Załącznik nr 1 do ZO

Szczegółowy opis przedmiotu zamówienia

Część pierwsza. Dostawa oprogramowania antywirusowego

1. **Warunki wstępne:**
   1) Kompleksowa ochrona antywirusowa 150 urządzeń na okres trzech lat z uwzględnieniem terminu wygaśnięcia posiadanych licencji.
   2) Zamawiający posiada m. in. licencje programu antywirusowego:
      - ESET Endpoint Antivirus for Windows o identyfikatorze: 33C-E59-5PH – ważną do 30.06.2021,
   3) Zamawiający ma prawo do korzystania z licencji typu Biznes
   4) Zamawiający użytkuje konsolę zdalnego zarządzania ESET Protect
   5) Zamawiający wymaga by Wykonawca zapewnił kompleksową, ciągłą ochronę antywirusową dla min. 150 użytkowników (150 stacji roboczych), **przez okres trzech lat, określony w umowie.** Zamawiający wymaga by Wykonawca zapewnił w każdym momencie trwania ochrony antywirusowej zarządzanie ochroną antywirusową każdej z chronionych stacji roboczych jedną konsolą zarządzania zdalnego.
   6) Jeśli do zarządzania wymagany jest plik licencyjny – Zamawiający wymaga jego dostarczenia.

Za równoważne Zamawiający dopuszcza oprogramowanie posiadające następujące funkcje:

2. **Minimalne funkcje oprogramowania:**
   1) Pełne wsparcie dla systemu Windows XP/Winndows7/ Windows 8/Windows 8.1/Windows 10.
   2) Wsparcie dla 32- i 64-bitowej wersji systemu Windows.
   3) Wersja programu dla stacji roboczych Windows dostępna w języku polskim.
   4) Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim.
   5) Pliki instalacyjne programu muszą być dystrybuowane w formie pakietu/pakietów *.msi umożliwiającym zdalną dystrybucje oprogramowania na stacje robocze.

3. **Ochrona antywirusowa i antyspyware:**
   1) Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. Wbudowana technologia do ochrony przed rootkitami. Ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
   2) Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
   3) Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
   4) Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
   5) Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
   6) Możliwość skanowania dysków sieciowych i dysków przenośnych.
   7) Skanowanie plików spakowanych i skompresowanych. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.

8) Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
9) Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
10) Wbudowany konektor dla programów MS Outlook. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express. 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). Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
11) Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie. Blokowanie możliwości przeglądania wybranych stron internetowych. Program musi umożliwić blokowanie danej strony internetowej po podaniu przynajmniej całego adresu URL strony lub części adresu URL.
12) Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron, ustalonej przez administratora.
13) Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
14) Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. Program ma zapewniać skanowanie ruchu szyfrowanego transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji, takich jak: przeglądarki internetowe oraz programy pocztowe.
15) Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika, w celu analizy przez laboratorium producenta.
16) Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
17) Program musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
18) Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania oraz przez moduły ochrony w czasie rzeczywistym.
19) Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
20) W przypadku, gdy stacja robocza nie będzie posiadała dostępu do sieci Internet, ma odbywać się skanowanie wszystkich procesów, również tych, które wcześniej zostały uznane za bezpieczne.
21) 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 heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

22) Możliwość automatycznego wysyłania nowych zagrożeń do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie.
23) Do wysłania próbki zagrożenia do laboratorium producenta, aplikacja nie może wykorzystywać klienta pocztowego zainstalowanego na komputerze użytkownika.
24) Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
25) Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
26) Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie.
27) Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło.
28) Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.
29) Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku aktualizacji – poinformować o tym użytkownika i wyświetlenia listy niezainstalowanych aktualizacji.
30) Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.
31) Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu zagrożeń.
32) System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku.
33) System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym.
34) Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
35) Funkcja blokowania nośników wymiennych, bądź grup urządzeń, ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń, minimum w oparciu o typ, numer seryjny, dostawcę oraz model urządzenia.
36) Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.
37) Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia.
38) Program ma posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
39) W momencie podłączenia zewnętrznego nośnika, aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
40) Administrator ma posiadać możliwość takiej konfiguracji programu, aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika.

41) Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
42) 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 program 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 program 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 program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach.
43) Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
44) Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
45) Oprogramowanie musi posiadać zaawansowany skaner pamięci.
46) Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.
47) Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany, 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.
48) Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić zagrożenie bezpieczeństwa.
49) Program ma posiadać funkcję, która aktywnie monitoruje wszystkie pliki programu, jego procesy, usługi i wpisy w rejestrze i skutecznie blokuje ich modyfikacje przez aplikacje trzecie.
50) Automatyczna, inkrementacyjna aktualizacja silnika detekcji.
51) Możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera.
52) Możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego program zgłosi posiadanie nieaktualnego silnika detekcji.
53) Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów.
54) Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP.
55) Program musi być wyposażony w funkcjonalność, umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback).
56) Program wyposażony tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa).
57) Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym.
58) W momencie wykrycia trybu pełnoekranowego, aplikacja ma wstrzymać wyświetlanie wszystkich powiadomień związanych ze swoją pracą oraz wstrzymać zadania znajdujące się w harmonogramie zadań aplikacji.
59) Użytkownik ma mieć możliwość skonfigurowania po jakim czasie włączone mają zostać powiadomienia oraz zadania, pomimo pracy w trybie pełnoekranowym.

60) Program ma być wyposażony w dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli stron internetowych i kontroli dostępu do urządzeń, skanowania oraz zdarzeń.
61) Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego przez producenta programu.
62) Program musi posiadać możliwość utworzenia dziennika diagnostycznego z poziomu interfejsu aplikacji.
63) Program musi posiadać możliwość aktywacji przy użyciu co najmniej jednej z trzech metod: poprzez podanie poświadczeń administratora licencji, klucza licencyjnego lub aktywacji programu w trybie offline.
64) Możliwość podejrzenia informacji o licencji, która znajduje się w programie.
65) W trakcie instalacji program ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór co najmniej następujących modułów do instalacji: kontrola dostępu do urządzeń, zapora osobista, ochrona poczty, ochrona protokołów, kontrola dostępu do stron internetowych, RMM.
66) Możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych.
67) Program musi posiadać możliwość definiowana stanów aplikacji, jakie będą wyświetlane użytkownikowi, co najmniej: ostrzeżeń o wyłączonych mechanizmach ochrony czy stanie licencji.
68) Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie.
69) Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
70) Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia zagrożenia.
71) Aplikacja musi posiadać dedykowany moduł, zapewniający ochronę przed oprogramowaniem wymuszającym okup.
72) Administrator ma możliwość dodania wykluczenia dla procesu, wskazując plik wykonywalny.
73) Program musi posiadać możliwość przeskanowania pojedynczego pliku, poprzez opcję „przeciągnij i upuść”.
74) Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
75) Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.
76) Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.
77) Administrator musi posiadać możliwość zastosowania reguł dla kontroli dostępu do stron w zależności od zdefiniowanego przedziału czasowego.
78) Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
79) Program musi umożliwiać ochronę przed dołączeniem komputera do sieci botnet.
80) Program ma posiadać pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.

4. **Ochrona przed spamem:**
    1) Program ma umożliwiać wyłączenie skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej.
    2) Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego.
    3) Możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną lub niepożądaną bezpośrednio z klienta pocztowego.
    4) Możliwość ręcznego dodania nadawcy wiadomości do białej lub czarnej listy bezpośrednio z klienta pocztowego.
    5) Możliwość definiowania folderu, gdzie program pocztowy będzie umieszczać spam.
    6) Możliwość zdefiniowania dowolnego tekstu, dodawanego do tematu wiadomości zakwalifikowanej jako spam.
    7) Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną, oznaczy ją jako „nieprzeczytana" Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości pożądanej na spam oznaczy ją jako „przeczytana". Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.

5. **Kontrola dostępu do stron internetowych**
    1) Aplikacja musi być wyposażona w zintegrowany moduł kontroli dostępu do stron internetowych.
    2) Moduł kontroli dostępu do stron internetowych musi posiadać możliwość utworzenia reguł w oparciu o użytkownika lub grupę użytkowników systemu Windows lub Active Directory.
    3) Aplikacja musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii. Podstawowe kategorie, w jakie aplikacja musi być wyposażona to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii.
    4) Moduł musi posiadać możliwość grupowania kategorii oraz adresów stron internetowych.
    5) Lista adresów URL znajdujących się w poszczególnych kategoriach, musi być automatycznie aktualizowana przez producenta.
    6) Administrator musi posiadać możliwość wyłączenia integracji modułu kontroli dostępu do stron internetowych.
    7) Aplikacja musi posiadać możliwość określenia przynajmniej jednej z akcji dla reguły kontroli dostępu do stron internetowych: zezwól, ostrzeż, blokuj.
    8) Program musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania, określonej w regułach, strony internetowej.

6. **Administracja zdalna**
    1. Serwer zarządzający musi być dostępny w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance) oraz dysku wirtualnego w formacie VHD.
    2. Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.
    3. Konsola administracyjna musi umożliwiać podgląd szczegółów, dotyczących bazy danych takich jak: serwer, nazwa, aktualny rozmiar, nazwa hosta, użytkownik.
    4. Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych.

5. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.
6. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
7. Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy.
8. Narzędzie administracyjne musi być kompatybilne z protokołami IPv4 oraz IPv6.
9. Podczas logowania do konsoli, administrator musi mieć możliwość wyboru języka, w jakim zostanie wyświetlony interfejs.
10. Zmiana języka interfejsu konsoli nie może wymagać jej zatrzymania, ani reinstalacji.
11. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
12. Konsola administracyjna musi ostrzegać administratora, kiedy używa niewspieranej przeglądarki, do administracji rozwiązaniem antywirusowym.
13. Narzędzie do administracji zdalnej musi posiadać moduł, pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.
14. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.
15. Serwer administracyjny musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
16. Serwer administracyjny musi posiadać wsparcie dla „VDI" oraz „Golden Master Image".
17. Instalacja serwera administracyjnego powinna posiadać możliwość pracy w sieci rozproszonej, nie wymagając dodatkowego serwera proxy.
18. Rozwiązanie ma posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
19. Administrator musi posiadać możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM.
20. Administrator musi posiadać możliwość instalacji serwera HTTP Proxy, pozwalającego na pobieranie aktualizacji silnika detekcji oraz pakietów instalacyjnych na stacjach roboczych.
21. Serwer HTTP Proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) pobieranych elementów.
22. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.
23. Serwer administracyjny musi posiadać możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi.
24. Serwer administracyjny musi pozwalać na zarządzanie programami zabezpieczającymi na maszynach z systemami Windows, MacOS, Linux, Android.
25. Serwer administracyjny musi pozwalać na centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, zapora osobista, kontrola dostępu do stron internetowych, które działają na stacjach roboczych w sieci.
26. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.
27. Administrator musi posiadać możliwość zarządzania stacjami roboczymi za pomocą dedykowanego agenta, na których nie jest zainstalowane oprogramowanie zabezpieczające.
28. Z poziomu konsoli zarządzania administrator ma mieć możliwość weryfikacji podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, typ i wersja oprogramowania układowego, 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 dla systemów Windows oraz MacOS z możliwością jego odinstalowania.

29. Serwer administracyjny musi posiadać możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.
30. Instalacja zdalna agenta z poziomu serwera administracyjnego nie może wymagać określenia architektury systemu (32 lub 64 bitowy) oraz jego rodzaju (Windows, MacOS, Linux), a wybór odpowiedniego pakietu musi być w pełni automatyczny.
31. W przypadku braku zainstalowanego produktu zabezpieczającego na urządzeniu mobilnym z systemem Android, musi istnieć możliwość jego pobrania ze sklepu Google Play.
32. Administrator musi posiadać możliwość utworzenia listy autoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.
33. Serwer administracyjny musi posiadać możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, a nie komunikację za pośrednictwem wiadomości SMS.
34. Administrator musi posiadać możliwość utworzenia użytkownika serwera administracyjnego.
35. Administrator musi posiadać możliwość dodania grupy użytkowników z Active Directory do serwera administracyjnego. Użytkownik grupy usługi katalogowej Active Directory musi mieć możliwość logowania się do konsoli administracyjnej swoimi poświadczeniami domenowymi.
36. Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
37. Serwer administracyjny musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, instalacją agentów, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
38. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.
39. Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta, bez konieczności logowania się do konsoli administracyjnej.
40. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności, po którym użytkownik zostanie automatycznie wylogowany.
41. Serwer administracyjny musi posiadać zadania klienta oraz zadania serwera. Zadania serwera muszą zawierać przynajmniej zadanie instalacji agenta, generowania raportów oraz synchronizacji elementów z Active Directory. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej.
42. Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji.
43. Serwer administracyjny musi posiadać możliwość instalacji oprogramowania z użyciem parametrów instalacyjnych.
44. Serwer administracyjny musi posiadać możliwość deinstalacji programu zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.
45. Serwer administracyjny musi posiadać możliwość wysłania polecenia: wyświetlenia komunikatu, aktualizacji systemu operacyjnego, zamknięcia komputera, uruchomienia ponownego komputera oraz uruchomienia komendy na stacji klienckiej.
46. Serwer administracyjny musi posiadać możliwość uruchomienia zadania automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.
47. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.

48. 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.
49. Serwer administracyjny musi posiadać możliwość utworzenia polityk dla programów zabezpieczających i komponentów środowiska serwera centralnego zarządzania.
50. Serwer administracyjny musi posiadać możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów.
51. Serwer administracyjny musi posiadać możliwość przypisania kilku polityk z innymi priorytetami dla pojedynczego klienta.
52. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień w programie zabezpieczającym na stacji roboczej.
53. Serwer administracyjny musi umożliwiać wyświetlenie polityk, które są przypisane do stacji.
54. Z poziomu konsoli musi istnieć możliwość scalania reguł zapory osobistej, harmonogramu, modułu HIPS z już istniejącymi regułami na stacji roboczej lub innej polityce.
55. Serwer administracyjny musi posiadać minimum 120 szablonów raportów, przygotowanych przez producenta.
56. Serwer administracyjny musi posiadać możliwość utworzenia własnych raportów.
57. Serwer administracyjny musi posiadać możliwość wyboru formy przedstawienia danych w raporcie w tym przynajmniej: w postaci tabeli, wykresu lub obu elementów jednocześnie.
58. Serwer administracyjny musi posiadać możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy.
59. Serwer administracyjny musi posiadać możliwość określenia danych, jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na osiach wykresu oraz ich odfiltrowania i posortowania.
60. Serwer administracyjny musi być wyposażony w mechanizm importu oraz eksportu szablonów raportów.
61. Serwer administracyjny powinien posiadać panel kontrolny z raportami, pozwalający na szybki dostępu do najbardziej interesujących danych. Panel ten musi być edytowalny.
62. Serwer administracyjny musi posiadać możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenia raportu na panelu kontrolnym. Raport może zostać wysłany za pośrednictwem wiadomości email, zapisany do pliku w formacie PDF, CSV oraz PS.
63. Raport na panelu kontrolnym musi być w pełni interaktywny, pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.
64. Serwer administracyjny musi posiadać możliwość utworzenia własnych powiadomień lub skorzystania z predefiniowanych wzorów.
65. Powiadomienia mailowe mają być wysyłane w formacie HTML.
66. Powiadomienia muszą być wywoływane po zmianie ilości członków danej grupy dynamicznej, wzroście liczby klientów grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń.
67. Administrator musi posiadać możliwość wysłania powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.
68. Serwer administracyjny musi posiadać możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu.
69. Serwer administracyjny musi posiadać możliwość synchronizacji danych dotyczących licencji.
70. Serwer administracyjny musi posiadać możliwość dodania licencji przynajmniej przy użyciu klucza licencyjnego, pliku offline licencji oraz konta systemu zarządzania licencjami.
71. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji produktów zarządzanych.

72. W przypadku posiadania tylko jednej dodanej licencji w konsoli zarządzania ma być ona wybierana automatycznie podczas konfiguracji zadania aktywacji lub instalacji produktu.
73. Serwer administracyjny musi posiadać możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela.
74. Serwer administracyjny musi posiadać możliwość wybudzania stacji roboczych przy użyciu Wake on Lan.
75. Serwer musi umożliwić podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.
76. Serwer ma posiadać możliwość wygenerowania dziennika diagnostycznego na stacji roboczej, który może zostać pobrany bezpośrednio z konsoli.
77. W szczegółach stacji roboczej, z poziomu konsoli, muszą być dostępne zaawansowane logi diagnostyczne, przynajmniej z modułów produktu zabezpieczającego, takich jak: antyspam, firewall, HIPS, kontrola dostępu do urządzeń, kontrola dostępu do stron internetowych.
78. Konsola webowa musi zawierać informacje, dotyczące wysłanych plików do analizy producenta.
79. Administrator musi mieć możliwość pobrania pliku z parametrami połączenia RDP do stacji roboczej bezpośrednio z poziomu konsoli.
80. Na panelu kontrolnym musi być dostępny dziennik zmian, dotyczący produktów zabezpieczających i komponentów środowiska centralnego zarządzania.
81. Serwer musi wspierać wysyłanie logów do systemu SIEM IBM qRadar w jego natywnym formacie.
82. Konsola administracyjna musi umożliwiać personalizację interfejsu webowego.
83. Konsola administracyjna musi mieć możliwość tagowania obiektów, w tym przynajmniej: polityki, zadania, komputery oraz szablony grupy dynamicznych.
84. Konsola administracyjna musi pozwalać na utworzenie wykluczeń globalnych, bez konieczności przypisywania ich do konkretnych polityk.
85. Serwer administracyjny musi oferować możliwość bezpośredniego sprawdzenia SHA-1 pliku, wykrytego przez produkt antywirusowy, na portalach służących do weryfikacji bezpieczeństwa (co najmniej VirusTotal).
86. Konsola administracyjna musi posiadać możliwość wyświetlania dziennika audytu czynności wykonanych przez administratorów serwera. Dziennik musi pozwalać na wyświetlanie informacji co najmniej ze zmian dotyczących: certyfikatów, zadań, wyzwalaczy, konfiguracji, grup, uprawnień administratorów, wykluczeń, powiadomień, raportów.

Jeżeli ze względu na zaoferowany przez Wykonawcę równoważne oprogramowanie zaistnieje konieczność poniesienia przez Zamawiającego dodatkowych nakładów (w szczególności na zmianę konfiguracji serwerów, usług sieciowych, szkolenie pracowników zamawiającego, wdrożenie dodatkowego oprogramowania zarządzającego) niezbędnych do sprawnego funkcjonowania serwerów w infrastrukturze teleinformatycznej Zamawiającego, wszelkie koszty z tym związane poniesie Wykonawca.

W przypadku odwołania się przez Zamawiającego w Opisie przedmiotu zamówienia do znaku towarowego, patentu, źródła pochodzenia, przyjmuje się, że Zamawiający wskazał wyłącznie na wymagane parametry, jakość, funkcjonalność i w tym zakresie Wykonawcy mogą oferować usługi i dostawy o równoważnych parametrach. W przypadku złożenia oferty o parametrach równoważnych, Wykonawca zobowiązany jest złożyć oświadczenie, że oferta jest równoważna z rozwiązaniami przyjętymi w opisie przedmiotu zamówienia. Wykonawca musi dołączyć dokumenty potwierdzające równoważność rozwiązań.

załącznik nr 2 do ZO

Polskie Radio – Regionalna Rozgłośnia w Poznaniu
Radio Poznań S.A.
ul. Berwińskiego 5
60-765 Poznań

FORMULARZ OFERTY

W odpowiedzi na ogłoszenie postępowania na **„Dostawę oprogramowania antywirusowego”** prowadzonego w trybie art. 2 ust. 1 ustawy z dnia 11 września 2019 roku Prawo zamówień publicznych z późn. zm. i zasad udzielania zamówień publicznych o wartości mniejszej niż 130.000,00 zł, wprowadzone uchwałą nr 17/12/2021/Z/XI Zarządu Spółki Radio Poznań S.A. z dnia 30.03.2021r. na podstawie § 3,.

1. **Dane dotyczące Wykonawcy**

   Nazwa Wykonawcy/Wykonawców: …

   Adres Wykonawcy/Wykonawców: …

   Województwo *(nazwa)***:** …**REGON lub NIP:** …

   Rodzaj Wykonawcy *(proszę wpisać odpowiednio zgodnie z poniższą listą)*: **……** *(mikroprzedsiębiorstwo, małe przedsiębiorstwo, średnie przedsiębiorstwo, jednoosobowa działalność gospodarcza, osoba fizyczna nieprowadząca działalności gospodarczej, inny rodzaj)*

   Reprezentowany przez: …

   telefon: ……., **adres poczty elektronicznej:** …

   adres skrzynki ePUAP: …

2. **Cena za realizację przedmiotu zamówienia.**

Dostawa oprogramowania antywirusowego w okresie od 01.07.2021 roku do 30.06.2024 roku.

Lp.	Nazwa producenta oprogramowania	Nazwa oprogramowania i dokładne oznaczenie wersji oferowanej licencji	Liczba licencji **/szt./**	Cena netto za sztukę **/zł/**	Wartość netto **/zł/**	Stawka VAT **/%/**	Wartość brutto **/zł/**
a	**b**	**c**	**d**	**e**	**F** = **d** x **e**	**g**	**H=F+(F** x **g)**
1							

2							
						RAZEM	

Słownie wartość brutto zł: ……

Oferowane oprogramowanie spełnia wszystkie wymagania określone w opisie przedmiotu zamówienia zawarte w załączniku nr 1 do ZO

Oferowana cena zawiera wszystkie koszty realizacji zamówienia określone na podstawie zapytania ofertowego

Termin realizacji zamówienia (*wymagany: maksymalnie 7 dni*): **……** dzień/dni (słownie:…… dzień/dni) **od dnia zawarcia umowy.**

Termin realizacji zamówienia (*wymagany: maksymalnie 7 dni*): **……** dzień/dni (słownie:…… dzień/dni) **od dnia zawarcia umowy.**

3. Warunki płatności: Wynagrodzenie płatne będzie w formie przelewu, na rachunek Wykonawcy w terminie **14 dni** od dnia dostarczenia prawidłowo wystawionej faktury VAT Zamawiającemu.

4. Oświadczamy, że jesteśmy związani niniejszą ofertą **do ……. 2021 roku.**

5. Dostawę określoną *wykonawca zamierza powierzyć podwykonawcom oraz podać nazwę podwykonawcy*) ……
(**Uwaga.** Punkt 5 należy wypełnić tylko w przypadku, gdy Wykonawca przewiduje udział Podwykonawcy w realizacji zamówienia).

6. Oświadczamy, że zapoznaliśmy się z treścią zapytania ofertowego z załącznikami (w skrócie: ZO) i przyjmujemy ją bez zastrzeżeń.

7. Oświadczamy, że zapoznaliśmy się z treścią umowy w zakresie *(niepotrzebne skreślić)* **oferowanej / oferowanych** przez nas dostawy i przyjmujemy ją bez zastrzeżeń.

8. Oświadczamy, że wybór naszej oferty ***(niepotrzebne skreślić)*** **będzie / nie będzie** prowadził do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług.

Z uwagi, iż wybór naszej oferty będzie prowadził do powstania obowiązku podatkowego u Zamawiającego wskazujemy następujące informacje:

Nazwa (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do powstania obowiązku podatkowego u Zamawiającego	Wartość bez podatku od towarów i usług **/zł/**	Kwota podatku od towarów i usług **/zł/**

9. Oświadczamy, że uzyskanie, zwielokrotnianie i rozpowszechnianie oprogramowania dokonywane w celu wykonania przedmiotowego zamówienia, nie naruszyło i nie będzie naruszać praw

własności intelektualnej żadnej osoby trzeciej i jest zgodne z Ustawą o prawie autorskim i prawach pokrewnych z dnia 4 lutego 1994 r. (tekst jednolity: Dz. U. z 2019, poz. 1231 z późn. zm.), Prawem własności przemysłowej z dnia 30 czerwca 2000 r. (tekst jednolity: Dz. U. z 2021, poz. 324) oraz innymi obowiązującymi przepisami polskiego prawa. Oświadczam również, że certyfikaty i etykiety producenta oprogramowania dołączone do oprogramowania i inne elementy oprogramowania, są oryginalne.

10. Oferujemy realizację zamówienia zgodnie z wymaganiami Zamawiającego, za cenę i w terminie podanym w niniejszym formularzu oferty na warunkach w nim określonych.

11. Oświadczamy, że akceptujemy warunki załączonego do ZO projektu umowy i zobowiązujemy się do podpisania umowy w przypadku wyboru naszej oferty w miejscu i terminie wskazany przez Zamawiającego.

12. Oświadczamy, że wycena przedmiotu umowy uwzględnia wszystkie uwarunkowania oraz czynniki związane z realizacją zamówienia i obejmuje cały zakres rzeczowy zamówienia – jest kompletna.

13. Oświadczam, że wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO[1)] wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem/pozyskałam w celu ubiegania się o udzielenie zamówienia w niniejszym postępowaniu.*

[1)] rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1 z późn. zm.).

* W przypadku gdy wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia wykonawca nie składa (usunięcie treści oświadczenia np. przez jego wykreślenie).

Oferta zawiera: ..... stron.

.....
(miejsce, data)

KWALIFIKOWANY PODPIS ELEKTRONICZNY, PODPIS ZAUFANY LUB PODPIS OSOBISTY osoby/osób uprawnionych/upoważnionych

OŚWIADCZENIE WYKONAWCY DOTYCZĄCE PODANYCH INFORMACJI

Oświadczam/ oświadczamy, że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia Zamawiającego w błąd przy przedstawianiu informacji.

……*(miejscowość),* dnia…….r.

…….

podpis elektroniczny kwalifikowany lub podpis zaufany lub osobisty osoby uprawnionej/ osób uprawnionych do reprezentowania Wykonawcy lub pełnomocnika lub podpis zaufany lub osobisty osoby uprawnionej/ osób uprawnionych do reprezentowania Wykonawcy lub pełnomocnik