



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

Numer sprawy: RIBMG.7031.2.2026.PK

Rossosz, dnia 22.01.2026 r.

Szczegółowy Opis Przedmiotu Zamówienia

na dostawy sprzętu i oprogramowania związane z realizacją projektu
w ramach grantu

„Cyberbezpieczny Samorząd”



Cyberbezpieczny
Samorząd

Spis treści

1. Zestawienie ilościowe.....	3
2. Zasada równoważności rozwiązań i neutralności technologicznej.	4
3. Przedmiot zamówienia dla Części nr 1.	7
3.1. Wymagania ogólne.....	7
3.2. Zakup UPS (1 szt.).....	10
3.3. Zakup UTM (1 szt.).....	11
4. Przedmiot zamówienia dla Części nr 2.	13
4.1. Wymagania ogólne.....	13
4.2. Zakup NAS (1 szt.).....	17
4.3. Zakup oprogramowania do backup (1 szt.).....	18
5. Opis przedmiotu zamówienia części nr 3.	20
5.1. Wymagania ogólne.....	20
5.2. Rozbudowa oprogramowania antywirusowego o funkcje XDR, szyfrowanie danych, analizę podatności (1 szt.).....	24
5.3. Zakup oprogramowania do zarządzania bezpieczeństwem IT (DLP, monitoring zasobów, zarządzanie dostępem).	33

1. Zestawienie ilościowe.

Część nr 1 – Dostawa UPS i UTM.

Lp.	Nazwa	Ilość
1.	Zakup UPS	1 szt.
2.	Zakup UTM	1 szt.

Część nr 2 – Dostawa systemu backup.

Lp.	Nazwa	Ilość
1.	Zakup oprogramowania do backup	1 szt.
2.	Zakup NAS	1 szt.

Część nr 3 – Dostawa oprogramowania informatycznego.

Lp.	Nazwa	Ilość
1.	Rozbudowa oprogramowania antywirusowego o funkcje XDR, szyfrowanie, analizę podatności	1 szt.
2.	Zakup oprogramowania do zarządzania bezpieczeństwem IT (DLP, monitoring zasobów, zarządzanie dostępem)	1 szt.

2. Zasada równoważności rozwiązań i neutralności technologicznej.

1. Za równoważne do wyspecyfikowanego rozwiązania Zamawiający uzna rozwiązanie o tym samym przeznaczeniu, cechach technicznych, jakościowych i funkcjonalnych odpowiadających cechom technicznym, jakościowym i funkcjonalnym wskazanych w opisie przedmiotu zamówienia, lub lepszych, oznaczonych innym znakiem towarowym, patentem lub pochodzeniem.
2. Rozwiązanie równoważne musi pozwalać na zrealizowanie zakładanego przez Zamawiającego celu poprzez parametry wydajnościowe i funkcjonalne, mające wpływ na skuteczność działania, takie same lub lepsze od wskazanych wymagań minimalnych.
3. Użycie w opisie przedmiotu zamówienia nazw rozwiązań służy ustaleniu minimalnego standardu wykonania i określenia właściwości i wymogów technicznych założonych w dokumentacji technicznej dla projektowanych rozwiązań lub też stosowane jest w celu wskazania aktualnie użytkowanego środowiska Zamawiającego, z którym rozwiązanie równoważne powinno być kompatybilne.
4. Wykonawca zobligowany jest do wykazania, że oferowane rozwiązania równoważne spełnią zakładane wymagania minimalne. Wykonawca, który złoży ofertę na produkty równoważne musi do oferty załączyć dokumenty zawierające dokładny opis oferowanych produktów, z którego wynikać będzie zachowanie warunków równoważności. Wykonawca, który posługuje się równoważnymi certyfikatami musi je załączyć do oferty. Przez certyfikat równoważny Zamawiający rozumie certyfikat analogiczny co do zakresu z certyfikatami wskazanymi z nazwy, który potwierdza spełnianie normy charakteryzującej się cechami właściwymi dla normy wymienionej przez Zamawiającego, wystawiony przez niezależny podmiot uprawniony do wystawiania certyfikatów.
5. Brak określenia „minimum” oznacza wymaganie na poziomie minimalnym, a Wykonawca może zaoferować rozwiązanie o lepszych parametrach.
6. W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega lub jest lepsze od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym.
7. Nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób.
8. Przez bardzo zbliżoną (podobną) wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic nie wpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego.
9. W przypadku wskazania przez Zamawiającego określonych testów wydajności Zamawiający zastrzega, iż w celu sprawdzenia poprawności przeprowadzonych testów może wezwać

Wykonawcę do przedstawienia wskazanego przez Zamawiającego oprogramowania testującego wraz z testowanym urządzeniem i/lub oprogramowaniem. Wszystkie testy wydajnościowe wykonawca musi przeprowadzić w oferowanej konfiguracji, przy automatycznych ustawieniach konfiguratora oprogramowania testującego i natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzeniach. Nie dopuszcza się stosowania overclockingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację), jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający dopuszcza prowadzenie testów wydajnościowych w oparciu o dowolny system operacyjny zainstalowany na urządzeniu.

10. W przypadku wskazania przez Zamawiającego określonych testów wydajności Zamawiający dopuszcza równoważne im testy wydajnościowe umożliwiające potwierdzenie zakładanych poziomów wydajności. W przypadku użycia przez Wykonawcę równoważnych testów wydajności Zamawiający zastrzega, iż w celu sprawdzenia równoważności przeprowadzonych testów Wykonawca może zostać wezwany do dostarczenia Zamawiającemu wskazanego przez Zamawiającego oprogramowania testującego i równoważnego do niego oprogramowania testującego wraz z testowanym urządzeniem i/lub oprogramowaniem. Wszystkie testy wydajnościowe wykonawca musi przeprowadzić w oferowanej konfiguracji, przy automatycznych ustawieniach konfiguratora oprogramowania testującego i natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzeniach. Nie dopuszcza się stosowania overclockingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację), jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający dopuszcza prowadzenie testów wydajnościowych w oparciu o dowolny system operacyjny zainstalowany na urządzeniu.
11. Dodatkowo, wszędzie tam, gdzie zostało wskazane pochodzenie (marka, znak towarowy, producent, dostawca itp.) materiałów lub normy, aprobaty, specyfikacje i systemy, o których mowa w ustawie Prawo Zamówień Publicznych (zwana dalej ustawą), Zamawiający dopuszcza oferowanie sprzętu lub rozwiązań równoważnych pod warunkiem, że zapewnią uzyskanie parametrów technicznych takich samych lub lepszych niż wymagane przez Zamawiającego w dokumentacji przetargowej. Zamawiający dopuszcza oferowanie materiałów lub urządzeń równoważnych. Materiały lub urządzenia pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, a także jakościowe (m.in.: wymiary, skład, zastosowany materiał, kolor, odcień, przeznaczenie materiałów i urządzeń, estetyka itp.) jakim muszą odpowiadać materiały lub urządzenia oferowane przez Wykonawcę, aby zostały spełnione wymagania stawiane przez Zamawiającego. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Posługiwanie się nazwami producentów / produktów ma wyłącznie charakter przykładowy. Zamawiający, wskazując oznaczenie konkretnego producenta (dostawcy), konkretny produkt lub materiały przy opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych lub lepszych parametrach. Zamawiający opisując przedmiot zamówienia przy pomocy określonych norm, aprobat czy specyfikacji technicznych i systemów odniesienia dopuszcza rozwiązania równoważne opisywanym. Wykonawca, który powołuje się na rozwiązania równoważne

opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów uwiarygodniających te rozwiązania.

3. Przedmiot zamówienia dla Części nr 1.

3.1. Wymagania ogólne.

1. Dostarczony sprzęt i oprogramowanie muszą być wolne od wad prawnych i fizycznych oraz nienoszący oznak użytkowania.
2. Dostarczony sprzęt i oprogramowanie muszą być fabrycznie nowe (tzn. wyprodukowane nie wcześniej, niż na 9 miesięcy przed ich dostarczeniem), muszą pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez producenta dla oferowanego modelu sprzętu i oprogramowania.
3. Niedopuszczalne są produkty prototypowe, nie dopuszcza się urządzeń długotrwale magazynowanych oraz pochodzących z programów wyprzedażowych producenta. Urządzenia nie mogą znajdować się na liście „end-of-sale”, „end-of-support”, „end-of-life” producenta lub innych listach prowadzonych przez producentów produktów świadczących o tym, że produkt został wycofany ze sprzedaży, wsparcie dla niego zostało zakończone lub producent zaprzestaje wydawania aktualizacji, poprawek bezpieczeństwa czy też napraw dla produktu.
4. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy) jakichkolwiek portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, itp., niedopuszczalne jest zastosowanie jakichkolwiek zewnętrznych przejściówek czy konwerterów. Niedopuszczalna jest realizacja tylko części funkcji bądź wymaganych standardów zamiast innych określonych jako minimalne w niniejszym dokumencie. Wszystkie wymagania minimalne muszą zostać zapewnione przez dostarczane produkty bez konieczności zakupu żadnych dodatkowych elementów przez Zamawiającego, chyba że z niniejszego dokumentu wynika inaczej.
5. Wszystkie urządzenia będą zasilane bezpośrednio z sieci 230V.
6. Wykonawca zapewni dostawę do wskazanej lokalizacji w siedzibie Zamawiającego.
7. Wykonawca jest odpowiedzialny za skonfigurowanie połączeń fizycznych, logicznych, podłączenie i skonfigurowanie urządzeń do działania, pozwalające na rozpoczęcie pracy oraz dostarczenie odpowiedniej ilości kabli zasilających, połączeniowych w celu przygotowania zamawianego sprzętu do działania.
8. Wykonawca zobowiązany jest do skonfigurowania zamawianego sprzętu w uzgodnieniu z Zamawiającym.
9. Prace instalacyjne będzie można realizować wyłącznie w terminach uzgodnionych z Zamawiającym.
10. Wykonawca będzie zobowiązany do złożenia dokumentacji powykonawczej, zawierającej w szczególności wszystkie dane dostępu do urządzeń i oprogramowania, które będą wykorzystywane podczas instalacji i konfiguracji sprzętu i oprogramowania.
11. Dla dostaw sprzętu informatycznego z oprogramowaniem Zamawiający wymaga fabrycznie nowego oprogramowania (nieużywanego nigdy wcześniej), w wersji z certyfikatem autentyczności dla każdej licencji, o ile producent oferowanego oprogramowania stosuje certyfikaty autentyczności. Wykonawca zobowiązany jest do dostarczenia fabrycznie nowego oprogramowania (w tym systemu operacyjnego) nieużywanego oraz nigdy wcześniej nieaktywowanego na innym urządzeniu oraz pochodzącego z legalnego źródła sprzedaży. W przypadku oprogramowania naklejka hologramowa winna być zabezpieczona przed możliwością odczytania klucza za pomocą zabezpieczeń stosowanych przez producenta, o ile producent

oferowanego oprogramowania stosuje takie zabezpieczenia. Zamawiający zastrzega możliwość weryfikacji dostarczonego oprogramowania na etapie oceny ofert jak i na etapie dostawy pod kątem legalności oprogramowania bezpośrednio u producenta oprogramowania. Zamawiający zastrzega możliwość żądania od Wykonawcy na etapie dostawy przedstawienia dokumentów dotyczących zakupu oprogramowania (faktury, rachunki) w autoryzowanym kanale dystrybucyjnym producenta oprogramowania.

12. Dla dostaw oprogramowania Zamawiający wymaga fabrycznie nowego oprogramowania (nieużywanego nigdy wcześniej), w wersji z certyfikatem autentyczności dla każdej licencji, o ile producent oferowanego oprogramowania stosuje certyfikaty autentyczności. Wykonawca zobowiązany jest do dostarczenia fabrycznie nowego oprogramowania, nieużywanego oraz nigdy wcześniej nieaktywowanego oraz pochodzącego z legalnego źródła sprzedaży. W przypadku oprogramowania posiadającego fizyczny nośnik naklejka hologramowa winna być zabezpieczona przed możliwością odczytania klucza za pomocą zabezpieczeń stosowanych przez producenta, o ile producent oferowanego oprogramowania stosuje takie zabezpieczenia. Zamawiający zastrzega możliwość weryfikacji dostarczonego oprogramowania na etapie oceny ofert jak i na etapie dostawy pod kątem legalności oprogramowania bezpośrednio u producenta oprogramowania. Zamawiający zastrzega możliwość żądania od Wykonawcy na etapie dostawy przedstawienia dokumentów dotyczących zakupu oprogramowania w autoryzowanym kanale dystrybucyjnym producenta oprogramowania.
13. Wymagania instalacyjne i wdrożeniowe dla dostarczonego sprzętu i oprogramowania:
 - a. Instalacja ma odbyć się na komputerach oraz serwerach wskazanych przez Zamawiającego, a w przypadku jeżeli dostarczone oprogramowanie działa w modelu rozwiązania chmurowego to Wykonawca jest zobligowany do konfiguracji oprogramowania w chmurze Wykonawcy bądź Producenta oferowanego oprogramowania.
 - b. Zamawiający dopuszcza instalację i wdrożenie zdalne przy wykorzystaniu narzędzia Wykonawcy, z zastrzeżeniem, że Wykonawca jest zobowiązany dostarczyć oprogramowanie do zdalnej pracy umożliwiające szyfrowanie połączeń oraz nagrywanie sesji serwisowych.
 - c. W przypadku jeżeli dotyczy, Wykonawca wykona wdrożenie na wybranym serwerze/maszynie wirtualnej wskazanym przez Zamawiającego oraz na stanowiskach wskazanych przez Zamawiającego.
 - d. Wykonawca, pomimo zapewnienia serwisu producenta zobowiązany będzie do udzielania pomocy technicznej Zamawiającemu przez okres gwarancji.
 - e. Usługa wsparcia wdrożenia obejmuje:
 - i. przeprowadzenie analizy przedwdrożeniowej,
 - ii. pomoc przy instalacji silnika bazy danych – jeżeli będzie wymagana instalacja,
 - iii. rejestracja produktu – jeżeli wymagana,
 - iv. instalację oprogramowania: na stacji roboczej lub serwerze – jeżeli dotyczy,
 - v. dystrybucję oprogramowania na wybranych stacjach roboczych – jeżeli dotyczy,
 - vi. konfigurację oprogramowania,
 - vii. optymalizację ustawień pod wymogi sieciowe i sprzętowe Zamawiającego,
 - viii. szkolenie administratorów z zakresu pracy z programem,
 - ix. w uzgodnionym terminie z Zamawiającym zostanie przeprowadzane kontrolne połączenie zdalne w celu weryfikacji ustawień oraz poprawienia konfiguracji.
14. Proces współpracy między Wykonawcą a Zamawiającym w celu wdrożenia sprzętu i oprogramowania – wymagania minimalne:

- a. Wykonawca przygotowuje projekt techniczny realizacji koncepcji, uwzględniający dobre praktyki i rekomendacje eksploatacyjne publikowane przez producentów wdrażanego sprzętu i oprogramowania, po wykonaniu analizy istniejącego u Zamawiającego rozwiązania wraz z koncepcją uwzględniające obecne u Zamawiającego uwarunkowania organizacyjne i sprzętowe, łącznie zwane dalej projektem technicznym. W projekcie technicznym muszą być zawarte:
 - i. scenariusze testowe, procedury oraz wzory raportów testów,
 - ii. szczegółowy harmonogram realizacji prac wdrożeniowych i migracyjnych, uwzględniający specyfikę organizacji Zamawiającego,
 - iii. opis koncepcji realizacji prac,
 - iv. zalecenia przedwdrożeńowe dla Zamawiającego, jeżeli będą wymagane.
 - b. Akceptacja projektu technicznego wraz z procedurami oraz wzorami raportów z testów będzie podlegała następującej procedurze:
 - i. Wykonawca przekaże do akceptacji Zamawiającego, drogą elektroniczną projekt techniczny wraz z procedurami oraz wzorami raportów z testów, w terminie nie dłuższym niż 10 dni roboczych od dnia zawarcia umowy,
 - ii. Zamawiający w terminie nie dłuższym niż 5 dni roboczych od dnia dostarczenia przez Wykonawcę kompletnych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
 - iii. wszystkie uwagi do dokumentów zgłoszone przez Zamawiającego zostaną wprowadzone przez Wykonawcę, w terminie nie dłuższym niż 5 dni roboczych od dnia ich otrzymania,
 - iv. Zamawiający w terminie 5 dni roboczych od dnia powtórnego dostarczenia przez Wykonawcę poprawionych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
 - v. w przypadku nieuwzględnienia uwag Zamawiającego, Zamawiający zastrzega sobie prawo do wskazania ostatecznego terminu dostarczenia projektu technicznego wraz z procedurami oraz wzorami raportów z testów,
 - vi. zatwierdzony projekt techniczny wraz z procedurami zostaną przekazane Zamawiającemu w 1 egzemplarzu oraz w formie elektronicznej na pendrive, w postaci plików do edycji i PDF.
 - c. Wykonawca zrealizuje wdrożenia i migracje zgodnie z zakresem prac i projektem technicznym.
 - d. Wykonawca przeprowadzi testy akceptacyjne wdrożonych rozwiązań.
 - e. Wykonawca opracuje i przedstawi raport z testów. W przypadku zrealizowania scenariusza testowego z wynikiem negatywnym, Wykonawca przedstawi nowe rozwiązanie wadliwego elementu systemu i przeprowadzi ponowny test wg scenariusza, w terminie wyznaczonym przez Zamawiającego, dochowując terminu wykonania Umowy. Raport z testów powinien zawierać listę przeprowadzonych testów wraz z ich wynikiem.
 - f. Wykonawca opracuje dokumentację powykonawczą oraz procedury administracyjne i eksploatacyjne w zakresie uzgodnionym z Zamawiającym, w tym: dokumentację wdrożeniową, procedury operacyjne, procedury „Disaster Recovery”. Akceptacja dokumentacji powykonawczej będzie przebiegała zgodnie z zasadami określonymi dla akceptacji projektu technicznego.
15. Instruktaże w zakresie dostarczonego sprzętu i oprogramowania – wymagania minimalne.

- a. Instruktaże stanowiskowe będą prowadzone w języku polskim w siedzibie Zamawiającego i obejmą zakresem m.in.: użytkowane oprogramowanie; budowę, architekturę i konfigurację rozwiązania; administrowanie wdrożonym rozwiązaniem.
 - b. Instruktaże stanowiskowe zostaną przeprowadzone przez osoby prowadzące prace wdrożeniowe w ramach niniejszego zamówienia.
 - c. Instruktaże powinny trwać minimum 8 godzin lekcyjnych (45 minut) i będą przeprowadzone dla wskazanej przez Zamawiającego liczby osób (maksymalnie 2 osoby).
 - d. Zamawiający dopuszcza przeprowadzenia instruktaży w trybie zdalnym (online).
 - e. Administratorzy rozwiązania po zakończeniu Instruktaży stanowiskowych muszą w szczególności umieć wykonywać czynności administracyjne, a także instalacji oprogramowania, znać i umieć realizować procedury backupu. Ponadto powinni znać typowe zagrożenia i problemy związane z funkcjonowaniem rozwiązania, a także sposoby ich przeciwdziałania, wykrywania i usuwania. Powinni umieć instalować, konfigurować, rekonfigurować, monitorować i prawidłowo eksploatować wdrożone rozwiązanie, jak również znać jego wdrożoną konfigurację.
16. W poniżej wskazanych wymaganiach Zamawiający posługuje się terminami „musi”, „powinien”, „możliwość” określając w ten sposób wymaganą funkcjonalność oprogramowania.

3.2. Zakup UPS (1 szt.).

Minimalne parametry techniczne urządzenia:

1. Typ obudowy: RACK, max 2U, Wykonawca jest zobowiązany dostarczyć szyny do montażu UPS w szafie RACK.
2. Moc pozorna: min. 3000 VA.
3. Moc rzeczywista: min. 2700 W.
4. Architektura UPSa: line-interactive lub online.
5. Typ przebiegu: sinusoidalny.
6. Liczba i rodzaj gniazdek z utrzymaniem zasilania: min. 8x IEC320 C13.
7. Typ gniazda wejściowego: C14 lub C20.
8. Czas podtrzymania dla obciążenia 100%: min. 3 min.
9. Czas podtrzymania przy obciążeniu 50%: min. 10 min.
10. Zabezpieczenia: przeciwprzepięciowe, przeciwzwarceniowe, przeciwprzeciążeniowe.
11. Wyświetlacz LCD lub diody LED sygnalizujące stan pracy urządzenia.
12. Alarmy dźwiękowe urządzenia sygnalizujące stan pracy urządzenia w zakresie określonych przez producenta zdarzeń.
13. Interfejsy: min. 1 x USB, 1 x RJ45.
14. Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowany UPS spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci deklaracji RoHS dla produktu lub oświadczenia producenta UPS lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda załączenia do oferty

przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowane UPSy wymagań w zakresie określonym powyżej.

15. Gwarancja producenta: min. 24 miesiące.

3.3. Zakup UTM (1 szt.).

W ramach działania przewiduje się zakup urządzenia UTM wraz z licencjami subskrypcyjnymi. Subskrypcja musi umożliwić Zamawiającemu korzystanie z aktualnych baz funkcji ochronnych producenta i serwisów oraz obejmować firewall, IPS, kształtowanie pasma, antywirus, antyspam, web filtering. W ramach przedmiotu zamówienia Wykonawca musi zapewnić także wsparcie techniczne, które może być tylko realizowane przez producenta, dystrybutora, bądź oficjalnego partnera dystrybutora. Subskrypcja dla urządzenia UTM obejmująca wszystkie wymagania wskazane powyżej musi być dostarczona na okres do dnia 26.06.2026 r. niezależnie od oferowanych modeli licencjonowania producenta.

Minimalne wymagania techniczne urządzenia:

1. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza.
2. System musi wspierać IPv4 oraz IPv6 w zakresie minimum: firewall, ochrony IPS oraz usług sieciowych.
3. Interfejsy: liczba portów Ethernet 2,5 Gbps – min. 8; liczba portów światłowodowych 1 Gbps – min. 1; urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
4. Wydajność:
 - Przepustowość firewall – co najmniej 4 Gbps,
 - Liczba równoległych sesji – co najmniej 0,3 mln,
 - Przepustowość IPS – co najmniej 1 Gbps,
 - Liczba jednoczesnych klientów SSL VPN – co najmniej 50.
5. Funkcje Systemu Bezpieczeństwa dostępne w ramach dostarczonej licencji:
 - Komercyjny antywirus,
 - Firewall,
 - Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN,
 - Ochrona przed atakami - Intrusion Prevention System,
 - Kontrola stron WWW,
 - Kontrola zawartości poczty – Antyspam,
 - Zarządzanie pasmem (Traffic shaping),
 - Analiza ruchu szyfrowanego protokołem SSL.
6. Polityki firewall:
 - Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, IPS i aplikacje, reakcje zabezpieczeń, rejestrowanie zdarzeń,
 - System musi zapewniać translację adresów NAT oraz PAT,
7. Połączenia VPN:
 - System musi umożliwiać konfigurację połączeń typu IPSec VPN,

- System musi umożliwiać konfigurację połączeń typu SSL VPN.
8. Routing i obsługa łącz WAN:
- W zakresie routingu rozwiązanie powinno zapewniać obsługę: routingu statycznego, Policy Based Routingu, protokołów dynamicznego routingu,
 - System musi umożliwiać obsługę kilku (co najmniej dwóch) łącz WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia.
9. Kontrola antywirusowa:
- Administrator musi mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym,
 - Administrator musi mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji.
10. Ochrona przed atakami:
- Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS,
 - Moduł IPS musi nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia,
 - Urządzenie musi umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS,
 - Administrator musi mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP,
 - Urządzenie musi umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0,
 - Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.
11. Kontrola WWW:
- Urządzenie musi posiadać wbudowany filtr URL,
 - Filtr URL musi działać w oparciu o klasyfikację URL,
 - Administrator musi mieć możliwość dodawania własnych kategorii URL,
 - Administrator musi mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru musi być przynajmniej:
 - i. blokowanie dostępu do adresu URL,
 - ii. zezwolenie na dostęp do adresu URL,
 - iii. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora,
 - Administrator musi mieć możliwość skonfigurowania stron z komunikatem o zablokowaniu strony,
 - Filtr URL musi uwzględniać komunikację po protokole HTTPS,
 - Urządzenie musi umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane,
 - Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania.
12. Uwierzelnianie użytkowników w ramach sesji:
- System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą co najmniej haseł statycznych,

- Rozwiązanie musi umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory.

13. Zarządzanie:

- Konfiguracja urządzenia musi być możliwa z wykorzystaniem polskiego interfejsu graficznego,
 - Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS,
 - Urządzenie musi umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami,
 - Urządzenie musi umożliwiać zarządzanie z poziomu konsoli (SSH),
 - Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup,
 - Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników,
 - Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog),
 - Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa),
14. Urządzenie powinno umożliwiać monitorowanie logów ruchu, administracja urządzenia musi być możliwa poprzez graficzny interfejs zarządzania, rozwiązanie powinno umożliwiać wysyłanie alarmów przez SNMP lub e-mail, urządzenie powinno mieć możliwość generowania raportów.
15. Urządzenie musi posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
16. W ramach Zamówienia Wykonawca dostarczy licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować firewall, IPS, kształtowanie pasma, antywirus, antyspam, web filtering na okres do dnia 26.06.2026 r.
17. Urządzenie musi być objęte serwisem gwarancyjnym producenta na okres do dnia 26.06.2026 r. obejmującym w przypadku zgłoszenia awarii urządzenia, wysyłkę urządzenia zastępczego lub wysyłkę sprawnego urządzenia w dniu potwierdzenia awarii, a dostawa takiego urządzenia na wskazany przez zgłaszającego adres zaplanowana musi zostać na kolejny dzień roboczy.

4. Przedmiot zamówienia dla Części nr 2.

4.1. Wymagania ogólne.

1. Dostarczony sprzęt i oprogramowanie muszą być wolne od wad prawnych i fizycznych oraz nienoszący oznak użytkowania.
2. Dostarczony sprzęt i oprogramowanie muszą być fabrycznie nowe (tzn. wyprodukowane nie wcześniej, niż na 9 miesięcy przed ich dostarczeniem), muszą pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez producenta dla oferowanego modelu sprzętu i oprogramowania.
3. Niedopuszczalne są produkty prototypowe, nie dopuszcza się urządzeń długotrwale magazynowanych oraz pochodzących z programów wyprzedażowych producenta. Urządzenia nie mogą znajdować się na liście „end-of-sale”, „end-of-support”, „end-of-life” producenta lub innych

listach prowadzonych przez producentów produktów świadczących o tym, że produkt został wycofany ze sprzedaży, wsparcie dla niego zostało zakończone lub producent zaprzestaje wydawania aktualizacji, poprawek bezpieczeństwa czy też napraw dla produktu.

4. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy) jakichkolwiek portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, itp., niedopuszczalne jest zastosowanie jakichkolwiek zewnętrznych przejściówek czy konwerterów. Niedopuszczalna jest realizacja tylko części funkcji bądź wymaganych standardów zamiast innych określonych jako minimalne w niniejszym dokumencie. Wszystkie wymagania minimalne muszą zostać zapewnione przez dostarczane produkty bez konieczności zakupu żadnych dodatkowych elementów przez Zamawiającego, chyba że z niniejszego dokumentu wynika inaczej.
5. Wszystkie urządzenia będą zasilane bezpośrednio z sieci 230V.
6. Wykonawca zapewni dostawę do wskazanej lokalizacji w siedzibie Zamawiającego.
7. Wykonawca jest odpowiedzialny za skonfigurowanie połączeń fizycznych, logicznych, podłączenie i skonfigurowanie urządzeń do działania, pozwalające na rozpoczęcie pracy oraz dostarczenie odpowiedniej ilości kabli zasilających, połączeniowych w celu przygotowania zamawianego sprzętu do działania.
8. Wykonawca zobowiązany jest do skonfigurowania zamawianego sprzętu w uzgodnieniu z Zamawiającym.
9. Prace instalacyjne będzie można realizować wyłącznie w terminach uzgodnionych z Zamawiającym.
10. Wykonawca będzie zobowiązany do złożenia dokumentacji powykonawczej, zawierającej w szczególności wszystkie dane dostępu do urządzeń i oprogramowania, które będą wykorzystywane podczas instalacji i konfiguracji sprzętu i oprogramowania.
11. Dla dostaw sprzętu informatycznego z oprogramowaniem Zamawiający wymaga fabrycznie nowego oprogramowania (nieużywanego nigdy wcześniej), w wersji z certyfikatem autentyczności dla każdej licencji, o ile producent oferowanego oprogramowania stosuje certyfikaty autentyczności. Wykonawca zobowiązany jest do dostarczenia fabrycznie nowego oprogramowania (w tym systemu operacyjnego) nieużywanego oraz nigdy wcześniej nieaktywowanego na innym urządzeniu oraz pochodzącego z legalnego źródła sprzedaży. W przypadku oprogramowania naklejka hologramowa winna być zabezpieczona przed możliwością odczytania klucza za pomocą zabezpieczeń stosowanych przez producenta, o ile producent oferowanego oprogramowania stosuje takie zabezpieczenia. Zamawiający zastrzega możliwość weryfikacji dostarczonego oprogramowania na etapie oceny ofert jak i na etapie dostawy pod kątem legalności oprogramowania bezpośrednio u producenta oprogramowania. Zamawiający zastrzega możliwość żądania od Wykonawcy na etapie dostawy przedstawienia dokumentów dotyczących zakupu oprogramowania (faktury, rachunki) w autoryzowanym kanale dystrybucyjnym producenta oprogramowania.
12. Dla dostaw oprogramowania Zamawiający wymaga fabrycznie nowego oprogramowania (nieużywanego nigdy wcześniej), w wersji z certyfikatem autentyczności dla każdej licencji, o ile producent oferowanego oprogramowania stosuje certyfikaty autentyczności. Wykonawca zobowiązany jest do dostarczenia fabrycznie nowego oprogramowania, nieużywanego oraz nigdy wcześniej nieaktywowanego oraz pochodzącego z legalnego źródła sprzedaży. W przypadku oprogramowania posiadającego fizyczny nośnik naklejka hologramowa winna być zabezpieczona przed możliwością odczytania klucza za pomocą zabezpieczeń stosowanych przez producenta, o ile producent oferowanego oprogramowania stosuje takie zabezpieczenia. Zamawiający zastrzega

możliwość weryfikacji dostarczonego oprogramowania na etapie oceny ofert jak i na etapie dostawy pod kątem legalności oprogramowania bezpośrednio u producenta oprogramowania. Zamawiający zastrzega możliwość żądania od Wykonawcy na etapie dostawy przedstawienia dokumentów dotyczących zakupu oprogramowania w autoryzowanym kanale dystrybucyjnym producenta oprogramowania.

13. Wymagania instalacyjne i wdrożeniowe dla dostarczonego sprzętu i oprogramowania:

- a. Instalacja ma odbyć się na komputerach oraz serwerach wskazanych przez Zamawiającego, a w przypadku jeżeli dostarczone oprogramowanie działa w modelu rozwiązania chmurowego to Wykonawca jest zobligowany do konfiguracji oprogramowania w chmurze Wykonawcy bądź Producenta oferowanego oprogramowania.
- b. Zamawiający dopuszcza instalację i wdrożenie zdalne przy wykorzystaniu narzędzia Wykonawcy, z zastrzeżeniem, że Wykonawca jest zobowiązany dostarczyć oprogramowanie do zdalnej pracy umożliwiające szyfrowanie połączeń oraz nagrywanie sesji serwisowych.
- c. W przypadku jeżeli dotyczy, Wykonawca wykona wdrożenie na wybranym serwerze/maszynie wirtualnej wskazanym przez Zamawiającego oraz na stanowiskach wskazanych przez Zamawiającego.
- d. Wykonawca, pomimo zapewnienia serwisu producenta zobowiązany będzie do udzielania pomocy technicznej Zamawiającemu przez okres gwarancji.
- e. Usługa wsparcia wdrożenia obejmuje:
 - i. przeprowadzenie analizy przedwdrożeniowej,
 - ii. pomoc przy instalacji silnika bazy danych – jeżeli będzie wymagana instalacja,
 - iii. rejestracja produktu – jeżeli wymagana,
 - iv. instalację oprogramowania: na stacji roboczej lub serwerze – jeżeli dotyczy,
 - v. dystrybucję oprogramowania na wybranych stacjach roboczych – jeżeli dotyczy,
 - vi. konfigurację oprogramowania,
 - vii. optymalizację ustawień pod wymogi sieciowe i sprzętowe Zamawiającego,
 - viii. szkolenie administratorów z zakresu pracy z programem,
 - ix. w uzgodnionym terminie z Zamawiającym zostanie przeprowadzane kontrolne połączenie zdalne w celu weryfikacji ustawień oraz poprawienia konfiguracji.

14. Proces współpracy między Wykonawcą a Zamawiającym w celu wdrożenia sprzętu i oprogramowania – wymagania minimalne:

- a. Wykonawca przygotowuje projekt techniczny realizacji koncepcji, uwzględniający dobre praktyki i rekomendacje eksploatacyjne publikowane przez producentów wdrażanego sprzętu i oprogramowania, po wykonaniu analizy istniejącego u Zamawiającego rozwiązania wraz z koncepcją uwzględniające obecne u Zamawiającego uwarunkowania organizacyjne i sprzętowe, łącznie zwane dalej projektem technicznym. W projekcie technicznym muszą być zawarte:
 - i. scenariusze testowe, procedury oraz wzory raportów testów,
 - ii. szczegółowy harmonogram realizacji prac wdrożeniowych i migracyjnych, uwzględniający specyfikę organizacji Zamawiającego,
 - iii. opis koncepcji realizacji prac,
 - iv. zalecenia przedwdrożeniowe dla Zamawiającego, jeżeli będą wymagane.
- b. Akceptacja projektu technicznego wraz z procedurami oraz wzorami raportów z testów będzie podlegała następującej procedurze:

- i. Wykonawca prześle do akceptacji Zamawiającego, drogą elektroniczną projekt techniczny wraz z procedurami oraz wzorami raportów z testów, w terminie nie dłuższym niż 10 dni roboczych od dnia zawarcia umowy,
 - ii. Zamawiający w terminie nie dłuższym niż 5 dni roboczych od dnia dostarczenia przez Wykonawcę kompletnych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
 - iii. wszystkie uwagi do dokumentów zgłoszone przez Zamawiającego zostaną wprowadzone przez Wykonawcę, w terminie nie dłuższym niż 5 dni roboczych od dnia ich otrzymania,
 - iv. Zamawiający w terminie 5 dni roboczych od dnia powtórnego dostarczenia przez Wykonawcę poprawionych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
 - v. w przypadku nieuwzględnienia uwag Zamawiającego, Zamawiający zastrzega sobie prawo do wskazania ostatecznego terminu dostarczenia projektu technicznego wraz z procedurami oraz wzorami raportów z testów,
 - vi. zatwierdzony projekt techniczny wraz z procedurami zostaną przekazane Zamawiającemu w 1 egzemplarzu oraz w formie elektronicznej na pendrive, w postaci plików do edycji i PDF.
- c. Wykonawca zrealizuje wdrożenia i migracje zgodnie z zakresem prac i projektem technicznym.
 - d. Wykonawca przeprowadzi testy akceptacyjne wdrożonych rozwiązań.
 - e. Wykonawca opracuje i przedstawi raport z testów. W przypadku zrealizowania scenariusza testowego z wynikiem negatywnym, Wykonawca przedstawi nowe rozwiązanie wadliwego elementu systemu i przeprowadzi ponowny test wg scenariusza, w terminie wyznaczonym przez Zamawiającego, dochowując terminu wykonania Umowy. Raport z testów powinien zawierać listę przeprowadzonych testów wraz z ich wynikiem.
 - f. Wykonawca opracuje dokumentację powykonawczą oraz procedury administracyjne i eksploatacyjne w zakresie uzgodnionym z Zamawiającym, w tym: dokumentację wdrożeniową, procedury operacyjne, procedury „Disaster Recovery”. Akceptacja dokumentacji powykonawczej będzie przebiegała zgodnie z zasadami określonymi dla akceptacji projektu technicznego.
15. Instruktaże w zakresie dostarczonego sprzętu i oprogramowania – wymagania minimalne.
- a. Instruktaże stanowiskowe będą prowadzone w języku polskim w siedzibie Zamawiającego i obejmą zakresem m.in.: użytkowane oprogramowanie; budowę, architekturę i konfigurację rozwiązania; administrowanie wdrożonym rozwiązaniem.
 - b. Instruktaże stanowiskowe zostaną przeprowadzone przez osoby prowadzące prace wdrożeniowe w ramach niniejszego zamówienia.
 - c. Instruktaże powinny trwać minimum 8 godzin lekcyjnych (45 minut) i będą przeprowadzone dla wskazanej przez Zamawiającego liczby osób (maksymalnie 2 osoby).
 - d. Zamawiający dopuszcza przeprowadzenia instruktaży w trybie zdalnym (online).
 - e. Administratorzy rozwiązania po zakończeniu Instruktaży stanowiskowych muszą w szczególności umieć wykonywać czynności administracyjne, a także instalacji oprogramowania, znać i umieć realizować procedury backupu. Ponadto powinni znać typowe zagrożenia i problemy związane z funkcjonowaniem rozwiązania, a także sposoby ich przeciwdziałania, wykrywania i usuwania. Powinni umieć instalować, konfigurować,

rekonfigurować, monitorować i prawidłowo eksploatować wdrożone rozwiązanie, jak również znać jego wdrożoną konfigurację.

16. W poniżej wskazanych wymaganiach Zamawiający posługuje się terminami „musi”, „powinien”, „możliwość” określając w ten sposób wymaganą funkcjonalność oprogramowania.

4.2. Zakup NAS (1 szt.).

Minimalne parametry techniczne NAS:

1. Obudowa do szafy RACK.
2. Procesor wielordzeniowy osiągający w teście wydajności PassMark Performance Test co najmniej wynik 4 500 punktów, testy powinny być aktualne w okresie nie dłuższym niż 30 dni przed składaniem ofert. **Zamawiający żąda załączenia do oferty przedmiotowego środka dowodowego określonego w SWZ potwierdzającego spełnienie przez oferowany procesor żądanej przez Zamawiającego wydajności.**
3. Pamięć RAM: min. 32 GB.
4. Funkcje: wsparcie dla wirtualizacji, scentralizowana pamięć masowa na dane, backup, udostępnianie i przywracanie systemu po awarii.
5. Możliwość zainstalowania łącznie 8 dysków 3,5 calowych, min. SATA 3 - 6 Gb/s.
6. Zainstalowane dyski: min. 6 x dysk 8 TB SATA 6 GB/s przeznaczonych dla systemów NAS pracujących w trybie ciągłym. dyski muszą być zgodne z urządzeniem NAS, tj. muszą znajdować się na liście zgodności prowadzonej przez producenta urządzenia NAS lub które zostały przetestowane pod kątem zgodności z produktami producenta urządzenia NAS.
7. Poziom RAID: 1,5,6.
8. Kompatybilność dysków: 3,5-calowe dyski twarde SATA; 2,5-calowe dyski twarde SATA; 2,5-calowe dyski SSD SATA.
9. Obsługa połączeń 10GbE SFP+ (co najmniej jeden port) oraz 10 GbE RJ45 (co najmniej dwa porty) wraz z wkładkami 10GbE SFP+ do NAS oraz niezbędnymi kablami do połączenia NAS z przełącznikiem za pomocą wszystkich interfejsów.
10. Porty USB: min. 2x USB 3.0.
11. Szyny do montażu w szafie RACK.
12. Dostawa oprogramowania do archiwizacji m.in. maszyn wirtualnych Hyper-V z możliwością automatycznego odtworzenia całej maszyny wirtualnej z kopii oraz z kopii już obecnie posiadanych maszyn wirtualnych.
13. Jakość produktu i sposobu jego wykonania: Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowany NAS spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci deklaracji RoHS dla produktu lub oświadczenia producenta NAS lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. **Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany NAS wymagań w zakresie określonym powyżej.**
14. Gwarancja producenta min. 24 miesiące realizowanej w miejscu instalacji sprzętu, z czasem naprawy do następnego dnia roboczego od przyjęcia zgłoszenia. Gwarancja musi obejmować także dyski. W przypadku awarii dyski twarde pozostają własnością Zamawiającego.

4.3. Zakup oprogramowania do backup (1 szt.).

Minimalne parametry funkcjonalne oprogramowania:

1. Wymagania ogólne:
 - a) licencja wieczysta na oprogramowanie ma umożliwiać backup 10 środowisk, przez backup 50 środowisk Zamawiający rozumie dowolnie dobrane przez siebie rodzaje środowisk przeznaczonych do backup, np. stacje robocze, maszyny wirtualne, serwery fizyczne itp.
 - b) oprogramowanie musi współpracować z infrastrukturą VMware oraz Microsoft Hyper-V;
 - c) oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami;
 - d) oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manager, klastrami hostów oraz pojedynczymi hostami;
 - e) oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V;
 - f) oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux;
2. Całkowite koszty posiadania:
 - a) oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej;
 - b) oprogramowanie musi tworzyć „samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków;
 - c) oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy;
 - d) oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów;
 - e) oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli;
 - f) oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu;
 - g) oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota;
 - h) oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API;
 - i) oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji;
 - j) oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej;
 - k) oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji konsol administracyjnych.
3. Wymagania RPO:

- a) oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji;
- b) oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty, które mogą zakłócić poprawne wykonanie backupu bez konieczności interakcji administratora;
- c) oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych;
- d) oprogramowanie musi posiadać wsparcie dla VMware vSAN;
- e) oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn;
- f) oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN;
- g) oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.

4. Wymagania RTO:

- a) oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.
- b) dodatkowo dla środowiska vSphere powyższa funkcjonalność powinna umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna);
- c) oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny;
- d) oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere;
- e) oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków;
- f) oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny;
- g) oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej;
- h) oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z AD, Microsoft System Objects, certyfikaty CA oraz elementy AD Sites.

5. Monitoring:

- i) system musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich;

- j) system musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn;
 - k) system musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej;
 - l) system musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora;
 - m) system musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej;
 - n) system musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego;
 - o) system musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
6. Raportowanie:
- a) system raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej;
 - b) system musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc;
 - c) system musi mieć możliwość ustawienia harmonogramu generowania raportów;
 - d) system musi mieć możliwość generowania raportów z dowolnego punktu w czasie;
 - e) system musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
7. Wykonawca zapewni gwarancję producenta oprogramowania na 24 miesiące.

5. Opis przedmiotu zamówienia części nr 3.

5.1. Wymagania ogólne.

1. Dostarczone oprogramowanie musi być wolne od wad prawnych i fizycznych oraz nienoszące oznak użytkowania.
2. Dostarczone oprogramowanie musi być fabrycznie nowe, musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez producenta dla oferowanego oprogramowania.
3. Niedopuszczalne są produkty prototypowe, oprogramowanie nie może znajdować się na liście „end-of-sale”, „end-of-support”, „end-of-life” producenta lub innych listach prowadzonych przez producentów produktów świadczących o tym, że produkt został wycofany ze sprzedaży, wsparcie dla niego zostało zakończone lub producent zaprzestaje wydawania aktualizacji, poprawek bezpieczeństwa czy też napraw dla produktu.
4. Wykonawca zapewni dostawę oprogramowania do wskazanej lokalizacji w siedzibie Zamawiającego.
5. Prace instalacyjne będzie można realizować wyłącznie w terminach uzgodnionych z Zamawiającym.

6. Wykonawca będzie zobowiązany do złożenia dokumentacji powykonawczej, zawierającej w szczególności wszystkie dane dostępu do urządzeń i oprogramowania, które będą wykorzystywane podczas instalacji i konfiguracji sprzętu i oprogramowania.
7. Dla dostaw oprogramowania Zamawiający wymaga fabrycznie nowego oprogramowania (nieużywanego nigdy wcześniej), w wersji z certyfikatem autentyczności dla każdej licencji, o ile producent oferowanego oprogramowania stosuje certyfikaty autentyczności. Wykonawca zobowiązany jest do dostarczenia fabrycznie nowego oprogramowania, nieużywanego oraz nigdy wcześniej nieaktywowanego oraz pochodzącego z legalnego źródła sprzedaży. W przypadku oprogramowania posiadającego fizyczny nośnik naklejka hologramowa winna być zabezpieczona przed możliwością odczytania klucza za pomocą zabezpieczeń stosowanych przez producenta, o ile producent oferowanego oprogramowania stosuje takie zabezpieczenia. Zamawiający zastrzega możliwość weryfikacji dostarczonego oprogramowania na etapie oceny ofert jak i na etapie dostawy pod kątem legalności oprogramowania bezpośrednio u producenta oprogramowania. Zamawiający zastrzega możliwość żądania od Wykonawcy na etapie dostawy przedstawienia dokumentów dotyczących zakupu oprogramowania w autoryzowanym kanale dystrybucyjnym producenta oprogramowania.
8. Wymagania instalacyjne i wdrożeniowe dla dostarczonego oprogramowania:
 - a. Instalacja ma odbyć się na komputerach oraz serwerach wskazanych przez Zamawiającego, a w przypadku jeżeli dostarczone oprogramowanie działa w modelu rozwiązania chmurowego to Wykonawca jest zobligowany do konfiguracji oprogramowania w chmurze Wykonawcy bądź Producenta oferowanego oprogramowania.
 - b. Zamawiający dopuszcza instalację i wdrożenie zdalne przy wykorzystaniu narzędzia Wykonawcy, z zastrzeżeniem, że Wykonawca jest zobowiązany dostarczyć oprogramowanie do zdalnej pracy umożliwiające szyfrowanie połączeń oraz nagrywanie sesji serwisowych.
 - c. W przypadku jeżeli dotyczy, Wykonawca wykona wdrożenie na wybranym serwerze/maszynie wirtualnej wskazanym przez Zamawiającego oraz na stanowiskach wskazanych przez Zamawiającego.
 - d. Wykonawca, pomimo zapewnienia serwisu producenta zobowiązany będzie do udzielania pomocy technicznej Zamawiającemu przez okres gwarancji.
 - e. Usługa wsparcia wdrożenia obejmuje:
 - i. przeprowadzenie analizy przedwdrożeniowej,
 - ii. pomoc przy instalacji silnika bazy danych – jeżeli będzie wymagana instalacja,
 - iii. rejestracja produktu – jeżeli wymagana,
 - iv. instalację oprogramowania: na stacji roboczej lub serwerze – jeżeli dotyczy,
 - v. dystrybucję oprogramowania na wybranych stacjach roboczych – jeżeli dotyczy,
 - vi. konfigurację oprogramowania,
 - vii. optymalizację ustawień pod wymogi sieciowe i sprzętowe Zamawiającego,
 - viii. szkolenie administratorów z zakresu pracy z programem,
 - ix. w uzgodnionym terminie z Zamawiającym zostanie przeprowadzane kontrolne połączenie zdalne w celu weryfikacji ustawień oraz poprawienia konfiguracji.
9. Proces współpracy między Wykonawcą a Zamawiającym w celu wdrożenia oprogramowania – wymagania minimalne:
 - a. Wykonawca przygotowuje projekt techniczny realizacji koncepcji, uwzględniający dobre praktyki i rekomendacje eksploatacyjne publikowane przez producentów wdrażanego oprogramowania, po wykonaniu analizy istniejącego u Zamawiającego rozwiązania wraz

z koncepcją uwzględniające obecne u Zamawiającego uwarunkowania organizacyjne i sprzętowe, łącznie zwane dalej projektem technicznym. W projekcie technicznym muszą być zawarte:

- i. scenariusze testowe, procedury oraz wzory raportów testów,
 - ii. szczegółowy harmonogram realizacji prac wdrożeniowych i migracyjnych, uwzględniający specyfikę organizacji Zamawiającego,
 - iii. opis koncepcji realizacji prac,
 - iv. zalecenia przedwdrożeniowe dla Zamawiającego, jeżeli będą wymagane.
 - b. Akceptacja projektu technicznego wraz z procedurami oraz wzorami raportów z testów będzie podlegała następującej procedurze:
 - i. Wykonawca przekaże do akceptacji Zamawiającego, drogą elektroniczną projekt techniczny wraz z procedurami oraz wzorami raportów z testów, w terminie nie dłuższym niż 10 dni roboczych od dnia zawarcia umowy,
 - ii. Zamawiający w terminie nie dłuższym niż 5 dni roboczych od dnia dostarczenia przez Wykonawcę kompletnych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
 - iii. wszystkie uwagi do dokumentów zgłoszone przez Zamawiającego zostaną wprowadzone przez Wykonawcę, w terminie nie dłuższym niż 5 dni roboczych od dnia ich otrzymania,
 - iv. Zamawiający w terminie 5 dni roboczych od dnia powtórnego dostarczenia przez Wykonawcę poprawionych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
 - v. w przypadku nieuwzględnienia uwag Zamawiającego, Zamawiający zastrzega sobie prawo do wskazania ostatecznego terminu dostarczenia projektu technicznego wraz z procedurami oraz wzorami raportów z testów,
 - vi. zatwierdzony projekt techniczny wraz z procedurami zostaną przekazane Zamawiającemu w 1 egzemplarzu oraz w formie elektronicznej na pendrive, w postaci plików do edycji i PDF.
 - c. Wykonawca zrealizuje wdrożenia i migracje zgodnie z zakresem prac i projektem technicznym.
 - d. Wykonawca przeprowadzi testy akceptacyjne wdrożonych rozwiązań.
 - e. Wykonawca opracuje i przedstawi raport z testów. W przypadku zrealizowania scenariusza testowego z wynikiem negatywnym, Wykonawca przedstawi nowe rozwiązanie wadliwego elementu systemu i przeprowadzi ponowny test wg scenariusza, w terminie wyznaczonym przez Zamawiającego, dochowując terminu wykonania Umowy. Raport z testów powinien zawierać listę przeprowadzonych testów wraz z ich wynikiem.
 - f. Wykonawca opracuje dokumentację powykonawczą oraz procedury administracyjne i eksploatacyjne w zakresie uzgodnionym z Zamawiającym, w tym: dokumentację wdrożeniową, procedury operacyjne, procedury „Disaster Recovery”. Akceptacja dokumentacji powykonawczej będzie przebiegała zgodnie z zasadami określonymi dla akceptacji projektu technicznego.
10. Wymagania licencyjne dla dostarczonego oprogramowania:
- a. Licencjobiorcą licencji będzie Gmina Rossosz.
 - b. Zamawiający dopuszcza udzielenie licencji w wersji papierowej i/lub elektronicznej. W przypadku jeżeli producent oprogramowania nie wystawia licencji w zakresie oferowanego

oprogramowania Wykonawca powinien dostarczyć stosowne oświadczenie producenta oprogramowania bądź jego dystrybutora.

- c. Licencje muszą obowiązywać do dnia 26.06.2026 r. niezależnie od modeli dystrybucji poszczególnych producentów oferowanego oprogramowania.
 - d. Oferowane licencje muszą pozwalać na użytkowanie oprogramowania zgodnie z przepisami prawa.
 - e. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do przeniesienia oprogramowania na inny serwer/komputer.
 - f. Licencja na oprogramowanie nie może w żaden sposób ograniczać sposobu pracy użytkowników końcowych (np. praca w sieci LAN, praca zdalna poprzez Internet). Użytkownik może pracować w dowolny dostępny technologicznie sposób.
 - g. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do wykonania kopii bezpieczeństwa oprogramowania w ilości, którą uzna za stosowną.
 - h. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do instalacji użytkowania oprogramowania na serwerach zapasowych uruchamianych w przypadku awarii serwerów podstawowych.
 - i. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do korzystania z oprogramowania na dowolnym urządzeniu klienckim (licencja nie może być przypisana do komputera/urządzenia).
 - j. Licencja oprogramowania nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji ze zgromadzonych danych.
 - k. Wykonawca zapewni gwarancję producenta oprogramowania, która obejmie gwarancję aktualizacji oprogramowania do najnowszej wersji oprogramowania w okresie objętym gwarancją.
11. Wymagania gwarancyjne i serwisowe dla dostarczonego oprogramowania w formie licencji czasowych lub subskrypcyjnych:
- a. Gwarancja producenta musi zostać zapewniona przez Wykonawcę na oferowane oprogramowanie do dnia 26.06.2026 r.
 - b. W ramach gwarancji Zamawiający ma prawo zgłaszać błędy w oprogramowaniu do serwisu producenta lub jego dystrybutora.
 - c. Serwis producenta musi zostać zapewniony przez Wykonawcę do dnia 26.06.2026 r.
 - d. Serwis polega na świadczeniu usługi wsparcia technicznego udzielonego przez producenta lub autoryzowanego dystrybutora producenta w języku polskim i objąć musi minimum:
 - i. dostęp do najnowszych wersji oprogramowania,
 - ii. wsparcie telefoniczne w zakresie oferowanego oprogramowania zespołu inżynierów technicznych,
 - iii. wsparcie w prawidłowym i zgodnym z wymaganiami producenta użytkowaniu oprogramowania,
 - iv. przyjmowanie i realizacja zgłoszeń serwisowych,
 - v. doradztwo techniczne w zakresie konfiguracji i optymalizacji oprogramowania,
- w przypadku jeżeli w dalszej części niniejszego dokumentu zdefiniowano wymogi serwisu lub gwarancji w innym zakresie powyższe wymogi są obowiązujące i należy potraktować jako podstawowe, precyzowane przez dodatkowe wymagania opisane w dalszej części dokumentu.

12. W poniżej wskazanych wymaganiach Zamawiający posługuje się terminami „musi”, „powinien”, „możliwość” określając w ten sposób wymaganą funkcjonalność oprogramowania.

5.2. Rozbudowa oprogramowania antywirusowego o funkcje XDR, szyfrowanie danych, analizę podatności (1 szt.).

Aktualnie Zamawiający posiada licencje oprogramowania antywirusowego ESET Endpoint Antywirus. Przedmiotem zamówienia jest rozbudowa istniejącego oprogramowania antywirusowego poprzez podniesienie wersji istniejącego oprogramowania dla Urzędu Gminy Rossosz do wersji ESET PROTECT Elite ważnej w okresie do dnia 26.06.2026 r. dla 25 użytkowników/urządzeń oraz umożliwienie zarządzania wszystkimi użytkownikami/urządzeniami końcowymi z jednej konsoli chmurowej wraz z wdrożeniem oprogramowania zgodnie z wytycznymi wynikającymi z rozdziału nr 4.1. Wymagania ogólne niniejszego dokumentu w zakresie modułów XDR, zarządzania podatnościami i szyfrowania dysków

lub dostawa równoważnej platformy bezpieczeństwa zgodnie z określonymi poniżej kryteriami równoważności.

Minimalne wymagania (kryteria równoważności) określone dla równoważnej platformy bezpieczeństwa:

Administracja zdalna w chmurze.

1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.
2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.
4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

Ochrona stacji roboczych.

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
2. Rozwiązanie musi wspierać architekturę ARM64.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
10. Rozwiązanie musi integrować się z Intel Threat Detection Technology.
11. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
13. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
14. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
15. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
 - a. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
 - b. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
 - c. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,

- d. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
 - e. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
17. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
 18. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
 19. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
 20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
 21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
 22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
 23. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:
 - a. tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
 - b. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
 - c. tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
 - d. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
 24. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
 25. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
 26. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
 27. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
 28. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
 29. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
 30. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

Ochrona serwera.

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, Ubuntu Server (SLES) 15, Oracle Linux 8 oraz Amazon Linux.

2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
Dodatkowe wymagania dla ochrony serwerów Windows:
9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
13. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
14. Rozwiązanie musi automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.
Dodatkowe wymagania dla ochrony serwerów Linux:
18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
20. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonych mikro-serwisu.

Szyfrowanie.

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10/11 32-bit i 64-bit.

2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
3. Aplikacja musi posiadać autentykację typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
4. Aplikacja musi umożliwiać szyfrowanie danych na komputerach z UEFI.

Ochrona urządzeń mobilnych opartych o system Android.

1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.
5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
 - a. usunięcie zawartości urządzenia,
 - b. przywrócenie urządzenia do ustawień fabrycznych,
 - c. zablokowania urządzenia,
 - d. uruchomienie sygnału dźwiękowego,
 - e. lokalizację GPS.
 - f. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
 - g. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
 - h. nazwę aplikacji,
 - i. nazwę pakietu,
 - j. kategorię sklepu Google Play,
 - k. uprawnienia aplikacji,
 - l. pochodzenie aplikacji z nieznanego źródła.

Ochrona serwera pocztowego MS Exchange.

1. Rozwiązanie musi wspierać instalację na systemach Microsoft Windows Server 2012 i nowszych.
2. Rozwiązanie musi zapewniać wsparcie dla systemów poczty Microsoft Exchange 2010/2013/2016/2019.
3. Rozwiązanie musi zapewniać wsparcie dla ról Mailbox, Edge, Hub.
4. Rozwiązanie musi skanować pocztę przychodzącą i wychodzącą na serwerze MS Exchange.
5. Rozwiązanie musi zapewnić skanowanie bezpośrednio w bazach danych Exchange przy pomocy VSAPI.
6. Rozwiązanie musi mieć możliwość tworzenia różnych reguł blokowania wiadomości w tym co najmniej po zdefiniowanym nadawcy, odbiorcy, temacie wiadomości, typie załącznika, rozmiarze załącznika, rozmiarze wiadomości, nagłówku wiadomości, na podstawie uzyskanego wyniku skanowania antyspamowego i antywirusowego, godzinie odbioru, obecności załącznika chronionego hasłem lub uszkodzonego archiwum.
7. Rozwiązanie musi posiadać wbudowany w oprogramowanie filtr antyspamowy odpowiedzialny za filtrowanie niechcianej poczty.

8. System antyspamowy ma być wyposażony przynajmniej w możliwość sprawdzania list RBL, DNSBL oraz mechanizm reputacji poczty.
9. Administrator musi mieć możliwość dodania własnych adresów list RBL oraz DSBL, z których będzie korzystać aplikacja.
10. Rozwiązanie ma posiadać mechanizm greylisting (szara lista).
11. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.

Sandbox w chmurze.

1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.
3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
7. Po zakończonej analizie pliku, rozwiązanie musi przysyłać wynik analizy do wszystkich wspieranych produktów.
8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizację stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzewać jakie pliki zostały wysłane do analizy oraz przez kogo.
12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:
 - a. Czysty,
 - b. Podejrzany,
 - c. Bardzo podejrzany,
 - d. Szkodliwy.
13. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

Ochrona usługi Microsoft 365.

1. Rozwiązanie musi obejmować ochroną usługi Microsoft, takie jak Exchange Online, Onedrive, Sharepoint oraz aplikację Teams.
2. Rozwiązanie musi posiadać możliwość dodania kilku tenantów usługi Microsoft 365.

3. Administrator musi mieć możliwość wskazania, które konto użytkownika będzie objęte ochroną.
4. Rozwiązanie musi być zarządzane za pomocą dowolnej przeglądarki internetowej z dowolnego miejsca w sieci.
5. Rozwiązanie musi być dostępne w języku polskim.
6. Konsola rozwiązania musi posiadać możliwość raportowania co najmniej:
 - a. użytkowników, otrzymujących najwięcej spamu,
 - b. użytkowników, otrzymujących najwięcej wiadomości typu „phishing”,
 - c. użytkowników, otrzymujących największą ilość szkodliwego oprogramowania,
 - d. kont użytkowników, które mogą być podejrzane.
7. Konsola rozwiązania musi posiadać funkcjonalność logowania zdarzeń z podziałem na dzienniki dla Exchange Online i Onedrive.
8. Dzienniki Exchange Online muszą posiadać funkcjonalność informowania co najmniej:
 - a. jaka ilość wiadomości została przeskanowana,
 - b. wynik skanowania poszczególnych wiadomości,
 - c. czynność podjęta przez rozwiązanie.
9. Dzienniki Onedrive muszą posiadać funkcjonalność informowania co najmniej o: zagrożeniach, które zostały wykryte,
 - a. na jakim koncie zostały wykryte,
 - b. jakie zagrożenie zostało wykryte,
 - c. podjętą czynność.
10. Rozwiązanie musi posiadać funkcjonalność kwarantanny, do której będą przenoszone zainfekowane obiekty z usługi Exchange Online oraz Onedrive.
11. Musi istnieć możliwość pobrania plików z kwarantanny w formie oryginalnego pliku i pliku zabezpieczonego hasłem.
12. Administrator musi posiadać możliwość przypisania konfiguracji, do dodanych do rozwiązania tenantów lub do poszczególnych grup i użytkowników.
13. Administrator musi posiadać możliwość konfiguracji rozwiązania w oparciu o co najmniej:
 - a. wykorzystania do analizy mechanizmów chmurowych, tego samego producenta,
 - b. wprowadzenia białych i czarnych list adresów ochrony Exchange’a Online,
 - c. dodania znacznika do tematu wiadomości zakwalifikowanej jako SPAM i phishing.
14. Rozwiązanie musi zapewniać funkcję ochrony przed zagrożeniami 0-day.
15. Funkcja ochrony przed zagrożeniami 0-day musi wykorzystywać do działania chmurę producenta.
16. Funkcja ochrony przed zagrożeniami 0-day musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
17. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
18. Rozwiązanie musi posiadać możliwość przesyłania powiadomień e-mail z funkcją wyboru preferowanego języka.

Moduł zarządzania podatnościami i aktualizacjami.

1. Rozwiązanie musi mieć możliwości wykrywania podatności w systemach operacyjnych (co najmniej Windows 10, Windows 11) oraz aplikacjach zainstalowanych na zarządzanych stacjach.
2. Baza wykrywanych podatności musi zawierać minimum 35000 CVE.

3. Rozwiązanie nie może wymagać instalacji dodatkowej konsoli ani innych dodatkowych komponentów na stacjach końcowych.
4. Automatyczne wykrywanie podatności musi wykonywać się zgodnie z harmonogramem, nie częściej niż raz dziennie.
5. Moduł wykrywania podatności musi umożliwiać wyświetlanie szczegółów danej podatności zawierające minimum:
 - a. nazwę aplikacji lub systemu operacyjnego;
 - b. punktację CVSS;
 - c. opis wykrytej podatności;
 - d. wartość ryzyka oceniona przez wewnętrzne mechanizmy producenta.
6. Moduł wykrywania podatności musi wykrywać podatności w minimum 700 aplikacjach.
7. Moduł zarządzania aktualizacjami musi umożliwiać wykonanie automatycznej aktualizacji dla minimum 150 popularnych aplikacji.
8. Moduł zarządzania aktualizacjami musi umożliwiać stworzenie białej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje będą aplikowane tylko dla wskazanych aplikacji w białej liście. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.
9. Moduł zarządzania aktualizacjami musi umożliwiać stworzenie czarnej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje oprogramowania będą realizowane dla wszystkich - ponad 150 aplikacji, oprócz aplikacji wskazanych na czarnej liście. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.
10. Zarządzanie aktualizacjami aplikacji musi umożliwiać ręczne wdrażanie poprawek na wybranych stacjach.
11. Moduł zarządzania aktualizacjami oraz wykrywania podatności musi być zintegrowany bezpośrednio z programem antywirusowym tego samego producenta zainstalowanym na zarządzanym komputerze.
12. Stacja robocza posiadająca włączony moduł wykrywania podatności oraz zarządzania aktualizacjami musi być w odpowiedni sposób oznaczona w konsoli centralnego zarządzania.
13. Administrator konsoli musi mieć możliwość włączenia modułu wykrywania podatności i zarządzania aktualizacjami przy pomocy menu kontekstowego dostępnego w konsoli centralnego zarządzania.
14. Moduł wykrywania podatności ma umożliwiać wyłączenie powiadomień dla wybranej podatności.

Moduł XDR.

1. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
2. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
3. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
4. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
5. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”.
6. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.
7. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.

8. Serwer musi posiadać minimum 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.
9. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.
10. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.
11. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.
12. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
13. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
14. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.
15. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.
16. Konsola administracyjna musi mieć możliwość tagowania obiektów.
17. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.

Ochrona poprzez dwuskładnikowe uwierzytelnianie.

1. Rozwiązanie musi wspierać systemy operacyjne Microsoft Windows Server: Windows Server 2016 / Windows Server 2016 Essentials / Windows Server 2019 / Windows Server 2019 Essentials / Windows Server 2022.
2. Rozwiązanie musi wspierać system operacyjne Windows 10 / Windows 11.
3. Rozwiązanie musi wspierać architekturę 32 i 64-bitową systemu Windows.
4. Oprogramowanie musi wspierać integrację z Microsoft Exchange 2007 / 2010 / 2013 / 2016 / 2019.
5. Oprogramowanie musi wspierać integrację z Microsoft Dynamics CRM 2011 / 2013 / 2015 / 2016.
6. Oprogramowanie musi wspierać integrację z Microsoft Sharepoint 2010 / 2013 / 2016 / 2019.
7. Oprogramowanie musi wspierać integrację z Microsoft Remote Desktop Web Access.
8. Oprogramowanie musi wspierać integrację z Microsoft Terminal Services Web Access.
9. Oprogramowanie musi wspierać integrację z Microsoft Remote Web Access.

10. Rozwiązanie musi posiadać wbudowany serwer RADIUS umożliwiający uwierzytelnianie użytkowników dla rozwiązań VPN, które wspierają protokół RADIUS.
11. Aplikacja mobilna musi wspierać telefony działające pod kontrolą systemów mobilnych: Android (w wersji 4.4 lub wyższej), iOS (12 lub wyższej).
12. Aplikacja mobilna do generowania OTP (jednorazowego hasła) musi być dostarczona przez producenta rozwiązania w ramach zakupionej licencji.
13. Użytkownik musi mieć możliwość dodatkowego zabezpieczenia aplikacji w postaci kodu PIN.
14. Aplikacja do działania nie może wymagać od użytkownika aktywnego połączenia z Internetem – generowanie OTP (jednorazowego hasła) musi odbywać się w trybie offline.
15. Dwuskładnikowe uwierzytelnienie musi być możliwe również przy użyciu jednorazowych haseł SMS.
16. Aplikacja zainstalowana na urządzeniach mobilnych musi umożliwiać generowanie OTP dla więcej niż jednego serwera uwierzytelniającego.

Rozwiązania zastępujące dotychczas funkcjonujące u Zamawiającego Wykonawca dostarcza i wdraża na swój koszt. Wykonawca przeprowadzi instruktaże stanowiskowe i będzie świadczył asystę techniczną w zakresie umożliwiającym pracownikom jednostki Zamawiającego płynną obsługę wymienianego oprogramowania. Wdrożenie rozwiązania równoważnego nie może zakłócić bieżącej pracy Zamawiającego oraz musi zapewnić ciągłość pracy i musi odbywać się zgodnie z wytycznymi wynikającymi z rozdziału nr 4.1. Wymagania ogólne niniejszego dokumentu.

5.3. Zakup oprogramowania do zarządzania bezpieczeństwem IT (DLP, monitoring zasobów, zarządzanie dostępem).

Minimalne wymagania funkcjonalne dla oprogramowania specjalistycznego do zarządzania zasobami IT:

1. Oprogramowanie musi składać się serwera zarządzającego, zdalnych konsoli oraz Agentów.
2. Komunikacja pomiędzy Serwerem a Agentami i Konsolami nawiązywana powinna być przy użyciu szyfrowanego protokołu TLS 1.2.
3. Oprogramowanie musi umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych.
4. Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, musi być objęty kontrolą na poziomie wybranych Administratorów - nadawanie kontom administracyjnym różnych poziomów dostępu oraz uprawnień zarówno do grup urządzeń, jak i użytkowników.
5. Oprogramowanie musi posiadać funkcjonalność monitorowania infrastruktury serwerowej i sieciowej w zakresie:
 - a. wykrywania urządzeń w sieci poprzez skanowanie ping (oraz arp-ping),
 - b. wizualizacji stanu urządzeń w postaci ikon urządzeń na mapach sieci,
 - c. wizualizacji połączeń pomiędzy urządzeniami a przełącznikami i informacji, do którego portu przełącznika podłączone jest dane urządzenie.
 - d. serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów,
 - e. serwerów pocztowych: - monitorowanie serwisu odbierającego, jak i wysyłającego pocztę, - możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), - możliwość wykonywania operacji testowych, - możliwość wysłania powiadomienia, jeśli serwer pocztowy nie działa,

- f. monitorowania serwerów WWW i adresów URL,
 - g. obsługi szyfrowania SSL/TLS w powiadomieniach e-mail.
 - h. obsługi komunikatów syslog i pułapek SNMP.
 - i. monitoringu routerów i przełączników wg: - zmian stanu interfejsów sieciowych, - ruchu sieciowego, - podłączonych stacji roboczych- ruchu generowanego przez podłączone stacje robocze,
 - j. kontroli nad monitorem usług Windows,
 - k. monitorowania wydajności systemów Windows: - obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy.
6. Oprogramowanie musi umożliwiać automatyczne gromadzenie danych o sprzęcie i oprogramowaniu na stacjach roboczych w zakresie:
- a. informacji dotyczących sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.;
 - b. zestawienia posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade;
 - c. informacji o zainstalowanych aplikacjach oraz aktualizacjach Windows, umożliwiających audytowanie i weryfikację użytkownika licencji w organizacji;
 - d. informacji o wszystkich zmianach przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.;
 - e. możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiegokolwiek zmiany konfiguracji sprzętowej komputera;
 - f. możliwość odczytania numeru seryjnego (klucze licencyjne);
 - g. możliwość automatycznego zarządzania instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych;
 - h. możliwość przeglądu informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.
7. Oprogramowanie musi mieć możliwość prowadzenia bazy ewidencji majątku IT w zakresie:
- a. przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji;
 - b. definiowania własnych typów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer i skan faktury zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu i skan gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, inny dowolny załącznik (np. plik .DOCX, .XLSX, .PDF), skan dowolnego dokumentu, czy też własny komentarz, możliwość importu danych z zewnętrznego źródła np. (.CSV);
 - c. generowania zestawienia wszystkich środków trwałych, w tym urządzeń i zainstalowanego na nich oprogramowania;
 - d. archiwizacji i porównywania audytów środków trwałych;
 - e. tworzenia kodów kreskowych w Środkach Trwałych;
 - f. drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla środków trwałych, które posiadają numer inwentarzowy;

- g. inwentaryzacji sprzętu posiadającego kody kreskowe za pomocą aplikacji mobilnej co najmniej na system Android;
 - h. inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji dodatkowego oprogramowania poprzez manualne wykonanie skanów inwentaryzacji offline).
8. Oprogramowanie musi zapewniać funkcjonalność w zakresie monitorowania aktywności użytkowników na stacjach roboczych w zakresie:
- a. faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy);
 - b. monitorowania procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika);
 - c. użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona);
 - d. informacji o edytowanych przez użytkownika dokumentach;
 - e. historii pracy (cykliczne zrzuty ekranowe);
 - f. listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt),
 - g. transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika),
 - h. wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek.
9. Oprogramowanie musi zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:
- a. skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie, archiwów ZIP;
 - b. zarządzanie posiadanymi licencjami;
 - c. audyt legalności oprogramowania oraz powiadamianie w razie przekroczenia liczby posiadanych licencji;
 - d. zarządzanie posiadanymi licencjami: raport zgodności licencji;
 - e. możliwość przypisania do programów numerów seryjnych, wartości itp.
10. Oprogramowanie musi zapewniać integrację z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych.
11. W zakresie pomocy technicznej system musi umożliwiać:
- a. tworzenie zgłoszeń serwisowych i zarządzanie nimi (przypisywanie do administratorów);
 - b. załączanie komentarzy, zrzutów ekranów i załączników w zgłoszeniach;
 - c. konfigurowanie pól niestandardowych, powiązanych w wybraną kategorię zgłoszenia;
 - d. przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o Sygnalistach”);
 - e. dokumenty prawne dot. ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę;
 - f. planowanie zastępstw w przydzielaniu zgłoszeń;
 - g. funkcję rozbudowanych raportów;
 - h. powiadomienia i widok zgłoszenia odświeżany w czasie rzeczywistym;
 - i. baza zgłoszeń z rozbudowaną wyszukiwarką;
 - j. przejrzysty i intuicyjny interfejs webowy;

- k. wewnętrzny komunikator (czat) z możliwością przydzielania uprawnień oraz przesyłania plików i tworzenia rozmów grupowych;
 - l. komunikaty wysyłane do użytkowników/komputerów z możliwym/obowiązkowym potwierdzeniem odczytu;
 - m. zdalny dostęp do komputerów z możliwością blokady myszy/klawiatury;
 - n. dwukierunkowa wymiana plików;
 - o. zarządzanie procesami Windows z poziomu okna informacji o urządzeniu;
 - p. zadania dystrybucji oraz uruchamiania plików (zdalna instalacja oprogramowania);
 - q. procesowanie zgłoszeń z wiadomości e-mail;
 - r. integracja bazy użytkowników z Active Directory;
 - s. zarządzanie kontami lokalnych użytkowników Windows (tworzenie, usuwanie, edycja, reset hasła, eskalacja/deeskalacja uprawnień oraz włączanie/wyłączanie kont).
12. W zakresie kontroli dostępu do danych system musi umożliwiać:
- a. automatyczne nadawanie użytkownikowi domyślnej polityki monitorowania i bezpieczeństwa;
 - b. ograniczenie ryzyka wycieku strategicznych danych za pośrednictwem przenośnych pamięci masowych oraz urządzeń mobilnych;
 - c. zabezpieczenie sieci firmowej przed wirusami instalującymi się automatycznie z pendrive'ów lub dysków zewnętrznych;
 - d. integracja z Windows Defender: zarządzanie ustawieniami wbudowanego antywirusa wraz z możliwością alarmowania o wykrytych problemach oraz wynikach skanowania;
 - e. integracja z Windows Firewall: włączanie i wyłączanie zapory dla wybranych typów połączeń, tworzenie reguł ruchu, odczyt stanu zapory na stacjach roboczych;
 - f. możliwość usuwania nieistniejących/zutylizowanych nośników danych (np. USB);
 - g. alarmy o podłączonym urządzeniu obcym (nieposiadającym atrybutu „nośnik zaufany”);
 - h. integracja z Windows BitLocker: odczyt stanu modułu TPM oraz zaszyfrowania woluminów
 - i. zdefiniowanie polityki przenoszenia danych firmowych przez pracowników wraz z odpowiednimi uprawnieniami;
 - j. informacje o urządzeniach podłączonych do danego komputera;
 - k. lista wszystkich urządzeń podłączonych do komputerów w sieci;
 - l. audyt (historia) połączeń i operacji na urządzeniach przenośnych oraz na udziałach sieciowych;
 - m. zarządzanie prawami dostępu (zapis, uruchomienie, odczyt) dla urządzeń, komputerów i użytkowników;
 - n. centralna konfiguracja: ustawienie reguł dla całej sieci, dla wybranych map sieci oraz dla grup i użytkowników Active Directory.

Wymagania instalacyjne i wdrożeniowe dla dostarczonego oprogramowania:

- a. Licencja musi mieć charakter licencji wieczystej.
- b. Wykonawca musi zapewnić serwis producenta oprogramowania nie dłużej niż do 26.06.2026 r.
- c. Instalacja ma odbyć się na komputerach oraz serwerach posiadanych przez Zamawiającego w Urzędzie Gminy Rossosz – maksymalnie 25 indywidualnych użytkowników.
- d. Zamawiający dopuszcza instalację i wdrożenie zdalne.
- e. Wykonawca wykona wdrożenie na wybranym serwerze/maszynie wirtualnej wskazanym przez Zamawiającego oraz na stanowiskach wskazanych przez Zamawiającego.

- f. Wykonawca będzie udzielał pomocy technicznej Zamawiającemu przez okres serwisu nie dłużej niż do 26.06.2026 r.