|  |
| --- |
| **Dostawa oprogramowania antywirusowego** |
| 1 | **Równoważność oprogramowania antywirusowego** **w stosunku do oprogramowania określonego w punkcie 2 tabeli**.Przez równoważność oprogramowania należy rozumieć spełnienie następujących wymagań:1. oferowane oprogramowanie musi spełniać wymagania określone w punkcie 2 zawierającym specyfikację wymagań funkcjonalnych oraz zapewniać osiągnięcie poziomu zabezpieczeń nie mniejszego niż oferowane przez mechanizmy wdrożonego u Zamawiającego oprogramowania ESET PROTECT Essential (ESET Endpoint Protection Standard),
2. wykonawca przeszkoli personel techniczny w zakresie używania, zarządzania oraz administrowania dostarczonym programem:

- szkolenie dla 7 osób,- czas trwania szkolenia to minimum 4 godziny (zgodnie z ofertą Wykonawcy). Zamawiający dopuszcza maksymalnie 7 godzin szkolenia podczas 1 dnia roboczego, w przypadku zaoferowania dłuższego czasu trwania szkolenia konieczne będzie wydłużenie terminu szkolenia na kolejne dni robocze. Maksymalny punktowany czas trwania szkolenia to 14 godzin.- tryb szkolenia zdalny lub stacjonarny (na terenie miasta Kraków)- szkolenie odbędzie się w terminie ustalonym przez Zamawiającego i Wykonawcę, jednak nie później niż do 3 tygodni od dnia podpisania umowy - szkolenie wraz z wystawieniem certyfikatu zakończenia szkolenia dla każdego z uczestników. 1. wykonawca przygotuje i przekaże Zamawiającemu wersję elektroniczną w języku polskim instrukcji obsługi interfejsu użytkownika oprogramowania zainstalowanego na komputerze,
 |
| 2 | **Specyfikacja wymagań funkcjonalnych.**1. **Wymagania ogólne:**
2. pełne wsparcie dla systemu Windows 10/Windows11/Windows Server (od 2012 R2 w górę)/Linux Server (Debian wersje od 10 do 12, Centos wersje 7, 8, 9, RHEL wersje 7,8,9), podstawowe wsparcie dla MacOS: w sumie 500 licencji
3. Urządzenia mobilne Android 15 licencji,
4. wsparcie dla 64-bitowej wersji systemu Windows,
5. wersja programu dla stacji roboczych Windows dostępna w języku polskim,
6. **Ochrona antywirusowa i antyspyware:**
7. pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami,
8. program musi oferować funkcję samo-ochrony,
9. wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.,
10. skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików,
11. możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu,
12. możliwość skanowania dysków sieciowych i dysków przenośnych,
13. skanowanie plików spakowanych i skompresowanych,
14. możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach,
15. możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu,
16. 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,
17. skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook
18. skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie,
19. program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe,
20. możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych z opcją wygenerowania raportu ze skanowania i przesłania do konsoli zarządzającej,
21. możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie i skanerów rezydentnych),
22. możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, adresów MAC, wersji systemu operacyjnego oraz domeny, do której dana stacja robocza należy, ostatnio zalogowanego użytkownika,
23. możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu,
24. możliwość skanowania sieci z centralnego serwera zarządzającego w poszukiwaniu niezabezpieczonych stacji roboczych,
25. możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła,
26. 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,
27. program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu,
28. automatyczna, przyrostowa aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu,
29. program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli stron Internetowych i kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania,
30. wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
31. **Administracja zdalna: Konsola Cloud – serwer administracyjny po stronie producenta**
32. centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na w systemach wymienionych w pkt 1,
33. centralna konfiguracja: zarządzanie ochroną antywirusową, antyspyware’ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na urządzeniach klienckich,
34. serwer administracyjny musi oferować możliwość utworzenia jednego zadania dla kilku klientów lub grupy,
35. serwer administracyjny musi oferować możliwość utworzenia polityk dla programów zabezpieczających i modułów serwera centralnego zarządzania,
36. serwer administracyjny musi oferować możliwość skorzystania z raportów,
37. serwer administracyjny musi oferować możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela,
38. narzędzie administracyjne musi być wyposażone w mechanizm wyszukiwania zarządzanych komputerów na podstawie co najmniej nazwy komputera, adresu IPv4 i IPv6 lub wyszukania konkretnej nazwy zagrożenia,
 |
| 3 |  licencja: 36 miesięcy od daty rozpoczęcia licencji |

|  |
| --- |
| **Dostawa oprogramowania antywirusowego – Wypełnia Wykonawca** |
| Forma szkolenia – …………………………..Czas trwania szkolenia – ……………………. godzin |
| Termin dostawy - …………………….. dni |
| Specyfikacja wymagań funkcjonalnych: …………………….. |
| Nazwa produktu …………………………….. |