit Mitigation)	System powinien chronić się przed szeregiem exploitów lub zagrożeń "aktywnego przeciwnika", takich jak: 1) Kradzież poświadczeń - Kradzież haseł i informacji o haszowaniu z pamięci, rejestru lub dysku twardego. 2) Naruszenie APC - Ataki wykorzystujące wywołania procedur aplikacji (APC) do uruchamiania złośliwych kodów. 3) Eskalacja uprawnień - Ataki eskalujące proces o niskich uprawnieniach do wyższych uprawnień dostępu do systemów. 4) Code Cave Utilisation - Złośliwy kod, który został wstawiony do innej, legalnej aplikacji. 5) Exploity weryfikatora aplikacji - Ataki, które wykorzystują weryfikatora aplikacji w celu uruchomienia nieautoryzowanego oprogramowania podczas uruchamiania.
Ochrona procesów	System powinien zapobiec przejęciu legalnych aplikacji przez złośliwe oprogramowanie, takie jak: • Ataki polegające na wydrążaniu procesów • Ładowanie bibliotek DLL z niezaufanych folderów • Kradzież poświadczeń

	• Wykorzystanie jaskini kodu • Naruszenie APC • Eskalacja uprawnień
Wykrywanie złośliwego ruchu (MTD)	System powinien wykryć komunikację między komputerami końcowymi, a serwerami dowodzenia i kontroli zaangażowanymi w botnet lub inne ataki złośliwego oprogramowania.
System zapobiegania włamaniom (IPS)	- System powinien zapobiec złośliwemu ruchowi sieciowemu za pomocą inspekcji pakietów (IPS). - System powinien skanować ruch na najniższym poziomie i blokować zagrożenia przed uszkodzeniem systemu operacyjnego lub aplikacji.
Ochrona przed oprogramowaniem ransomware	- Musi mieć możliwość przywrócenia zaszyfrowanych plików do stanu przed zaszyfrowaniem. - W celu przeprowadzenia wykrywania ochrona przed exploitami i oprogramowaniem ransomware nie wymaga użycia usługi Cloud Lookup. - Gdy funkcja Anti-crypto podejrzewa, że pewne zachowanie nie jest zgodne z zamierzonym procesem, Rejestrator Danych rozpoczyna buforowanie danych, podczas gdy wspomniane zachowanie jest dokładnie sprawdzane w celu ustalenia, czy aplikacja jest legalna lub czy działanie jest uzasadnione. Maksymalny rozmiar rejestratora danych wynosi 100 MB, a funkcja Anti-crypto buforuje pliki poniżej 75 MB. - Funkcja Anti-crypto spogląda wstecz na wszystkie złośliwe modyfikacje plików dokonane przez ten proces i przywraca je do ich pierwotnej lokalizacji. - Jeśli infekcja ransomware zdoła się dostać, szczegółowe historyczne śledzenie pochodzenia infekcji i sposobu jej rozprzestrzeniania się zostanie zgłoszone dzięki Threat Cases (RCA). - System powinien chronić przed oprogramowaniem ransomware, które szyfruje główny rekord rozruchowy i przed atakami, które czyszczą dysk twardy.
Ochrona AMSI	- System powinien chronić się przed złośliwym kodem (na przykład skryptami PowerShell) przy użyciu interfejsu Microsoft Antimalware Scan Interface (AMSI). - System powinien skanować kod przekazywany przez AMSI przed uruchomieniem, a aplikacje używane do uruchamiania kodu są powiadamiane o zagrożeniach. Jeśli zostanie wykryte zagrożenie, zdarzenie jest rejestrowane.
Zapobieganie utracie danych (DLP)	- System powinien monitorować i ograniczać przesyłanie plików zawierających poufne dane. - System powinien możliwość tworzenia niestandardowych polityk DLP lub polityk na podstawie szablonów. - System powinien powsiadać szablony polityk DLP, które obejmują standardową ochronę danych dla różnych regionów.
Kontrola urządzeń peryferyjnych	- System powinien mieć możliwość kontrolowania i ograniczania wymiennych urządzeń pamięci masowej (pamięci USB, CD Rom, zewnętrzne dyski twarde USB, iPody, odtwarzacze MP3 itp.), A także urządzeń połączeniowych (Wi-Fi, Bluetooth, podczerwień, modemy itp.). - System powinien mieć możliwość dodawania wyłączeń urządzeń według identyfikatora modelu lub identyfikatora wystąpienia.
Kontrola aplikacji	- System powinien mieć możliwość ograniczenia aplikacji potrzebnych dla określonych grup użytkowników. - System powinien być w stanie wykryć i zablokować kategorie aplikacji, które mogą nie być odpowiednie do użycia w środowisku przedsiębiorstwa. - System powinien mieć predefiniowane kategorie aplikacji dla często używanych aplikacji.

Kontrola Web	- System powinien blokować ryzykowne pobieranie, chronić przed utratą danych, uniemożliwiać użytkownikom dostęp do stron internetowych, które są nieodpowiednie do pracy, i generować dzienniki zablokowanych odwiedzanych witryn. - System powinien mieć opcje zabezpieczeń, aby skonfigurować dostęp do reklam, witryn bez kategorii lub niebezpiecznych plików do pobrania. - System zapewnić administratorowi możliwość zdefiniowania ustawień "dopuszczalnego korzystania z sieci" (zdefiniowanych przez kategorie) w celu kontrolowania witryn które użytkownicy mogą odwiedzać. Administrator musi mieć dostęp kontrolny do stron internetowych, które zostały zidentyfikowane i sklasyfikowane w ich własnych kategoriach. - System powinien mieć opcję ochrony przed utratą danych, która pozwala administratorowi kontrolować dostęp do internetowych wiadomości e-mail i pobierania plików, z możliwością blokowania danych, zezwalania na udostępnianie danych lub dostosowywania tego wyboru.
Zasady Zapory systemu Windows	- System powinien być w stanie monitorować i konfigurować Zaporę Systemu Windows na zarządzanych komputerach i serwerach przy użyciu zasad Zapory Systemu Windows. - System powinien mieć możliwość zastosowania zasad Zapory Systemu Windows do poszczególnych urządzeń (komputerów lub serwerów), lub grup urządzeń.
Analiza przyczyn źródłowych (Root Cause Analysis)	- System powinien mieć możliwość zidentyfikowania co się stało, skąd pochodzi naruszenie, jakie pliki zostały naruszone oraz zapewnia wskazówki, jak wzmocnić stan bezpieczeństwa organizacji. - System powinien być w stanie rejestrować łańcuch zdarzeń, które miały miejsce po wykryciu infekcji, umożliwiając określenie pochodzenia infekcji, wszelkich wynikających z tego uszkodzeń zasobów, potencjalnie narażonych danych i łańcucha zdarzeń prowadzących do zatrzymania infekcji. - Zawiera podsumowanie zdarzenia: jaki exploit został wykryty, gdzie wystąpiło zdarzenie beacon (zasób), kiedy wystąpiło, w jaki sposób infekcja się powiodła. Np. "Outlook.exe". - Przedstawia zalecenia dotyczące rozwiązania problemu: rzeczy, których należy szukać po ataku. Na przykład oprócz plików przywracanych z zaszyfrowanych, sprawdź ustawienia przeglądarki, aby upewnić się, że w wyniku infekcji nie powstały żadne luki. - Rekord aktywności umożliwia administratorom dodawanie notatek do sprawy. Wszystkie uwagi dotyczące spraw zostaną wymienione w tej kolumnie. - Możliwość modyfikowanie stanu sprawy przez administratora (Nowa, W toku, Zamknięta) i ustawianie priorytetu (Niski, Średni, Wysoki). Po zamknięciu administrator może dodawać notatki, a także jest zobowiązany do potwierdzenia (za pomocą pól wyboru), że podjęto kroki naprawcze: przeanalizowano wpływ na pliki / zasoby i wdrożono odpowiednie ulepszenia środowiskowe. - Zapewnia tabelaryczny widok wszystkiego, czego dotyczy atak. Elementy mogą być filtrowane na podstawie typu — np. pliki, procesy, klucze rejestru. Administrator może przeglądać informacje o każdym elemencie, np. nazwa pliku (plik ofiary lub agent złośliwego oprogramowania), identyfikator procesu, znacznik czasu rozpoczęcia/zatrzymania zdarzenia. - Wskazuje początek głównej przyczyny, kreśląc serię zdarzeń wynikających z ataku jako zbiór węzłów. Każdy węzeł zawiera określone informacje o plikach, procesach, kluczach rejestru itp. zaangażowanych na tym etapie. Zdarzenie beacon (oznaczone niebieską kropką) zostanie zidentyfikowane w łańcuchu, ale zostaną również wyświetlone wszelkie zdarzenia wykonane przez proces zidentyfikowany jako zdarzenie beacon.

Blokowanie aplikacji	Natychmiastowe wykrywanie i usuwania potencjalnie złośliwych plików Portable Executable (PE) z chronionych komputerów. Opcję blokowania aplikacji przy użyciu ich hasła SHA-256.
Poszukiwanie zagrożeń na żądanie	Opcja „żądania poszukiwania zagrożeń" podejrzanych plików, co spowoduje przesłanie pliku do zespołu badawczego producenta ds. złośliwego oprogramowania w celu dalszej analizy. Możliwość dostarczenia raport podsumowujący analizę podejrzanego pliku za pomocą uczenia maszynowego oraz ze szczegółową analizą podejrzanego pliku, aby pomóc zdecydować, czy jest on złośliwy, czy nie.
Adaptacyjna aktywna ochrona przed zagrożeniami	Funkcja adaptacyjnej aktywnej ochrony przed atakującymi zagrożeniami, która składa się z serii reguł behawioralnych skoncentrowanych na technice, mających na celu zakłócenie działania zagrożenia, która jest automatycznie włączana po wykryciu potencjalnego zagrożenia. Reguły trybu zakłócania muszą być wyzwalane na urządzeniu tylko po innych, dość specyficznych zdarzeniach ochrony przed złośliwym oprogramowaniem, wskazujących na aktywnego przeciwnika. Reguły trybu zakłócania powinny również dodawać klasyfikacje taktyki, techniki i procedury (TTP), które będą widoczne w konsoli administracyjnej.
Ostrzeżenia o atakach krytycznych	System MUSI powiadomić o aktywnym ataku. System powinien przedstawić wskaźnik o dużym wpływie zaawansowanego ataku w toku na wielu punktach końcowych lub serwerach w chronionym środowisku. Powinien wysyłać alerty do administratorów kont za pośrednictwem poczty e-mail i powiadomień push na urządzenia mobilne objęte licencją ochrony przed zagrożeniami.
Live Query	Możliwość zapewnienia analitykom ds. bezpieczeństwa i administratorom IT możliwość uruchamiania zapytań SQL w celu uzyskania odpowiedzi dowolne zapytanie pytanie dotyczące punktów końcowych i na serwerów.
	Możliwość zapytań OSquery pozwalająca administratorom zrozumieć bieżący stan działania ochrony urządzenia. Szybkie wykrywanie problemów z operacjami IT i zadawanie szczegółowych pytań SQL, aby wykryć podejrzaną aktywność. Możliwość wyboru źródła danych, które ma zostać użyte podczas konfigurowania i uruchamiania zapytania: • Punkty końcowe, które są obecnie online (90 dni danych przechowywanych na urządzeniu), • Data Lake w chmurze (30 dni przechowywania w chmurze), Możliwość używania wydajnych, gotowych, w pełni konfigurowalnych zapytań SQL, które mogą szybko przeszukiwać do 90 dni bieżących i historycznych danych obejmujących operacje IT i wykrywanie zagrożeń.
Integracja z systemami firm trzecich	Dostępne gotowe integracje z rozległym ekosystemem zewnętrznych dostawców ochrony punktów końcowych, zapór sieciowych, sieci, poczty e-mail, tożsamości i zabezpieczeń chmury, takich jak: Microsoft Crowdstrike Palo Alto Networks Fortinet Mimecast Trendmicro Darktrace AWS, itp.
	Musi mieć możliwość wywołania głębokiego czyszczenia po każdym aktywnym wykryciu exploita lub ransomware.

Zaawansowane czyszczenie systemu	Zapewniać zaawansowane wykrywanie złośliwego oprogramowania poprzez wyszukiwanie następujących elementów:
	A. Pliki
	Oznaczone jako złe.
	Plik został pobrany z Internetu.
	We właściwościach pliku brakuje informacji o nazwisku/wersji autora, tj. Personifikując wspólny plik systemowy systemu Windows. Przeżywalność ponownego uruchomienia jest energicznie chroniona.
	Używane nietypowe rozszerzenie pliku.
	Zawiera anomalie struktury PE i sugestie zaciemnienia
	B. Procesy
	Nasłuchiwanie połączeń przychodzących.
	Brakujący źródłowy plik wykonywalny.
	Brak elementów interfejsu użytkownika.
	Randomizacja układu przestrzeni adresowej (ASLR) została usunięta z systemu.
Zintegrowany system zabezpieczeń	Dostarczony system powinien być w stanie współpracować z innymi produktami zabezpieczającymi dostawcy w celu udostępniania informacji i reagowania na incydenty.
Punkt końcowy + brama poczty e-mail	Musi być w stanie automatycznie izolować zainfekowane skrzynki pocztowe i czyścić zainfekowane komputery wysyłające wychodzący spam i złośliwe oprogramowanie.
Punkt końcowy + Zapora sieciowa	Możliwość automatycznego izolowania zainfekowanych punktów końcowych w sieci. Możliwość manualnego izolowania zainfekowanych punktów końcowych w sieci w trakcie analizy zagrożenia.
	Możliwość zidentyfikowania wszystkich aplikacji w sieci. Możliwość zidentyfikowania źródeł złośliwego ruchu na urządzeniach.
	Powiązanie zagrożenia z poszczególnymi użytkownikami i komputerami.
	Możliwość klasyfikowania i blokowania wszystkich niepożądanych aplikacji wykorzystujących przepustowość, możliwość blokowania przepustowości wskazanym aplikacjom.
Punkt końcowy + bezprzewodowy punkt dostępowy	- Musi mieć możliwość automatycznego ograniczenia dostępu do Internetu dla zainfekowanych punktów końcowych połączonych z siecią Wi-Fi. - Rozszerzone wykrywanie i reagowanie na zagrożenia. - Dostarczone oprogramowanie powinno być w stanie przechowywać dane o zagrożeniach na urządzeniu oraz w chmurze. Rozwiązanie powinno gromadzić dane w czasie rzeczywistym. Musi współpracować z rozwiązaniami innych producentów.
Detekcja	- Oprogramowanie musi być wstanie wykrywać podejrzane działania w systemach. Oprogramowanie posiada możliwość nadawania priorytetów wykrytych zdarzeń za pomocą silnika AI. - Automatyczne mapowanie zgodną z MITRE Framework. - Wykrywanie zachowań i exploitów w kontenerach Linux. - Korelacja i analiza zdarzeń między produktami. - Centrum analizy zagrożeń. - Automatyczne i ręczne tworzenie przypadków. - Narzędzie zapytań Live Discover. - Zaplanowane zapytania. - Proste wyszukiwanie (bez SQL). - Eksport danych kryminalistycznych. - Reagowanie. - Automatyczne usuwanie złośliwego oprogramowania. - Automatyczne zakańczanie procesów. - Automatyczne przywracanie szyfrowania plików ransomware.

	- Automatyczna izolacja urządzeń . - Izolacja urządzeń na żądanie.
Dodatkowe funkcjonalności XDR do ochrony serwerów	
Ochrona serwerów powinna spełniać wszystkie powyższe wymagania dla systemu ochrony urządzeń końcowych oraz powinna posiadać dodatkowe poniższe funkcjonalności:	
Automatyczne wykluczenia	Możliwość automatycznego wykluczania aktywności znanych aplikacji (takich jak Microsoft Exchange i Microsoft SQL) ze skanowania, jeśli jest to włączone w ramach zasad dla serwera.
	Biała lista.
	Możliwość zablokowania serwera i zezwalania na uruchamianie tylko zatwierdzonych aplikacji. Kontrolowanie tego, co może uruchamiać i zmieniać aplikację, utrudnia atakującym włamanie się do serwera.
	Monitorowanie integralności plików.
	Monitorowanie krytycznych dla systemu plików i kluczy rejestru w celu zapewnienia dodatkowego bezpieczeństwa. Domyślne reguły, które monitorują zmiany krytycznych plików systemowych Windows, a także zapewniają możliwość dodawania dodatkowych lokalizacji monitorowania i wykluczeń za pośrednictwem zasad. Monitorowanie plików, folderów, kluczy rejestru i wartości rejestru.
Wykrywanie zagrożeń dla serwerów Linux i kontenerów	Możliwości wykrywania i reagowania na obciążenia serwera Linux i kontenery w chmurze, lokalnie i we wdrożeniach wirtualnych. Powinny być możliwe następujące detekcje dla systemu Linux i kontenerów: • Ucieczki kontenerów: Identyfikuje atakujących, którzy podwyższają uprawnienia dostępu do kontenera, aby przejść do hosta kontenera • Kryptominery: Wykrywa nazwy programów lub argumenty powszechnie kojarzone z górnikami kryptowalut • Niszczenie danych: Alerty, że atakujący może próbować usunąć wskaźniki naruszenia, które są częścią trwającego dochodzenia • Efekty jądra: Podświetla, czy wewnętrzne funkcje jądra są modyfikowane na hoście.
Opcje wdrożenia ochrony Linux	Podstawowy, tzw. “lekki” agent Linux, który przekazuje kluczowe informacje potrzebne do badania i reagowania na zagrożenia behawioralne, exploity i złośliwe oprogramowanie w jednym miejscu. Opcja wdrażania powinna umożliwić zarządzanie wszystkimi natywnymi rozwiązaniami dostawców z jednego panelu oraz wyszukiwanie zagrożeń, naprawę i zarządzanie. Sensor Linux - wysoce elastyczna opcją wdrażania, dostrojoną pod kątem wydajności. Sensor Linux wykorzystuje interfejsy API do integrowania detekcji zagrożeń w czasie wykonywania, w środowiskach hosta lub kontenera, z istniejącymi narzędziami reagowania na zagrożenia. Zapewnia szerszy zakres detekcji, kontrolę w celu tworzenia niestandardowych zestawów reguł i opcje konfiguracji w celu dostrojenia wykorzystania zasobów hosta.
Zarządzania profilami wykrywania środowiska Linux	Umożliwienie użytkownikom dostrajania wykrywania środowiska wykonawczego dla agentów i sensorów. Umożliwienie użytkownikom korzystanie z domyślnej zawartości wykrywania opublikowanej przez laboratoria dostawców i dalsze dostrajanie logiki wykrywania dla ich środowiska. Możliwość włączania i wyłączania określonych wykryć i dostrajania logiki listy w celu filtrowania aktywności dozwolonej dla środowiska.
Integracja czujników Linux	Czujnik Linux musi mieć opcję wysyłania zdarzeń wykrywania w czasie wykonywania do Data Lake dostawcy. Zdarzenia wysyłane z czujnika Linux muszą być dostępne w konsoli zarządzania jako wykrycia i możliwe do przeszukiwania za pomocą zapytań Data Lake.

	Umożliwienie administratorom przeglądania danych wykrywania w czasie wykonywania z agenta Linux i podobnych danych wykrywania z czujnika Linux. Możliwość wyszukiwania zagrożeń i badania w systemach Linux ze zwiększoną widocznością przy użyciu znanego interfejsu w konsoli zarządzania.
Skanowanie na żądanie w systemie Linux	Możliwość skonfigurowania, czy skanowanie w trybie na żądanie jest wykonywane podczas odczytu, zapisu czy obu w celu zmniejszenia obciążenie skanowania w przypadku obciążeń wymagających dużego odczytu lub systemów o ograniczonych zasobach.

Tabela nr 4. Szczegółowe wymagania minimalne dla serwerów

Serwer – 2 szt. (miejsce instalacji: w infrastrukturze serwerowej Zamawiającego)	
Nazwa parametru	**Minimalne wymagania**
Obudowa	Maksymalnie 2U RACK 19 cali (wraz z szynami montażowymi) Możliwość wyposażenia serwera w ramie do prowadzenia kabli. Serwer wyposażony w zamykany, zdejmowany panel przedni chroniący przed nieuprawionym dostępem do dysków Serwer wyposażony w czujniki otwarcia obudowy współpracującego z BIOS/UEFI. Serwer wyposażony w moduł TPM 2.0
Parametry wydajnościowe	Serwer wyposażony w dwa procesory 16-rdzeniowe, x86 - 64 bity powinien osiągać w testach SPECrate2017_int_base powyżej 339. Wynik testu opublikowany na stronie www.spec.org. Wykonawca ma obowiązek dostarczenia w dniu składania oferty wydruku ze strony wyników testu potwierdzającego osiągnięcie większej niż minimalna liczba punktów. Płyta główna wspierająca zastosowanie procesorów od 8 do 60 rdzeniowych, mocy do min. 350W i taktowaniu CPU do min. 3.6GHz.
Liczba zainstalowanych procesorów	W dostarczonym serwerze zainstalowany 1 procesor (serwer dwuprocesorowy)
Pamięć operacyjna	128 GB RDIMM DDR5 5600 MT/s w modułach o pojemności 64GB każdy. Płyta główna z minimum 32 slotami na pamięć i umożliwiająca instalację do minimum 8TB.
Sloty rozszerzeń	3 aktywne gniazda PCI-Express generacji 5, w tym min. 1 slot x16 (szybkość slotu – bus width) pełnej wysokości (full height). Możliwość rozbudowy do 6 slotów PCI-Express generacji 5.
Dysk twardy	Zatoki dyskowe gotowe do zainstalowania 8 dysków SFF typu Hot Swap, NVMe/SAS/SATA/SSD, 2,5” i opcja rozbudowy/rekonfiguracji o dodatkowe 8 dysków typu Hot Swap, NVMe/SAS/SATA/SSD, 2,5”.. Zainstalowany dodatkowy moduł bootowania wyposażony w min. 2 dyski systemowe 480GB SSD NVMe pracujące w kontrolerze sprzętowym RAID 1 (moduł bootwania i dyski nie mogą zajmować zatok na dyski SFF).
Kontroler	Kontroler macierzowy software przeznaczony dla dysków SATA zapewniający obsługę RAID 0/1/1/5/10. Możliwość doposażenia serwera w kontroler sprzętowy z min 8GB cache, który zapewnia podtrzymanie pamięci cache w razie braku zasilania zgodny z RAID 0/1/10/5/50/6/60 oraz obsługujący typy dysków: SSD/SATA/SAS/NVMe. Kontroler sprzętowy powinien umożliwiać jednoczesną pracę w trybach RAID i JBOD.
Interfejsy sieciowe LAN	Minimum 1 karta 4-portowa 10/25GbE SFP28 z funkcją Wake-On-LAN, wsparciem dla PXE, które nie zajmują gniazd PCIe. Karta wyposażona w chipset BCM 57504 lub o równoważnych parametrach wydajnościowych.

Interfejsy sieciowe LAN	Minimum 1 karta 4-portowa 10/25Gb SFP28 z funkcją Wake-On-LAN, wsparciem dla PXE. Karta wyposażona w chipset BCM 57504 lub o równoważnych parametrach wydajnościowych.
Karta graficzna	Zintegrowana karta graficzna
Porty	4 x USB 3.0 (w tym 1 port wewnętrzny) 1x VGA Możliwość rozbudowy o: - dodatkowy port typu DisplayPort dostępny z przodu serwera - port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45
Napęd	Możliwość instalacji wewnętrznego napędu DVD-ROM lub DVD-RW
Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 1000W.
Karta/moduł zarządzający	Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia mininmalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: • monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe • wparcie dla agentów zarządzających oraz możliwość pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP • dostęp do karty zarządzającej poprzez - dedykowany port RJ45 z tyłu serwera lub - przez współdzielony port zintegrowanej karty sieciowej serwera dostęp do karty możliwy - z poziomu przeglądarki webowej (GUI) - z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP) - z poziomu skryptu (XML/Perl) - poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface) • wbudowane narzędzia diagnostyczne • zdalna konfiguracji serwera(BIOS) i instalacji systemu operacyjnego • obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie • wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników • przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough) • obsługa zdalnego serwera logowania (remote syslog) • wirtualna zadalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów CD/DVD i USB i i wirtualnych folderów • mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie

	• funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności • monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji • konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping) • zdalna aktualizacja oprogramowania (firmware) • zarządzanie grupami serwerów, w tym: - tworzenie i konfiguracja grup serwerów - sterowanie zasilaniem (wł/wył) - ograniczenie poboru mocy dla grupy (power caping) - aktualizacja oprogramowania (firmware) - wspólne wirtualne media dla grupy • możliwość równoczesnej obsługi przez 3 administratorów • autentykacja dwuskładnikowa (Kerberos) • wsparcie dla Microsoft Active Directory • obsługa SSL i SSH • enkrypcja AES/3DES oraz RC4 dla zdalnej konsoli • wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API • wsparcie dla Integrated Remote Console for Windows clients • możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)
Inne	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta.
Gwarancja i wsparcie techniczne	Co najmniej 36 miesięcy gwarancji producenta realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia. Uwaga: okres udzielonej gwarancji powinien być nie krótszy niż okres gwarancji zadeklarowany w formularzu oferty. W okresie gwarancji producenta powinna być możliwość zgłaszania awarii w trybie 8x5 (od poniedziałku do piątku, w godzinach 8 -16) poprzez ogólnopolską linię telefoniczną lub system zgłoszeń producenta, możliwość aktualizacji sterowników i oprogramowania układowego. Obsługa gwarancyjna realizowana przez polski oddział serwisu producenta.
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001. Serwer musi posiadać deklaracja CE.
Obsługa systemów operacyjnych i systemów wirtualizacyjnych	Zgodność z systemami: Microsoft Windows Server min. w wersji 2019, 2022 i 2025 Ubuntu 20.04 LTS, 22.04 LTS Red Hat Enterprise Linux (RHEL) 8.6, 9.0 VMware ESXi 7.0 U3, 8.0, 8.0 U1/U2

Tabela nr 5. Szczegółowe wymagania minimalne dla serwerowego systemu operacyjnego

Serwerowy system operacyjny oraz licencje umożliwiające korzystanie użytkowników z zasobów – 1 kpl.	
Nazwa parametru	**Minimalne wymagania**

Architektura systemu	System przeznaczony do obsługi dwóch serwerów dostarczonych w ramach realizacji przedmiotu zamówienia, pracujących w trybie wysokiej dostępności HA (High Availability).
Licencjonowanie	W ramach realizacji przedmiotu zamówienia wymagane jest dostarczenie licencji z prawem wieczystego użytkowania zapewniających co najmniej: – zainstalowanie i uruchomienie serwerowego systemu operacyjnego w środowisku 2 dostarczonych serwerów fizycznych, wraz z obsługą funkcjonalności HA (High Availability) oraz z możliwością instalacji co najmniej 6 maszyn wirtualnych środowisk dostarczanego serwerowego systemu operacyjnego, licencja powinna obejmować pełną liczbę rdzeni w 2 dostarczonych serwerach fizycznych wraz z obsługą funkcjonalności HA (High Availability), – licencje umożliwiające korzystanie użytkowników z zasobów serwerowego systemu operacyjnego dla co najmniej 70 użytkowników wewnętrznych pracujących w sieci wewnętrznej urzędu. – uruchomienie serwerowego systemu operacyjnego do jednego serwera fizycznego na potrzeby wdrożenia Active Directory, licencja powinna zapewniać możliwość instalacji co najmniej 2 maszyn wirtualnych środowisk dostarczanego serwerowego systemu operacyjnego, licencja powinna obejmować liczbę do 16-rdzeni w serwerze fizycznym. Dostarczone licencje powinny dotyczyć systemu w najnowszej wersji oferowanej przez producenta.
Funkcjonalności	Współpraca z procesorami o architekturze x86 – 64bit.
	Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.
	Możliwość budowania klastrów składających się z 64 węzłów.
	Praca w roli klienta domeny Microsoft Active Directory.
	Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie funkcjonalności Microsoft Windows Server 2022 i wyższych wersji.
	Możliwość zestawienie i skonfigurowanie klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu.
	Możliwość uruchomienia roli klienta i serwera NTP.
	Możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
	Możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
	Możliwość uruchomienia roli serwera stron WWW.
	W ramach dostarczonej licencji użytkownik ma prawo do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera.
	W ramach dostarczonej licencji użytkownik ma prawo do pobierania poprawek systemu operacyjnego.
	Wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).
	Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
	Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
	Wbudowane wsparcie instalacji i pracy na wolumenach, które:

	a. pozwalają na zmianę rozmiaru w czasie pracy systemu, b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
	Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
	Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
	Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET.
	Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
	Możliwość wykorzystania standardu http/2.
	Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
	Skonfigurowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
	Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
	Mechanizmy logowania w oparciu o: a. login i hasło, b. karty z certyfikatami (smartcard), c. wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).
	Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: a. określonych grup użytkowników, b. zastosowanej klasyfikacji danych, c. centralnych polityk dostępu w sieci, d. centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
	Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
	Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
	Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
	Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
	Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
	Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: a. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC. b. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:

	– podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, – ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, – odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza, – bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1., c. zdalna dystrybucja oprogramowania na stacje robocze, d. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników, e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego umożliwiające: – dystrybucję certyfikatów poprzez https, – konsolidację CA dla wielu lasów domeny, – automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, – automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509, f. szyfrowanie plików i folderów, g. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), h. szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi, i. możliwość tworzenia systemów wysokiej dostępności (klastry typu failover) oraz rozłożenia obciążenia serwerów, j. serwis udostępniania stron WWW, k. wsparcie dla protokołu IP w wersji 6 (IPv6), l. wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, m. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie nieograniczonej liczby aktywnych środowisk wirtualnych systemów operacyjnych (liczba ograniczona parametrami fizycznymi serwera), n. możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci, o. możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. p. mechanizmy wirtualizacji mające wsparcie dla: – dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, – obsługi ramek typu jumbo frames dla maszyn wirtualnych, – obsługi 4-KB sektorów dysków, – nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, – możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego, q. możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów, r. wsparcie dla rozwiązania Kubernetes,

	s. możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet, t. wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). u. mechanizmy deduplikacji i kompresji na wolumenach, v. mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, w. mechanizm konfiguracji połączenia VPN do platformy Azure. x. wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu, y. mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów, z. możliwość instalacji i poprawnej pracy Systemu Bazodanowego (Microsoft SQL Server Standard),

Tabela nr 6. Szczegółowe wymagania minimalne dla macierzy sieciowej

Macierz sieciowa – 1 szt. (miejsce instalacji: w infrastrukturze serwerowej Zamawiającego)	
Nazwa parametru	**Minimalne wymagania**
Typ obudowy	Macierz musi być przystosowana do montażu w szafie rack 19”. Macierz wyposażona w zdejmowany panel przedni chroniący przed nieuprawionym dostępem do dysków. Możliwość instalacji minimum 24 dysków 2.5” typu Hot-Plug.
Przestrzeń dyskowa	Macierz musi być wyposażona w minimum 10 dysków SAS 10k o pojemności minimum 2,4TB każdy.
Możliwość rozbudowy	Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 240 dysków twardych przez podłączenie półek rozszerzeń i obsługi co najmniej 7PB przestrzeni dyskowej.
Obsługa dysków	Macierz musi obsługiwać dyski 2,5” SSD, SAS i NL SAS. Komunikacja z dyskami 12Gb SAS.
Wydajność	Co najmniej 750k IOPS (Random Read) i 220k IOPS (Random Write)
Sposób zabezpieczenia danych	- Macierz musi obsługiwać mechanizmy RAID zgodne z RAID1, RAID10, RAID5, RAID6 realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków twardych (tzw. wide-striping). - Macierz musi umożliwiać utworzenie pojedynczej grupy RAID zabezpieczonej podwójną parzystością stworzonej ze 128 dysków. Konfiguracja takiej grupy RAID musi umożliwiać zmianę rozmiaru takie grupy poprzez dodawanie i odejmowanie pojedynczych dysków w trybie online bez konieczności przerywania dostępu do danych.
Tryb pracy kontrolerów macierzowych	Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe w sieci FC 32Gb. Kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów FC i LAN.
Pamięć cache	- Każdy kontroler macierzowy musi być wyposażony w minimum 24GB pamięci Cache, 48 GB sumarycznie w macierzy. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. - Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi.

	- Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat.
Rozbudowa pamięci cache	Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash.
Interfejsy do hostów	Macierz musi posiadać, co najmniej 4 porty FC 32Gb obsadzone wkładkami SFP SW 32 Gb/s z możliwością rozbudowy do 8 portów FC 32Gb.
Zarządzanie	- Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej. - Wymagana możliwość autentykacji poprzez LDAP oraz funkcjonalność role-based access control. - Wymaga się możliwości definiowania przynajmniej następujących poziomów dostępu do macierzy: - administrator – pełen dostęp, - monitor – możliwość odczytu konfiguracji.
Kreator konfiguracji	System zarzadzania powinien posiadać funkcjonalność kreatora konfiguracji uruchamianego w przypadku braku zdefiniowanych pul dyskowych i wolumenów, w przypadku braku zdefiniowanych powiadomień oraz braku wykrycia jakichkolwiek zadań wykonywanych na macierzy.
Zarządzanie grupami dyskowymi oraz dyskami logicznymi	Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej. Możliwość tworzenia wolumenów logicznych o pojemności maksymalnej co najmniej 140TB. Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy.
Thin Provisioning	Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie Thin Provisioning. Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP). Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Wewnętrzne kopie migawkowe	Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii. Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Wewnętrzne kopie pełne	Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Migracja danych w obrębie macierzy	Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać

	zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 2 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Zdalna replikacja danych	Macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Podłączanie zewnętrznych systemów operacyjnych	Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami). Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, Linux. Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie.
Redundancja	Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap", a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.
Dodatkowe wymagania	Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych.
Warunki gwarancji	**Co najmniej 36 miesięcy** gwarancji producenta realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia oraz z opcją pozostawienia uszkodzonych dysków. **Uwaga: okres udzielonej gwarancji powinien być nie krótszy niż okres gwarancji zadeklarowany w formularzu oferty**. W okresie gwarancji producenta powinna być możliwość zgłaszania awarii w trybie 8x5 (od poniedziałku do piątku, w godzinach 8 -16) poprzez ogólnopolską linię telefoniczną lub system zgłoszeń producenta, możliwość aktualizacji sterowników i oprogramowania układowego. Obsługa gwarancyjna realizowana przez polski oddział serwisu producenta.
Certyfikaty	Macierz wyprodukowana zgodnie z normą ISO 9001:2008 oraz 14001

Tabela nr 7. Szczegółowe wymagania dla przełącznika do segmentacji sieci LAN

Przełącznik LAN 48-portowy – 1 sztuka (miejsce instalacji: OPS)	
Nazwa parametru	**Minimalne wymagania**

Ilość i typ portów	Minimum 48 portów 100BaseTX/1000BaseT z autonegocjacją (zgodność z IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX, IEEE 802.3ab Type 1000Base-T); duplex 10Base-T/100Base-TX: pół lub pełny duplex; 1000Base-T: tylko pełny duplex;) Minimum 4 porty SFP/SFP+ 1 port szeregowy konsoli RJ45 lub USB
Parametry wydajnościowe	Warstwa przełączania: 3 Tablica routingu: 10000 wpisów (IPv4), 5000 wpisów (IPv6), Prędkość przełączania: 175 Gbps Przepustowość: 110 Mpps Ilość wpisów tablicy adresów MAC: min. 32000 Opóźnienie: <3.8 µs dla 1000 Mbit, <3.0 8 µs dla 10Gbit Ilość obsługiwanych VLAN-ów:min. 512 (802.1q)
Zarządzanie	CLI, SSH, WWW, telnet. Dedykowany port konsolowy do zarządzania poza pasmowego, w pełni niezależny od portów liniowych. Możliwość scentralizowanego zarządzania zarówno przez dedykowane oprogramowanie producenta jak i chmurowo.
Procesor i pamięć	Taktowanie procesora min. 1000MHz min. 4GB pamięci flash min. 1GB DDR3 pamięci RAM
Funkcje wysokiej dostępności	Spanning Tree (802.1d), Rapid Convergence Spanning Tree (802.1w), Muliple Spanning Tree (802.1s), RPVST+
Funkcje stackowania	Obsługa VSF(Virtual Switching Framework) do czterech urządzeń w stosie przez dowolny port uplink
Agregacja portów	zgodna z 802.3ad LACP
QoS	priorytetyzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 4 kolejek, rate-limiting, algorytm opróżniania kolejek WDRR i SP, Voice VLAN, Layer 4 prioritization, Class of Service (CoS)
Monitorowanie	RMON 4 grupy statistics, history, alarm, events, SFLOW
Oprogramowanie	Aktualizacje dostępne na stronie producenta
Pozostałe funkcje	LLDP,LLDP-MED, dual flash images, obsługa ramek typu Jumbo, DHCP snooping, DHCP Server, BPDU Guard, BPDU Protection, izolacja portów, wsparcie dla IPv4 i Ipv6, Tunneled node dla ruchu z AP, Zero Touch Provisioning, wsparcie dla VRRP, obsługa GVRP and MVRP
Obudowa	Umożliwiająca instalację w szafie 19". Wysokość max. 1U.
Moc pobierana maksymalna	50W, zasilacz z certyfikatem 80 PLUS Silver
Zasilanie	200 - 240 VAC
Środowisko pracy	0°C do 45°C
Wyposażenie (dostarczone w komplecie z 2 przełącznikami)	a) Kabel konsolowy. b) Wyposażenie do połącznia przełączników typ 2 i typ 3 (stackowania) o przepływności co najmniej 10Gbit/s z wykorzystaniem portów SFP+. c) Wyposażenie do wykonania 4 połączeń z przełączników do portów LAN serwerów o przepływności co Ethernet 10Gbit/s z wykorzystaniem portów SFP+ w przełącznikach (do połączenia serwerów do przełączników nie dopuszcza się wykorzystywania portów 100BaseTX/1000BaseT przełączników i serwerów). d) Patchcordy Ethernet do połączenia portów zarządzania serwerów, macierzy i przełączników do wydzielonej podsieci zarządzania urządzeniami.
Gwarancja	Dożywotnia (tak długo jak Zamawiający posiada produkt) gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory)

	zapewniająca wysyłkę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii (AHR NBD). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.

Tabela nr 8. Szczegółowe wymagania dla przełączników do segmentacji sieci SAN

Przełącznik zarządzalny do segmentacji sieci SAN – 2 szt. (miejsce instalacji: w serwerowni urzędu)	
Nazwa parametru	**Minimalne wymagania**
Typ urządzenia	Zarządzalny przełącznik sieciowy z obsługą VLAN
Interfejsy	Urządzenie wyposażone co najmniej w interfejsy sieciowe: – 16 x 10Gb SFP+ – 1 x port zarządzania Ethernet PoE Input/RJ45 Porty 10Gb SFP+ powinny być kompatybilne z 1Gb SFP.
Parametry wydajnościowe	Pojemność przełączania co najmniej: 320 Gbps. Łączna przepustowość nieblokująca: 160 Gbps. Obsługa ramek jumbo 10218 bytes.
Obsługa QoS	– 8 kolejek priorytetowania, – Obsługa priorytetowania 802.1p CoS/DSCP, – Kontrola przepustowości, – Ograniczanie prędkości transferu w oparciu o port, – Limit prędkości.
Funkcje L2 i L2+	– Agregacja łączy , – LACP 802.3ad, – Wsparcie RSTP, – Wykrywanie pętli zwrotnych, – ACL, – VLAN per port, – Kontrola przepływu 802.3x, – LLDP
Funkcje VLAN	– W pełni kompatybilny ze standardem IEEE802.1Q – VLAN oparty na portach, – Do 250 wpisów VLAN, – Filtrowanie sieci VLAN,
Bezpieczeństwo	– DHCP & PPPoE Snooping, – Inspekcja ARP, – Ochrona źródłowego adresu IPv4, – Ochrona przed atakami DoS,

	– Ochrona portów poprzez ich statyczną/dynamiczną/stałą konfigurację, – Do 64 adresów MAC na port, – Storm Control Broadcast/Multicast/Unicast, – Kontrola dostępu w oparciu o IP/port/MAC, – Przydzielanie VLAN, – Izolacja portów, – Monitorowanie ruchu sieciowego w czasie rzeczywistym.
Funkcje zarządzania	– Interfejs graficzny GUI, – Interfejs linii poleceń CLI, – SNMP, – RMON.
Wymagania instalacyjne i zasilanie	Przeznaczony do instalacji w szafie rack 19” W zestawie dostarczone elementy wymagane do zainstalowania przełącznika w szafie rack 19” .
Wyposażenie (dostarczone w komplecie z 2 przełącznikami)	a) Kabel konsolowy. b) Okablowanie do wykonania 8 połączeń SAN iSCSI o przepływności co najmniej Ethernet 10Gbit/s z wykorzystaniem portów SFP+ z przełączników do serwerów i kontrolerów macierzy.
Gwarancja	Okres gwarancji co najmniej 36 miesięcy (jednak nie krócej niż okres gwarancji zadeklarowany w formularzu oferty), realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku stwierdzenia jego wady.

Tabela nr 9. Szczegółowe wymagania minimalne dla serwera plików NAS do urzędu

Serwer plików NAS – 1 kpl. (miejsce instalacji: w serwerowni urzędu)	
Nazwa parametru	**Minimalne wymagania**
Typ	Wysokowydajne urządzenie typu NAS w obudowie rack 2U, przeznaczone do pracy ciągłej .
Zastosowanie	Tworzenie kopii zapasowych baz danych, serwerów, maszyn wirtualnych, a także obsługa aplikacji intensywnie korzystających z danych.
Procesor	64-bitowy x86, taktowanie co najmniej do 5,0 GHz. Wbudowany procesor graficzny.
Pamięć operacyjna RAM	16GB RAM min. DDR5, możliwość rozbudowy do 192GB (w systemie co najmniej 4 sloty na kości pamięci RAM)
Pamięć podręczna	5GB pamięci flash (zabezpieczenie dual boot OS)
Pamięć masowa	Obudowa z co najmniej 12 wnękami, w tym: - min. 12 x 3,5”/2,5” SATA 6 Gb/s (HDD/SSD), wymienne na gorąco. Możliwość instalacji:

	- min. 2 x M.2 PCIe Gen 5 (kompatybilne z Gen 3 i 4) (SSD), Zainstalowane dyski co najmniej: - 2x SSD M.2 (NVMe, prędkości odczytu/zapisu co najmniej 3300/2800 MB/s, MTBF >1 700 000 godzin), - 6x HDD 8TB SATA 3,5” (dyski klasy Enterprise, SATA 6 Gb/s, 7200 obr./min, 256 MB cache, MTBF >1 900 000 godzin), **Zainstalowane dyski powinny być dostarczona przez producenta NAS lub być na liście kompatybilności dysków udostępnianej przez producenta NAS.**
Interfejsy	Co najmniej: • 2 x 10GbE RJ 45 (10G/5G/2,5G/1G/100M BASE-T), • 2 x 2.5GbE RJ45 (2,5G/1G/100M BASE-T), • 2 x USB 3.2 Gen 2 (USB-A), • 3 sloty PCIe (2x Gen4 x4, 1x Gen4 x8).
Wymagania instalacyjne	Obudowa 2U do instalacji w szafie rack 19”, w zestawie elementy montażowe.
Bezpieczeństwo danych	Szyfrowanie AES-256 z akceleracją sprzętową, kopie migawkowe, odzyskiwanie danych, chmura prywatna , ochrona przed ransomware.
Parametry niezawodnościowe	Dwa redundantne zasilacze mn. 500W, dyski wymienne na gorąco, RAID 0/1/5/6/10/50/60/JBOD, trunking portów.
Parametry wydajnościowe	1024 migawki na wolumin, 4096 na NAS, obsługa SSD caching, protokoły RTRR, rsync, FTP, CIFS/SMB, NFS, iSCSI. Min. 128 LUN.
Funkcjonalności systemu operacyjnego	- Oparty na jądrze Linux z systemem plików ext4, dostępny przez przeglądarkę i aplikacje mobilne. - Kopie zapasowe: Obsługuje oprogramowanie służące do tworzenia kopii zapasowych plików z komputerów z systemem Windows (Windows), Time Machine (macOS), Aplikacja, która oferuje wszystkie funkcje. Tworzenie kopii zapasowych, odzyskiwanie i synchronizacja danych z/do lokalnej pamięci masowej, usług w chmurze lub zdalnych serwerów korzystających z protokołów RTRR, Rsync, FTP, WebDAV i CIFS/SMB. - Migawki: Rejestracja stanu systemu i danych w dowolnym momencie, ochrona przed ransomware. - Wirtualizacja: System oferuje konteneryzacje (Docker, LXD, Kata Containers) do hostowania aplikacji w kontenerach. - Chmura prywatna: Integracja z chmurą, umożliwiająca zdalny dostęp, synchronizację i udostępnianie plików. - Zarządzanie plikami:(synchronizacja plików między urządzeniami), wyszukiwarka plików, automatyczna organizacja i archiwizacja. - Monitoring: obsługa aplikacji do budowy systemu nadzoru wideo z obsługą kamer IP i nagrywaniem w formacie MP4.

	Rozszerzalność: Centrum aplikacji z ponad 200 aplikacjami (np. VPN) Sieć: Obsługa trunkingu portów, load balancing, wirtualnych przełączników dla środowisk sieciowych. - Elastyczność: Możliwość przełączenia na system oparty na ZFS dla zaawansowanej deduplikacji i redukcji danych w środowiskach SSD.
Warunki gwarancji	**Co najmniej 36 miesięcy gwarancji producenta na urządzenie oraz co najmniej 36 miesięcy gwarancji na dyski.** **Uwaga: okres udzielonej gwarancji powinien być nie krótszy niż okres gwarancji zadeklarowany w formularzu oferty.** W okresie gwarancji producenta powinna być możliwość zgłaszania awarii w trybie 8x5 (od poniedziałku do piątku, w godzinach 8 -16) poprzez ogólnopolską linię telefoniczną lub system zgłoszeń producenta, możliwość aktualizacji sterowników i oprogramowania układowego. Obsługa gwarancyjna realizowana przez polski oddział serwisu producenta lub autoryzowanych partnerów producenta w Polsce.

Tabela nr 10. Szczegółowe wymagania minimalne dla oprogramowania do backup

Oprogramowania do backup – 1 kpl.	
Nazwa parametru	**Minimalne wymagania w zakresie parametrów**
Licencjonowanie	Dostarczona licencja wieczysta umożliwiająca: – Wykonywanie kopii zapasowych **nieograniczonej liczby maszyn wirtualnych** środowisk serwerowego systemu operacyjnego. Licencja powinna obejmować pełną liczbę rdzeni w dostarczonych **2 serwerach fizycznych wraz z obsługą funkcjonalności HA (High Availability)**, – Wykonywanie kopii zapasowych z **70 stacji roboczych** (fizycznych komputerów PC), W ramach licencji dostępne powinno być standardowe wsparcie producenta przez okres najmniej na okres jednego roku.
Bezpieczeństwo	- Szyfrowanie przy użyciu AES256bit, - Ochrona kontenera, - Kopia backupu: • Kopia backupu do lokalnego lub zdalnego repozytorium, • Natywna możliwość wykonywania kopii na napędy taśmowe, • Kopia backupu do usług chmurowych Amazon, Wasabi, itp., • Kopia wszystkich lub tylko ostatniego punktu przywracania, • Odtwarzanie bezpośrednio z kopii • Integracja urządzenia deduplikacyjnego - Ochrona przed ransomware – niezmienna pamięć masowa,
Funkcje	Backup bezagentowy maszyn wirtualnych,

	- obsługa backu w systemach wirtualizacji: • VMmware, • Hyper-V, • Nutanix, • Proxmox, Backup stacji roboczych z systemami Windows i Linux, - Backup przyrostowy typu Forever Incremental, - Pomijanie plików tymczasowych i pliku wymiany, - Replikacja backupu, - Backup inkrementalny VM, - Deduplikacja (NKV) i kompresja, - Kopia backupu, - Wsparcie trybu app-aware dla Windows, - Odtwarzanie plików i obiektów do wybranej maszyny fizycznej- Backup do chmury, - Natywny backup na napędy taśmowe: • obsługa napędów pojedynczych i bibliotek taśmowych, • kopie pełne lub przyrostowe, • zabezpieczenie anty-ransomware, • automatyzacja i harmonogramowanie procesów backu na napędy taśmowe, Zarządzanie napędami i kasetami danych, - Integracja z EMC, HPE, NEC, - Wsparcie urządzeń deduplikujących, co najmniej: • NEC HYDRAstor, • EMC Data Domain, • HPE StoreOnce, • HPE 3PAR, • NetApp, • Quantum DXi, Funkcjonalność Multi-tenant , • podgląd Zdarzeń
Zarządzanie	-Kompresja i deduplikacja w obrębie całego repozytorium backupu, - Możliwość wyszukiwania i kasowania niepotrzebnych backupów, - Weryfikacja backupu migawek, - Funkcje administracyjne (integracja z Microsoft Active Directory, ochrona danych oparta na politykach, hanmonogramy),
Przywracanie danych	- Przywracanie pełnych maszyn wirtualnych, - Przywracanie na poziomie plików - Natychmiastowe odzyskiwanie granularne, - Natychmiastowe przywracania P2V (Physical-to-Virtual), - Natychmiastowe przywracanie obiektów dla MSSQL, - Obcinanie logów transakcyjnych dla MSSQL,

Obsługa systemów	- Wsparcie dla najnowszych systemów wirtualizacji, - Microsoft Hyper-V oraz VMware - Linux RHEL 6.3 - 7.5, - Ubuntu 16.04, 18.04, - SLES 11 - 12 SP3 ,
Integracje i opcje	- Natywny backup na taśmy , - Oszczędność przestrzeni dzięki dwóm rodzajom kompresji software/hardware, - Obsługa backupu on-line aplikacji krytycznych, - Backup off-site, do Amazon Cloud i MS Azure.

Tabela nr 11. Szczegółowe wymagania minimalne dla biblioteki taśmowej

Biblioteka taśmowa wraz z wyposażeniem – 1 kpl. (miejsce instalacji: w infrastrukturze serwerowni UM)	
Nazwa parametru	**Minimalne wymagania**
Obudowa	Przystosowana i dostarczona wraz z niezbędnymi elementami do montażu w szafie 19”, wysokość nie może przekraczać 1U.
Rodzaj napędu	Biblioteka taśmowa musi być wyposażona w napęd LTO-9 SAS o wydajności, co najmniej 300MB/s oraz pojemności pojedynczej taśmy co najmniej 45TB – parametry podane po kompresji danych. Napęd LTO-9 musi umożliwiać wsparcie dla taśm typu WORM i sprzętowe szyfrowanie AES 256-bit. Napęd taśmowy musi być wyposażony w mechanizm dostosowujący automatycznie oraz płynnie prędkość przesuwu taśmy magnetycznej do wartości strumienia danych przekazywanego do napędu w zakresie co najmniej 101-300 MB/s.
Pojemność i sposób wymiany taśm	- Biblioteka musi być wyposażona w co najmniej 8 slotów na taśmy magnetyczne. - Biblioteka powinna posiadać możliwość konfiguracji co najmniej jednego tzw. „mail slot” umożliwiającego wymianę pojedynczej taśmy bez konieczności wyjmowania z biblioteki całego magazynka z taśmami.
Zarządzanie	- Oferowana biblioteka taśmowa musi posiadać możliwość zdalnego zarządzania za pośrednictwem przeglądarki internetowej. Połączenie z siecią Ethernet poprzez dedykowane złącze dostarczane razem z urządzeniem. - Biblioteka powinna posiadać system diagnostyczny – panel operatorski z wyświetlaczem LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie urządzenia.

Odczyt kodów kreskowych	Biblioteka taśmowa musi być wyposażona w czytnik kodów kreskowych od identyfikacji taśm.
Wyposażenie dostarczane wraz z biblioteką	Wraz z biblioteką należy dostarczyć min.: - 8 szt. taśm danych LTO-9 15TB RW, - min. 1 szt. taśmy czyszczącej, - zestaw etykiet kodów kreskowych obejmujący co najmniej 100 etykiet do oznaczania taśm danych i 10 etykiet do oznaczania taśm czyszczących, - kartę SAS do zainstalowania w serwerze Zamawiającego, wymaganą do podłączenia biblioteki taśmowej, - kabel SAS do podłączenia biblioteki.
Trwałość	Parametr MTBF co najmniej 100 000 godzin. Parametr MSBF co najmniej 2 000 000 pełnych cykli „załaduj/wyładuj”.
Złącza i sposób podłączenia	Biblioteka powinna posiadać wbudowane porty: - SAS, - RJ-45 Ethernet, - USB. Port USB powinien być przeznaczony do współpracy ze sprzętowym kluczem USB w celu przechowywania kluczy szyfrujących.
Warunki gwarancji	**Co najmniej 36 miesięcy** gwarancji producenta realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia oraz z opcją pozostawienia uszkodzonych nośników. **Uwaga: okres udzielonej gwarancji powinien być nie krótszy niż okres gwarancji zadeklarowany w formularzu oferty**. W okresie gwarancji producenta powinna być możliwość zgłaszania awarii w trybie 8x5 (od poniedziałku do piątku, w godzinach 8 -16) poprzez ogólnopolską linię telefoniczną lub system zgłoszeń producenta, możliwość aktualizacji sterowników i oprogramowania układowego. Obsługa gwarancyjna realizowana przez polski oddział serwisu producenta.
Dokumentacja	Zamawiający wymaga dokumentacji w języku polskim.
Certyfikaty	Biblioteka wyprodukowana zgodnie z normą ISO 9001:2008 oraz 14001.

Tabela nr 12. Szczegółowe wymagania minimalne dla zasilacza UPS

Systemu podtrzymania zasilania UPS z monitorowaniem środowiska serwerowni – temperatura, wilgotność – 2 kpl. (miejsce instalacji: w serwerownii)	
Nazwa parametru	**Minimalne wymagania**
Rodzaj urządzenia	Zasilacz awaryjny typu UPS
Technologia przetwarzania	Line-interactive o wysokiej częstotliwości (czysta sinusoida, wzmacniacz i ogranicznik)

Moc znamionowa	Co najmniej 3000VA / 3000W
Zakresy napięcia i częstotliwości wejściowej	Co najmniej 150V-294V i 47 do 70 Hz
Zakresy napięcia i częstotliwości wyjściowej	Co najmniej 230 V (+6/-10 %) i 50+/- 0,1%
Gniazdo wejściowe	1 gniazdo IEC C20 (16A)
Gniazda wyjściowe	Co najmniej: - 8 gniazd IEC C13 (10A), - 2 gniazdo C19 IEC (16A), w tym sterowane co najmniej 2 grupy po 2 gniazda.
Czas podtrzymania	Co najmniej 9 min. dla UPS bez modułu bateryjnego przy 50% obciążenia. Co najmniej 40 min. dla UPS z modułem bateryjnym przy 50% obciążenia.
Pomiar parametrów środowiskowych	UPS powinien być wyposażony w moduł umożliwiający rejestrowanie parametrów środowiskowych tj. temperatura i wilgotność oraz posiadać co najmniej 2 styki bezpotencjałowe do podłączenia innych czujników. Zdalne monitorowanie danych środowiskowych powinno być możliwe przy użyciu standardowej przeglądarki internetowej.
Zawartość zestawu	Zakres dostawy powinien obejmować: - zasilacz UPS - moduł komunikacyjny do UPS z interfejsem Ethernet (dopuszcza się zastosowanie UPS z fabrycznie wbudowanym modułem komunikacyjnym) - moduł umożliwiający monitorowanie parametrów środowiskowych W zestawie dostarczone elementy wymagane do zainstalowania w szafie rack 19”.
Wymagania instalacyjne	Urządzenia przeznaczone do instalacji w szafie rack 19”. Wysokość: - zasilacz UPS – max. 2U, - moduł bateryjny – max. 2U. Wykonawca powinien dostarczyć i zainstalować urządzenia w szafie serwerowej w serwerowni rezerwowej oraz podłączyć do zasilania i uruchomić UPS. Moduł komunikacyjny należy podłączyć do sieci i skonfigurować w systemie nadzoru używanym przez Zamawiającego.
Gwarancja	- Co najmniej 36 miesięcy gwarancji producenta na zasilacz UPS i moduł bateryjny, polegającej na

	naprawie lub wymianie urządzenia w przypadku stwierdzenia jego wady. - Uwaga: okres udzielonej gwarancji powinien być nie krótszy niż okres gwarancji zadeklarowany w formularzu ofertowym. - Serwis powinien być realizowany przez producenta rozwiązania lub autoryzowanego przedstawiciela producenta w zakresie serwisu gwarancyjnego, mających swoja siedzibę na terenie Polski.

Tabela nr 13. Szczegółowe wymagania minimalne dla systemu inwentaryzacji i monitorowania zasobów sieci teleinformatycznej

System inwentaryzacji i monitorowania zasobów sieci teleinformatycznej – 1 kpl. (miejsce instalacji: maszyna wirtualna na serwerze w infrastrukturze serwerowej Zamawiającego)	
Nazwa parametru	**Minimalne wymagania**
Licencjonowanie	Dostarczona licencja wieczysta (na czas nieoznaczony) umożliwiająca: – obsługę co najmniej 70 komputerów jednocześnie, – dostęp co najmniej dla 3 administratorów, – dostęp co najmniej 2 serwisantów do obsługi Helpdesku. W ramach licencji dostępne powinno być standardowe wsparcie producenta przez okres gwarancji
Architektura systemu	System powinien oferować architekturę typu klient-serwer, opartą na podstawowych założeniach takich jak: - Klient – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej. - Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej). - Panel pracownika – aplikacja webowa, niewymagająca dodatkowego logowania, dostępna dla pracowników, udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach. - Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z Klientami. - Baza danych – pracująca na silniku Microsoft SQL Server, system powinien zapewniać możliwość obsługi bazy danych w darmowej edycji Express oraz w edycjach komercyjnych tj. Standard lub

	Enterprise. Koszty zapewnienia licencji bazy danych w edycjach komercyjnych pokrywa Zamawiający. - Komponenty systemu (Klient, konsola administracyjna, serwer, baza danych) powinny aktualizować się automatycznie poprzez bezpieczne połączenie. - System powinien zawierć mechanizmy automatycznej konserwacji zgodnie z harmonogramem.
Wymagania systemowe	- Konsola administracyjna powinna działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5 (np. Internet Explorer 11, FireFox, Chrome, Opera). - Klient powinien działać na systemach 32 i 64 bitowych: Windows Server 2012/2012R2/2016/2019/2022/2025, Windows 7/8/8.1/10/11, MacOS 10.7/10.8, Linux dla wersji: Ubuntu v.11.04 lub wyższa, Debian v.6.0 lub wyższa, RedHat v.6.0 lub wyższa, CentOS v.6.0 lub wyższa, Fedora v.16 lub wyższa. - Klient powinien wspierać poniższe przeglądarki internetowe w zakresie monitorowania aktywności użytkownika w sieci: Opera wersja 63.0.3368.94, Chrome wersja 77.0.3865.90, FireFox wersja 69.0.2. - Serwer powinien działać na systemach 64 bitowych: Windows Server 2016/2019/2022/2025, Windows 7/8/8.1/10/11. - Serwer www powinien być oparty o platformę Microsoft 64 bit (Windows Server 2016/2019/2022/2025, Windows 10/11 oraz Java 8 (JRE lub JDK), Apache Tomcat 9. - Baza danych powinna działać na silniku Microsoft SQL Server 2014/2016/2017/2019/2022 w wersji 64 bitowych komercyjnej lub bezpłatnej (np. Microsoft SQL Server Express Edition). - System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare.
Wymagane funkcjonalności systemu zarządzania infrastrukturą IT	- **Funkcjonalność Klienta** - System musi umożliwiać pełne zdalne zarządzanie Klientami, obejmujące uruchamianie i wyłączanie, zmianę konfiguracji Klienta, inicjowanie skanowania oraz wykonanie poleceń systemowych. Klient powinien wyświetlać komunikaty w HTML z dokładnymi danymi o czasie wyświetlenia i użytkowniku. - **Funkcjonalność konsoli administracyjnej** - Konsola administracyjna powinna być wielojęzyczna (polski i angielski) i oferować intuicyjny interfejs z pełnym zestawem funkcji zarządzania (dodawanie, modyfikowanie, usuwanie). Musi także zawierać co najmniej 140 różnorodnych dashboardów, w tym dashboardy użytkownika, prezentujące parametry infrastruktury, sieci oraz bezpieczeństwa. Użytkownicy powinni mieć możliwość samodzielnego konfigurowania dashboardów użytkownika, a dashboardy sieciowe i

	bezpieczeństwa muszą zawierać szczegółowe widżety z informacjami o stanie usług i bezpieczeństwie. W konsoli powinna istnieć funkcja filtrowania danych na dashboardach oraz możliwość personalizacji interfejsu przez użytkownika, w tym definiowanie własnych pól, filtrów i widoków, z zachowaniem tych ustawień pomiędzy sesjami. Konsola musi także umożliwiać definiowanie poziomów uprawnień dla użytkowników i grup, z opcją dziedziczenia oraz integrację z Active Directory dla zarządzania dostępem. Konsola powinna posiadać zaawansowane funkcje zarządzania rekordami, w tym wykonanie poleceń na wielu rekordach jednocześnie oraz dostęp do szczegółowych informacji o pracy urządzeń. - **Funkcjonalność panelu pracownika** - Panel pracownika systemu powinien automatycznie uruchamiać się i autoryzować przy logowaniu użytkownika, z możliwością definiowania zakresu dostępnych informacji przez administratora dla poszczególnych grup pracowników. Panel kierownika powinien dodatkowo agregować i analizować dane z paneli pracowników. Informacje w panelu muszą być organizowane w logiczne sekcje, które można indywidualnie lub grupowo włączać i wyłączać przez administratora. - **Zarządzanie licencjami** - System powinien umożliwiać kompleksowe zarządzanie licencjami w różnych modelach i strukturach organizacyjnych, w tym audyty, zarządzanie oprogramowaniem i oprogramowaniem zabronionym, oraz przypisywanie i rozliczanie różnych typów licencji. Musi także rejestrować historię licencji oraz zapewniać funkcje inwentaryzacji i zdalnej dezinstalacji oprogramowania. - **Wzorce aplikacji i pakietów** - System powinien posiadać rozbudowaną bazę wzorców oprogramowania, umożliwiać definiowanie własnych wzorców i automatycznie importować nowe wzorce od producenta. Musi także dostarczać szczegółowe informacje o zainstalowanych pakietach i ich wykorzystaniu, w tym edycje Microsoft Office. - **Inwentaryzacja sprzętu komputerowego i urządzeń** - System powinien oferować rozbudowane funkcje inwentaryzacji sprzętu komputerowego, włączając automatyczną inwentaryzację zarówno w sieci lokalnej jak i zdalnej, szczegółowe skanowanie komponentów (np. RAM, monitory, dyski twarde) oraz zarządzanie informacjami o zainstalowanym sprzęcie. Powinien także umożliwiać ewidencję zmian konfiguracji sprzętu, identyfikować i klasyfikować urządzenia podłączane do komputerów oraz monitorować historię ich podłączeń. - **Inwentaryzacja urządzeń sieciowych** - System powinien posiadać zdolności do identyfikacji i zarządzania środowiskami wirtualizacji

	Hyper-V i VMware oraz urządzeniami sieciowymi. Wymagane jest posiadanie skanera sieci i SNMP oraz dla środowisk wirtualizacji, które automatycznie zbierają dane, analizują jakość połączeń i identyfikują urządzenia na sieci. System powinien także umożliwiać zdalną instalację Klientów i generowanie map sieci. - **Inwentaryzacja sprzętu** - System musi umożliwiać wszechstronną inwentaryzację sprzętu, włączając urządzenia inne niż komputery (np. drukarki, routery). Musi zapewniać zarządzanie dokumentacją związaną z urządzeniami, monitorować ich ruch oraz przypominać o terminach gwarancji i umowach utrzymaniowych.
Funkcjonalności zarządzania	- **Zdalna administracja komputerami** - System musi oferować kompleksową zdalną administrację komputerami, włączając w to automatyczne wykonywanie dowolnych poleceń (np. zarządzanie aplikacjami, plikami, rejestrami systemowymi) oraz zarządzanie cyklicznymi zadaniami z harmonogramem. Powinien obsługiwać technologię Intel vPro dla zdalnej konfiguracji i zarządzania, a także pozwalać na zdalne przejęcie kontroli nad komputerem za pomocą technologii Ultra VNC, umożliwiając operowanie na wielu sesjach jednocześnie. System powinien integrować zaawansowane mechanizmy skryptowe wspierane przez AI dla automatycznego generowania poleceń oraz umożliwiać zarządzanie i tworzenie zadań cyklicznych z różnorodnymi opcjami cykliczności i zakończenia. System musi zezwalać na wykonywanie zapytań WMI bez zdalnego połączenia do urządzenia. System musi zezwalać na edycję rejestrów urządzenia bez wykorzystania zdalnego połączenia pulpitu. - **Zdalne Zarządzanie Zaporą (Firewall)** - System powinien umożliwiać zdalne zarządzanie zaporą sieciową (firewall) globalnie w infrastrukturze, co obejmuje monitorowanie jej stanu w czasie rzeczywistym, definiowanie złożonych zasad zapory z centralnego panelu administracyjnego oraz szybkie identyfikowanie i reagowanie na potencjalne zagrożenia sieciowe. 1. Automatyzacja, 2. System musi oferować możliwość ustalania harmonogramu dla czynności konserwacyjnych, naprawczych i porządkujących, z opcją ustalania częstotliwości i parametrów wejściowych dla każdej czynności oraz możliwością ich zatrzymania lub uruchomienia. Dodatkowo, system musi posiadać mechanizmy automatyzacji takie jak wykonywanie kopii bezpieczeństwa, identyfikacja aplikacji i pakietów, porządkowanie bazy danych oraz usuwanie nadmiarowych danych. System również powinien wysyłać alerty o zdarzeniach takich jak nowe komputery w bazie

	danych, braki w licencjach i inne zdarzenia krytyczne dla infrastruktury IT. - **Zarządzanie magazynem IT** - System powinien umożliwiać efektywne zarządzanie magazynem IT, włączając obsługę dowolnej ilości magazynów w różnych lokalizacjach oraz obsługę dokumentów magazynowych typu PZ, RW, WZ, i inne. System powinien prowadzić ewidencję materiałów w magazynach zgodnie z metodą FIFO. Ponadto, system powinien umożliwiać automatyczne łączenie dokumentów magazynowych z zasobami systemu oraz zapewniać przegląd wszystkich dokumentów. - **Repozytorium** - Konsola administracyjna systemu powinna być wyposażona w repozytorium dokumentów dowolnego typu, które umożliwia dodawanie nowych dokumentów, przeszukiwanie. Repozytorium powinno także umożliwiać definiowanie kontenerów na dokumenty, co ułatwia organizację i zarządzanie dokumentacją. - **Kody kreskowe** - System powinien wspierać obsługę kodów kreskowych jedno i dwuwymiarowych, umożliwiając parametryzację kodu pod względem wielkości i atrybutów graficznych. System powinien umożliwiać podgląd oraz wydruk kodów kreskowych. - **Wysyłanie wiadomości -** System powinien oferować funkcję komunikatora, umożliwiającą bezpośrednią wymianę wiadomości między użytkownikiem a administratorem systemu, w tym inicjowanie czatu przez administratora oraz przechowywanie historii konwersacji. System powinien także umożliwiać wysyłanie jednorazowych wiadomości ALERT oraz tworzenie szablonów wiadomości do regularnego użytku, z opcją konfiguracji terminu, po którym wiadomość wygaśnie. Ponadto, system powinien wspierać szkolenie pracowników za pomocą wiadomości tekstowych z możliwością definiowania treści szkoleniowych i automatycznego ich wysyłania. System powinien posiadać możliwość eksportu / importu treści. - **Monitorowanie drukarek sieciowych i wydruków** - System musi umożliwić monitorowanie i zarządzanie wydrukami z dowolnej drukarki (lokalnej czy sieciowej), rejestrując szczegółowe informacje o każdym wydruku, w tym koszty, dzięki wbudowanemu cennikowi. System powinien również prognozować przyszłe koszty drukowania oraz pozwalać na zarządzanie drukarkami według różnych parametrów, w tym statusu i materiałów eksploatacyjnych. - **Monitorowanie serwerów WWW** - System musi zapewniać monitorowanie wybranych serwerów WWW, prezentując informacje o ich statusie i aktywności, umożliwiając analizę treści stron oraz graficzną prezentację danych związanych z ich działaniem, w tym czasem odpowiedzi i aktywnością w określonym okresie.

	- **Monitorowanie dziennika zdarzeń** - System musi posiadać zdolność do monitorowania dziennika zdarzeń komputerów, umożliwiając definiowanie i filtrowanie zdarzeń według różnych kategorii. System musi umożliwiać monitorowanie komunikatów Syslog. - **Monitorowanie pracy komputerów** - System musi oferować monitorowanie pracy komputerów, w tym dat startu i zakończenia pracy, logowania użytkowników, a także zdalne monitorowanie sesji połączeń, rejestrując szczegóły takie jak adresy IP i dane użytkowników. Monitorowanie uprawnień ACL - System musi umożliwić skanowanie i monitorowanie uprawnień ACL, oferując szczegółowe raporty, automatyczną aktualizacją danych i filtrami do zarządzania informacjami. - **Monitorowanie sensorów** - System musi integrować monitoring warunków środowiskowych za pomocą sensorów po SNMP, umożliwiając graficzną prezentację danych, wysyłanie alertów. - **Repozytorium CMDB** - System musi posiadać zintegrowane repozytorium CMDB, umożliwiające zarządzanie zasobami IT, w tym szczegółowe informacje o użytkownikach, urządzeniach, licencjach, a także o oprogramowaniu i jego licencjach, z możliwością importu i eksportu danych. - **Worktime manager** - System musi umożliwiać monitorowanie i analizę czasu pracy użytkowników, z możliwością definiowania grup przypisanych do przełożonych i prezentacji szczegółowych danych o aktywności użytkowników w formie widżetów i danych analitycznych. Informacje o czasie pracy, sesjach, aktywności w aplikacjach oraz produktywności powinny być możliwe do udostepnienia w panelu pracownika. - **Raportowanie i eksport danych** - System musi oferować zaawansowane możliwości raportowania i eksportu danych, umożliwiając wyeksportowanie informacji do różnych formatów, w tym xls, csv, html, oraz graficznych. Powinien także wspierać generowanie wieloparametrycznych raportów z możliwością stosowania filtrów, obsługę wieloinstancyjności raportowania oraz integrację z narzędziami do tworzenia raportów takimi jak SAP Crystal Reports i Stimulsoft, obejmując co najmniej 150 zdefiniowanych raportów. Dodatkowo, system musi posiadać możliwość konfiguracji harmonogramu umożliwiającego cykliczne wysyłanie raportów oraz zapisywanie ich w dowolnym miejscu, z automatycznym generowaniem raportu w formacie PDF jako wynikiem wykonania harmonogramu. - **Interfejs API** - System musi oferować rozbudowany interfejs API, umożliwiający komunikację za pomocą REST API. Musi on zapewniać szyfrowaną komunikację z użyciem protokołu TLS 1.3 oraz możliwość

	tworzenia złożonych requestów JSON. Klucze zabezpieczeń powinny być modyfikowalne i mogą mieć co najmniej 32 znaki. - **Powiadomienia** - System musi umożliwiać generowanie różnorodnych powiadomień, w tym alertów w konsoli, e-maili oraz wiadomości SMS, z możliwością edycji treści powiadomień i definiowania grup odbiorców. Powinien obsługiwać automatyczne wywoływanie zadań i integrować się z CMD oraz Windows PowerShell, zapewniając co najmniej 30 predefiniowanych powiadomień oraz możliwość ich personalizacji. - **Bezpieczeństwo** - System musi zapewniać rozbudowane funkcje bezpieczeństwa, w tym definicję i zarządzanie prawami dostępu oraz zaawansowane opcje uwierzytelniania. Wymaga silnych haseł, obsługuje wieloskładnikowe uwierzytelnianie i posiada mechanizmy szyfrowania danych.
Zarządzanie poprawkami / aktualizacjami	System powinien zapewniać zdalne i automatyczne zarządzanie pobieraniem i instalacją aktualizacji systemu Windows bez konieczności ingerencji użytkownika na wszystkich obsługiwanych komputerach. System powinien pozwalać na wymuszenie aktualizacji oraz kontrolować aktualną wersję systemu
Helpdesk	- System powinien umożliwiać obsługę zgłoszeń technicznych użytkowników. Formularz zgłoszeniowy powinien być dostępny dla użytkownika z poziomu dedykowanego panelu użytkownika. - System helpdesku powinien zapewniać możliwość tworzenia własnych kategorii, priorytetów i statusów zgłoszeń oraz przekazywać powiadomienia o zmianie statusu zgłoszeń.
Wsparcie i pomoc techniczna	- Wsparcie i pomoc techniczna powinna być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00. - Utrzymaniem Oprogramowania jest zapewnienie aktualizacji Oprogramowania (asysta techniczna) oraz nieprzerwanego działania Oprogramowania (usługi SLA), jak również zapewnienie świadczenia innych usług wspomagających korzystanie z Oprogramowania. - Czas trwania usługi SLA wynosi 24 miesięcy od dnia zakupu.

f