

Załącznik nr 5c do SWZ

Opis przedmiotu zamówienia - Część III

Zamawiający zastrzega sobie prawo sprawdzenia zgodności oferowanego oprogramowania w oparciu o informacje zamieszczone na stronie internetowej producenta, w przypadku braku takiej możliwości, Zamawiający będzie wymagał przedstawienia dokumentacji producenta potwierdzającej wymagania minimalne.

Przedmiotem zamówienia jest zakup i dostawa **oprogramowania do monitoringu sieci, użytkowników i kontroli dostępu** ze wsparciem serwisowym i aktualizacjami do 17.04.2026 r., na potrzeby Starostwa Powiatowego w Radomsku.

Parametr	Wymagania minimalne
Licencja	Bezterminowa
Liczba monitorowanych urzędzeń/użytkowników	170
Serwis/wsparcie techniczne	Oferowane oprogramowanie musi posiadać aktywne wsparcie producenta do 17.04.2026 r., umożliwiające bezpłatne aktualizacje w tym do najnowszych wersji oraz wsparcie w zakresie zgłaszania ewentualnych problemów drogą mailową lub przez portal online, a w dni robocze również telefonicznie, w godzinach 9:00 – 15:00. W ramach wsparcia technicznego producent lub oficjalny dystrybutor zapewni bezpłatną dostępność w języku polskim inżyniera w zakresie rozwiązywania problemów dotyczących przedmiotu zamówienia.
Serwer administracyjny	System musi umożliwiać instalację na jednej z platform systemowych: Microsoft Windows Server (minimum Server 2022) lub Redhat/Oracle Linux (minimum 7.x).
Stacje robocze/serwery	Pełne wsparcie dla posiadanych przez Zamawiającego stacji roboczych z systemami Windows 10/11, serwerów z Windows Server 2016-2022, Linux.

Baza danych	Jeżeli oprogramowanie wymaga do swego działania bazy danych, musi ona być w kalkulowana w cenę lub posiadać bezpłatną licencję.
Interfejs użytkownika	W związku z tym, że obsługa systemu ma objąć także użytkowników nieposługujących się biegle językiem angielskim, interfejs użytkownika musi umożliwiać obsługę w języku polskim.
Monitorowanie urządzeń	<p>Bezagentowe wykrywanie urządzeń w sieci poprzez skanowanie oraz na podstawie informacji odczytanych z Active Directory wraz z informacją o OU.</p> <p>Serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów - czas ich odpowiedzi i procent utraconych pakietów.</p> <p>Serwerów WWW i adresów URL.</p> <p>Routerów i przełączników sieciowych wg:</p> <ul style="list-style-type: none"> a) zmian stanu interfejsów sieciowych, b) ruchu sieciowego, c) podłączonych stacji roboczych – graficzna prezentacja panelu przełącznika, d) ruchu generowanego przez podłączone do portów stacje robocze. <p>Serwisów Windows - alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie / zatrzymanie / zrestartowanie.</p> <p>Stan maszyn wirtualnych Vmware - działa, nie działa, wstrzymano. Zarządzania stanem maszyn wirtualnych Vmware - wysyłanie poleceń włączenia, wstrzymania i wyłączenia zasilania do każdej z maszyn.</p> <p>Wydajności systemów Windows - obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy</p>

	<p>Serwerów pocztowych - monitorowanie stanu systemów oraz wysyłanie powiadomienia (e-mail, SMS) w przypadku braku odpowiedzi lub błędnego funkcjonowania.</p> <p>Czas ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS.</p> <p>Wyświetlanie statystyk przy każdym urządzeniu na mapie sieci takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, ostrzeżenie o zdarzeniu na urządzeniu.</p> <p>Wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci oraz połączeń pomiędzy urządzeniami i przełącznikami.</p> <p>Obsługa pułapek SNMP.</p>
<p>Monitorowanie użytkowników</p>	<p>Monitorowanie procesów wraz informacją o uruchomieniu na podwyższonych uprawnieniach.</p> <p>Użytkowania programów wraz z informacją, na którym komputerze wykonano daną aktywność.</p> <p>Informacji o edytowanych przez użytkownika dokumentach.</p> <p>Listy odwiedzanych stron WWW (tytuły, adresy, liczba i czas wizyt).</p> <p>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).</p> <p>Blokowanie stron internetowych - możliwość definiowania wyjątków zezwalających i zabraniających korzystania z danych domen/subdomen, reguły w postaci listy domen dla użytkownika lub grupy. Integracja list stron w formie plików .txt z dowolnego adresu zewnętrznego np. CERT. Wbudowana lista stron sklasyfikowanych jako zagrożenia. Automatyczne</p>

	odświeżania list stron zintegrowanych z adresów zewnętrznych.
	Blokowanie ruchu na wskazanych portach TCP/IP.
	Blokowanie pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem.
	Rejestru naruszeń blokad.
	Wysyłania powiadomień gdy użytkownik odwiedzi stronę z określonej grupy domen, naruszy skonfigurowane blokady.
	Ochrona przed wiadomościami phishingowymi i atakami APT.
Kontrola dostępu do danych	Blokowanie urządzeń i nośników danych. Możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny.
	Blokowanie urządzeń i interfejsów fizycznych: USB, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD.
	Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth.
	Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezauważanych.
	Monitorowanie stanu szyfrowania dysków oraz zdalne szyfrowanie dysków za pomocą BitLockera
	Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.
	Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci.
	Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych oraz podłączenie/odłączenie urządzenia przenośnego.
	Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika. Monitorowanie operacji na plikach

	na udostępnionych zasobach sieciowych (udziałach) na urządzeniach nieobsługiwanych przez Agenta (np. macierze, NAS itp.).
	Integracja z Windows Firewall - włączanie i wyłączanie zapory dla wybranych typów połączeń, tworzenie reguł ruchu, odczyt stanu zapory na stacjach roboczych.
Wymagania sprzętowe	<p>Oprogramowanie musi poprawnie funkcjonować i nie może mieć wymagań większych niż posiadany przez Zamawiającego sprzęt o parametrach:</p> <ul style="list-style-type: none"> - dwa procesory 8-rdzeniowe, klasy serwerowej x86, - pamięć 64 GB, - macierz dyskowa 4 TB, - system operacyjny Windows Server Standard 2022 x64.
Gwarancja	<ol style="list-style-type: none"> 1. Wykonawca zapewni prawidłowe i sprawne działanie oferowanego oprogramowania - systemu jako całości, jak również każdego z elementów tego systemu oddzielnie i udzieli gwarancji do 17.04.2026 roku na system i wszystkie jego elementy. 2. Wykonawca zapewni również wsparcie serwisowe dla dostarczonego rozwiązania, które będzie świadczone przez Producenta oprogramowania w ramach wynagrodzenia przysługującego Wykonawcy na podstawie umowy. 3. Zgłoszenia dotyczące wystąpienia wad, awarii mogą być przyjmowane drogą mailową lub przez portal online, a w dni robocze również telefonicznie, w godzinach 9:00 – 15:00. W ramach wsparcia technicznego Producent lub oficjalny dystrybutor zapewni bezpłatną dostępność w języku polskim inżyniera w zakresie rozwiązywania problemów dotyczących przedmiotu zamówienia. 4. Bieg terminu gwarancji rozpoczyna się od daty odbioru przedmiotu umowy.

5. W okresie gwarancji Wykonawca zobowiązuje się do bezpłatnego usunięcia stwierdzonych wad.
6. Gwarancja obejmuje wszelkie wady z wyjątkiem wad spowodowanych niewłaściwym lub niezgodnym z instrukcją obsługi użytkowaniem produktu oraz wad spowodowanych zdarzeniami losowymi.
7. Jeżeli usunięcie ujawnionej wady wdrożonego systemu jest możliwe wyłącznie w drodze dokonania zakupu jakichkolwiek udoskonaleń (w tym: unowocześnień, aktualizacji, dodatków sprzętowych, wszelkiego rodzaju usług, serwisów, licencji i uprawnień), Wykonawca jest zobowiązany dokonać tego zakupu na własny koszt i zainstalować przedmiot zakupu we wdrożonym systemie.
8. Wykonawca pokrywa w ramach gwarancji wszelkie koszty napraw i wymiany elementów systemu, w tym koszty dojazdu, transportu, demontażu, montażu, odinstalowania lub zainstalowania.
9. Udzielona przez Wykonawcę gwarancja nie wyłącza uprawnień Zamawiającego wynikających z rękojmi za wady oraz uprawnień Zamawiającego z tytułu gwarancji udzielonych przez producenta oprogramowania.
10. Wykonawca do oprogramowania dostarczonego Zamawiającemu na podstawie umowy dołącza Licencje oraz wszelkie inne dokumenty konieczne do prawidłowego korzystania z Systemu.
11. Dla oprogramowania wymaga się dostarczenia wsparcia technicznego producenta tego oprogramowania do 17.04.2026 roku z możliwością jego odnawiania po tym czasie.