



Fundusze  
Europejskie



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



**cupt**  
CENTRUM UNIJNYCH  
PROJEKTÓW TRANSPORTOWYCH

Załącznik nr 1 do SWZ

## OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest zakup licencji antywirusowych AV dla Centrum Unijnych Projektów Transportowych na okres 36 m-cy.
2. W miejscach, gdzie w opisie wymagań technicznych - równoważnych wskazano znaki towarowe, Zamawiający, zgodnie z art. 99 ust. 5 ustawy Pzp, dopuszcza składanie ofert równoważnych. Za rozwiązanie „równoważne” uznany zostanie Przedmiot zamówienia, którego zaoferowane parametry będą nie gorsze/nie niższe niż parametry rozwiązania opisanego w ust. 3, a zastosowanie ich gwarantować będzie osiągnięcie konkretnych wymagań funkcjonalnych, zgodnie z założeniami i warunkami określonymi przez Zamawiającego. Produkty pochodzące od konkretnych producentów stanowią wyłącznie wzorzec jakościowy Przedmiotu zamówienia. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. W przypadku, gdy Wykonawca zaoferuje rozwiązanie równoważne, zobowiązany jest wykazać jego równoważność, w stosunku do Przedmiotu zamówienia opisanego w ust. 3.
3. Minimalne parametry techniczno-jakościowe Przedmiotu zamówienia przedstawione zostały poniżej:

### I. Zamówienie podstawowe

Licencja na oprogramowanie antywirusowe na serwery Windows / Linux - 75 szt.

L.p.	Nazwa Oprogramowania	Opis wymagań technicznych
1	F-Secure Server Security <i>lub równoważny</i>	<p>Zaoferowane oprogramowanie musi spełniać, następujące wymagania:</p> <ol style="list-style-type: none"> <li>1. Ochrona serwerów: <ul style="list-style-type: none"> <li>• Microsoft® Windows Server 2016</li> <li>• Microsoft® Windows Server 2019</li> <li>• Microsoft® Windows Server 2022</li> <li>• Debian 10.x</li> <li>• Debian 11.x</li> <li>• Debian 12.x</li> </ul> </li> <li>1. Wsparcie dla poniższych wersji bazy danych Microsoft SQL Server: <ul style="list-style-type: none"> <li>• Microsoft® SQL Server 2014 (Enterprise, Business Intelligence, Standard, or Express Edition)</li> <li>• Microsoft® SQL Server 2016 (Enterprise, Business Intelligence, Standard, or Express Edition)</li> </ul> </li> </ol>



		<ul style="list-style-type: none"> <li>• Microsoft® SQL Server 2017 (Enterprise, Business Intelligence, Standard, or Express Edition</li> <li>• Microsoft® SQL Server 2017 (Enterprise, Business Intelligence, Standard, or Express Edition</li> </ul> <ol style="list-style-type: none"> <li>2. Ochrona całego systemu monitorowana i zarządzana z pojedynczej, centralnej konsoli.</li> <li>3. Zarządzanie aplikacją poprzez interfejs dostępny przez protokół https.</li> <li>4. Możliwość określenia adresów IP, z których można zarządzać aplikacją.</li> <li>5. Możliwość określenia portu, na którym dostępny będzie interfejs zarządzający aplikacją.</li> <li>6. Co najmniej dwa różne silniki antywirusowe, każdy z dedykowanymi bazami sygnatur, funkcjonujące jednocześnie i skanujące wszystkie dane.</li> <li>7. Zintegrowany silnik „antyrootkitowy”.</li> <li>8. Co najmniej dwa dedykowane silniki „antyspyware”.</li> <li>9. Możliwość blokowania zapytań DNS do witryn sklasyfikowanych, jako niebezpieczne lub podejrzane.</li> <li>10. Możliwość zezwolenia na zapytania DNS tylko do witryn sklasyfikowanych, jako zaufane.</li> <li>11. Skanowanie przez program na serwerze danych pobieranych i wysyłanych danych przy pomocy protokołu http.</li> <li>12. Blokowanie przez program na serwerze określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.</li> <li>13. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez serwery reputacyjne producenta.</li> <li>14. Ochrona przeglądarki internetowej, w tym: blokowanie wyskakujących okienek, blokowanie ciasteczek (cookies), blokowanie możliwości zmian ustawień w IE, analiza uruchamianych skryptów ActiveX</li> <li>15. Ochrona podczas przeglądania sieci Internet na podstawie badania reputacji – moduł działający na bazie Network Interceptor Framework (niezależnie od rodzaju i wersji przeglądarki).</li> </ol>
--	--	--



		<ol style="list-style-type: none"><li>16. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie, jak i ściąganie plików i ręczna aktualizacja na stacjach roboczych bez dostępu do Internetu.</li><li>17. Możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów za pomocą centralnej konsoli lub lokalnie przez określonego klienta.</li><li>18. Możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.</li><li>19. Możliwość wywołania skanowania podczas uruchamiania systemu operacyjnego lub po zalogowaniu użytkownika.</li><li>20. Możliwość wywołania szybkiego skanowania pod kątem programów typu rootkit.</li><li>21. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie operacyjnym.</li><li>22. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.</li><li>23. Możliwość pobierania aktualizacji definicji wirusów bezpośrednio z serwerów producenta, centralnej konsoli, dedykowanego proxy lub z innej stacji roboczej gdzie zainstalowane jest oprogramowanie antywirusowe.</li><li>24. Heurystyczna technologia do wykrywania nowych, nieznanych wirusów.</li><li>25. Wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „wirus”, „keylogger”, „dialer”, „trojan”, rootkitami”, „spyware”, ataki typu 0-day.</li><li>26. Program powinien posiadać kwarantannę wirusów, spyware oraz riskware.</li><li>27. Mechanizm skanujący wspólny dla wszystkich platform sprzętowych i programowych, wszystkich maszyn, wszystkich wersji oprogramowania, w tym bez względu na wersję językową oprogramowania – bez względu na to jak duża jest sieć lub jak bardzo jest złożona.</li><li>28. Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację</li></ol>
--	--	--



Fundusze  
Europejskie



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



cupt  
CENTRUM UNIJNYCH  
PROJEKTÓW TRANSPORTOWYCH

		<p>kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).</p> <p>29. Obsługa plików skompresowanych obejmująca najpopularniejsze formaty, w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2.</p> <p>30. Automatyczne usuwanie wirusów i zgłaszanie alertów w przypadku wykrycia wirusa.</p> <p>31. Automatyczne uruchamianie procedur naprawczych.</p> <p>32. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.</p> <p>33. Zarządzanie poprzez przeglądarkę WWW oraz centralnie z poziomu jednolitego systemu centralnego zarządzania dla systemów antywirusowych oferowanych przez producenta.</p> <p>34. Blokowanie aktywności sieciowej związanej ze znanymi botnetami włączając w to ataki ransomware i ataki ukierunkowane.</p> <p>35. Dezinstalacja oprogramowania antywirusowego na kliencie chroniona hasłem.</p> <p>36. Dodatkowe wymagania w przypadku systemów Linux:</p> <ul style="list-style-type: none"> <li>• Ochrona serwerów pracujących pod kontrolą systemu Linux</li> <li>• Ochrona całego systemu monitorowania i zarządzania lokalnie przy pomocy dowolnej przeglądarki WWW</li> <li>• Możliwość centralnego zarządzania w sposób zdalny wszystkimi istotnymi funkcjami oprogramowania wraz z opcją blokady ustawień</li> </ul>
--	--	---

## 2. Licencja na oprogramowanie antywirusowe na serwery pocztowe – 2 szt.

L.p.	Nazwa Oprogramowania	Opis wymagań technicznych
1	F-Secure Email and Server Security <i>lub równoważny</i>	<p>Zamawiający dopuszcza możliwość przedstawienia Oferowane oprogramowanie antywirusowe musi spełniać następujące wymagania:</p> <p>1. Możliwość instalacji na następujących systemach operacyjnych:</p> <ul style="list-style-type: none"> <li>• Microsoft® Windows Server 2016</li> <li>• Microsoft® Windows Server 2019</li> <li>• Microsoft® Windows Server 2022</li> </ul> <p>2. Możliwość integracji z następującymi serwerami poczty:</p> <ul style="list-style-type: none"> <li>• Microsoft Exchange Server 2016</li> <li>• Microsoft Exchange Server 2019</li> </ul>



		<p>3. Wsparcie dla następujących ról dla Microsoft Exchange Server 20016/2019:</p> <ul style="list-style-type: none"><li>• Edge Server role</li><li>• Hub Server role</li><li>• Mailbox Server role</li><li>• Combo Server (Mailbox Server and Hub Server roles)</li></ul> <p>4. Wsparcie dla poniższych konfiguracji Microsoft Exchange Server clusters:</p> <ul style="list-style-type: none"><li>• Microsoft Exchange Server 2016 Database Availability Groups</li><li>• Microsoft Exchange Server 2019 Database Availability Groups</li></ul> <p>5. Usuwanie niepożądanych treści typu „wirus”, „trojan”, „dialer”, „worm”, „exploit”, znajdujących się na serwerze pocztowym.</p> <p>6. Wsparcie dla architektury „active-active cluster” oraz „active-passive cluster”.</p> <p>7. Ochrona całego systemu monitorowana i zarządzana z pojedynczej, centralnej konsoli.</p> <p>8. Zarządzanie aplikacją poprzez interfejs dostępny przez protokół https.</p> <p>9. Możliwość określenia adresów IP, z których można zarządzać aplikacją.</p> <p>10. Możliwość określenia portu, na którym dostępny będzie interfejs zarządzający aplikacją.</p> <p>11. Co najmniej trzy różne silniki antywirusowe, każdy z dedykowanymi bazami sygnatur, funkcjonujące jednocześnie i skanujące wszystkie dane.</p> <p>12. Zintegrowany silnik „antymalware”.</p> <p>13. Co najmniej dwa dedykowane silniki „antyspyware”.</p> <p>14. Możliwość blokowania zapytań DNS do witryn sklasyfikowanych, jako niebezpieczne lub podejrzane.</p> <p>15. Możliwość zezwolenia na zapytania DNS tylko do witryn sklasyfikowanych, jako zaufane.</p> <p>16. Skanowanie przez program na serwerze pocztowym, danych pobieranych i wysyłanych danych przy pomocy protokołu http.</p> <p>17. Blokowanie przez program na serwerze pocztowym, określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.</p>
--	--	--



		<p>18. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez serwery reputacyjne producenta.</p> <p>19. Ochrona podczas przeglądania sieci Internet na podstawie badania reputacji – moduł działający na bazie Network Interceptor Framework (niezależnie od rodzaju i wersji przeglądarki).</p> <p>20. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie, jak i ściągnięcie plików i ręczna aktualizacja na stacjach roboczych bez dostępu do Internetu.</p> <p>21. Możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów za pomocą centralnej konsoli lub lokalnie przez określonego klienta.</p> <p>22. Możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.</p> <p>23. Możliwość wywołania skanowania podczas uruchamiania systemu operacyjnego lub po zalogowaniu użytkownika.</p> <p>24. Możliwość wywołania szybkiego skanowania pod kątem programów typu rootkit.</p> <p>25. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie operacyjnym.</p> <p>26. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.</p> <p>27. Możliwość pobierania aktualizacji definicji wirusów bezpośrednio z serwerów producenta, centralnej konsoli, dedykowanego proxy lub z innej stacji roboczej gdzie zainstalowane jest oprogramowanie antywirusowe.</p> <p>28. Heurystyczna technologia do wykrywania nowych, nieznanych wirusów.</p> <p>29. Wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „wirus”, „keylogger”, „dialer”, „trojan”.</p> <p>30. Program powinien posiadać kwarantannę wirusów, spyware oraz riskware.</p> <p>31. Mechanizm skanujący wspólny dla wszystkich platform sprzętowych i programowych, wszystkich maszyn, wszystkich wersji oprogramowania, w tym bez względu na wersję językową oprogramowania – bez</p>
--	--	--



		<p>względu na to jak duża jest sieć lub jak bardzo jest złożona.</p> <p>32. Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).</p> <p>33. Obsługa plików skompresowanych obejmująca najpopularniejsze formaty, w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2.</p> <p>34. Automatyczne usuwanie wirusów i zgłaszanie alertów w przypadku wykrycia wirusa.</p> <p>35. Automatyczne uruchamianie procedur naprawczych.</p> <p>36. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.</p> <p>37. Zarządzanie poprzez przeglądarkę WWW oraz centralnie z poziomu jednolitego systemu centralnego zarządzania dla systemów antywirusowych oferowanych przez producenta.</p> <p>38. Możliwość dodawania własnych reguł i klasyfikowania wiadomości.</p> <p>39. Możliwość definiowania czarnych i białych list nadawców, odbiorców, domen internetowych, adresów IP, itp.</p> <p>40. Możliwość dodawania tzw. „disclaimer” do przeskanowanego maila.</p> <p>41. Możliwość współpracy z innymi produktami antywirusowymi producenta dla serwerów/gateway'ów na tej samej stacji roboczej/serwerze.</p> <p>42. Definiowanie własnych powiadomień i ostrzeżeń, także w języku polskim.</p> <p>43. Kwarantanna lokalna dla treści sklasyfikowanych, jako niebezpieczne.</p> <p>44. Możliwość usuwania tylko i wyłącznie niebezpiecznych elementów (np. załącznik w przesyłce e-mail lub skrypt Active-X) z analizowanych danych.</p> <p>45. Wykrywanie treści zaszyfrowanych i zahasłowanych z możliwością traktowania ich, jako niebezpieczne.</p> <p>46. Inteligentne rozpoznawanie plików i załączników, niezależnie od tego, jakie rozszerzenie one posiadają.</p> <p>47. Skanowanie wszystkich przesyłanych treści, czyli załączników, skryptów oraz body e-maila.</p> <p>48. Blokowanie aktywności sieciowej związanej ze znanymi botnetami włączając w to ataki ransomware i ataki ukierunkowane.</p>
--	--	---





Fundusze  
Europejskie



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



cupt  
CENTRUM UNIJNYCH  
PROJEKTÓW TRANSPORTOWYCH

		<p>49. Możliwość ustawiania hasła w celu odinstalowania produktu</p> <p>50. Skanowanie w trybie testowym umożliwiające w celu sprawdzenia jak wiadomości i maila będą przetwarzane na podstawie bieżących ustawień</p>
--	--	--

### 3. Licencja na oprogramowanie antywirusowe na stacje robocze - 384 szt.

L.p.	Nazwa Oprogramowania	Opis wymagań technicznych
1	F-Secure Client Security lub równoważny	<p>Oferowane oprogramowanie antywirusowe musi spełniać następujące wymagania:</p> <ol style="list-style-type: none"> <li>Ochrona stacji klienckich z systemem: <ul style="list-style-type: none"> <li>Windows 10 (64 bit)</li> <li>Windows 11 (64 bit)</li> </ul> </li> <li>Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanowania heurystycznego, modułu skanującego nośniki i monitora poczty elektronicznej, monitora ruchu http oraz moduł antyrootkitowy.</li> <li>Co najmniej trzy różne silniki antywirusowe, funkcjonujące jednocześnie i skanujące wszystkie dane.</li> <li>Oddzielny silnik skanujący do wykrywania niepożądanych aplikacji takich jak oprogramowanie typu „spyware”, „adware”, „keylogger”, „dialer”, „trojan”.</li> <li>Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie, jak i ściągnięcie pliku offline ze strony producenta i ręczna aktualizacja na stacjach roboczych bez dostępu do Internetu.</li> <li>Możliwość wywołania skanowania komputera na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów za pomocą centralnej konsoli lub lokalnie przez określonego klienta.</li> <li>Możliwość wywołania skanowania komputera w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.</li> <li>Możliwość wywołania skanowania podczas uruchamiania systemu operacyjnego lub po zalogowaniu użytkownika.</li> <li>Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga</li> </ol>





		<p>zatrzymania procesu skanowania na jakimkolwiek systemie.</p> <ol style="list-style-type: none"> <li>10. Mikrodefinicje wirusów – przyrostowe (inkrementalne) - pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).</li> <li>11. Możliwość pobierania aktualizacji definicji wirusów bezpośrednio z serwerów producenta, centralnej konsoli, dedykowanego proxy lub z innej stacji roboczej gdzie zainstalowane jest oprogramowanie antywirusowe.</li> <li>12. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.</li> <li>13. Heurystyczna technologia do wykrywania nowych, nieznanych wirusów.</li> <li>14. Wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware”, „adware”, „keylogger”, „dialer”, „trojan”, „rootkit” oraz ataki typu 0-day</li> <li>15. Możliwość umieszczenia oprogramowania typu „spyware”, „adware”, „keylogger”, „dialer”, „trojan” w kwarantannie.</li> <li>16. Ochrona pliku 'hosts' przed niepożądanymi wpisami.</li> <li>17. Mechanizm centralnego zarządzania elementami kwarantanny znajdującymi się na stacjach klienckich.</li> <li>18. Mechanizm określania źródeł ataków prowadzonych przy użyciu zagrożeń hybrydowych, takich jak Code Red i Nimda.</li> <li>19. Obsługa plików skompresowanych obejmująca najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2</li> <li>20. Automatyczne usuwanie wirusów oraz oprogramowania typu malware i zgłaszanie alertów w przypadku wykrycia wirusa.</li> <li>21. Logowanie historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów z poziomu GUI aplikacji.</li> <li>22. Automatyczne uruchamianie procedur naprawczych.</li> </ol>
--	--	---



		<ol style="list-style-type: none"><li>23. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.</li><li>24. Średni czas reakcji producenta na nowy wirus poniżej 8 godzin, 24 godziny na dobę przez cały rok (24/7/365).</li><li>25. Automatyczne powiadomienie użytkowników oraz administratora o wykrytych zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona.</li><li>26. Skanowanie przez program na komputerze klienckim, danych pobieranych i wysyłanych danych przy pomocy protokołu http.</li><li>27. Blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.</li><li>28. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez serwery reputacyjne producenta.</li><li>29. Automatyczna kwarantanna blokująca ruch przychodzący i wychodzący, włączająca się w momencie, gdy stacja robocza posiada stare sygnatury antywirusowe.</li><li>30. Wsparcie dla technologii Microsoft Network Access Protection (NAP).</li><li>31. Ochrona podczas przeglądania sieci Internet na podstawie badania reputacji – moduł działający na bazie Network Interceptor Framework (niezależnie od rodzaju i wersji przeglądarki).</li><li>32. Możliwość ręcznego aktualizowania baz definicji wirusów poprzez odrębny plik wykonywalny dostarczony przez producenta.</li><li>33. Ochrona rejestrów systemowych, w tym odpowiedzialnych za konfigurację przeglądarki Internet Explorer, listę uruchamianych aplikacji przy starcie, przypisania rozszerzeń plików do zadanych aplikacji.</li><li>34. Kontrola oraz możliwość blokowania aplikacji próbujących uzyskać połączenie z Internetem lub siecią lokalną.</li><li>35. Osobista zapora ogniowa (tzw. personal firewall) z możliwością definiowania profili bezpieczeństwa możliwych do przypisania</li></ol>
--	--	---



Fundusze  
Europejskie



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



cupt  
CENTRUM UNIJNYCH  
PROJEKTÓW TRANSPORTOWYCH

		<p>dla pojedynczej stacji roboczej lub grup roboczych.</p> <p>36. Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.</p> <p>37. Możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej)</p> <p>38. Użytkownik podczas próby przejścia na witrynę znajdująca się w zablokowanej przez Administratora kategorii musi zostać powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej.</p> <p>39. Możliwość blokowania witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS.</p> <p>40. Możliwość blokowania zapytań DNS do witryn sklasyfikowanych, jako niebezpieczne lub podejrzane.</p> <p>41. Możliwość zezwolenia na zapytania DNS tylko do witryn sklasyfikowanych, jako zaufane.</p> <p>42. Brak konieczności restartu komputera po zainstalowaniu aplikacji w środowisku Windows 7/8/8.1, 10, 11.</p> <p>43. Możliwość automatycznego odinstalowania innego oprogramowania AV.</p> <p>44. Moduł kontroli urządzeń zapewniający możliwość zezwolenia lub zablokowania dostępu do urządzeń zewnętrznych (np. napędy USB, urządzenia bluetooth, czytniki kart pamięci, napędy CD/DVD, stacje dyskiety).</p> <p>45. Moduł kontroli urządzeń zarządzany z poziomu konsoli centralnego zarządzania.</p> <p>46. Moduł kontroli urządzeń umożliwia dodanie 'zaufanego urządzenia' poprzez podanie jego identyfikatora sprzętu.</p> <p>47. Blokowanie aktywności sieciowej związanej ze znanymi botnetami włączając w to ataki ransomware i ataki ukierunkowane</p>
--	--	--

#### 4. Licencja na oprogramowanie antywirusowe na urządzenia mobilne - 368 szt.

L.p.	Nazwa Oprogramowania	Opis wymagań technicznych
1	F-Secure Elements EPP for Mobiles lub równoważne	1. Dostarczone licencje muszą być w pełni kompatybilne z posiadanym przez Zamawiającego systemem F-Secure Protection Service for Business



		<p>Możliwość wdrożenia oraz aktualizacji i usuwania oprogramowania za pośrednictwem rozwiązania MDM VMware Workspace One Advanced.</p> <p>2. Licencje muszą zapewniać ochronę i wsparcie dla urządzeń mobilnych z systemami operacyjnymi:</p> <ul style="list-style-type: none"> <li>- Android (min. w wersji 8.x i wyższych),</li> </ul> <p>3. Możliwość centralnego zarządzania chronionymi urządzeniami mobilnymi, z opcją zmiany zasad bezpieczeństwa.</p> <p>4. Możliwość monitorowania stanu zabezpieczeń chronionych urządzeń, w tym dostęp do szczegółowych informacji takich jak numer telefonu czy wersja systemu operacyjnego.</p> <p>5. Możliwość automatycznego szyfrowania ruchu sieciowego podczas korzystania z publicznych sieci Wi-Fi i sieci komórkowych.</p> <p>6. Możliwość ukrycia lub zmiany wirtualnej lokalizacji urządzenia.</p> <p>7. Możliwość anonimowego połączenia internetowego przez ukrycie adresu IP urządzenia.</p> <p>8. Możliwość blokowania reklam internetowych.</p> <p>9. Możliwość chmurowej analizy zagrożeń pojawiających się na urządzeniach np. z wykorzystaniem algorytmów Big Data.</p> <p>10. Funkcja sprawdzania reputacji plików i aplikacji w czasie rzeczywistym.</p> <p>11. Funkcje ochrony przed przeglądaniem złośliwych witryn internetowych.</p> <p>12. Licencja powinna zapewniać wysoki poziom ochrony przeglądania niezależnie od rodzaju przeglądarki internetowej.</p> <p>13. Licencja powinna zapewniać ochronę przed śledzeniem użytkownika (ochrona przed zbieraniem informacji o wyszukiwanych hasłach, odwiedzanych stronach i klikniętych banerach, ochrona przed zbieraniem informacji o lokalizacji geograficznej, ochrona przed zbieraniem informacji przez pliki cookie, skrypty lub śledzenie pikseli).</p> <p>14. Możliwość zmniejszenia zużycia transferu danych dzięki blokowaniu zbędnego ruchu sieciowego, takiego jak reklamy oraz metody śledzenia użytkownika.</p> <p>16. Możliwość wdrożenia, w przypadku systemu Android, programu klienckiego za pomocą Google Play lub instalację pakietu APK.</p> <p>17. Możliwość wdrożenia, w przypadku systemu iOS, programu klienckiego za pomocą Apple App Store.</p> <p>18. Interfejs użytkownika w języku polskim.</p>
--	--	--



Fundusze  
Europejskie



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



cupt  
CENTRUM UNIJNYCH  
PROJEKTÓW TRANSPORTOWYCH

5. Licencja na oprogramowanie do centralnego systemu zarządzania - 1 szt.

L.p.	Nazwa Oprogramowania	Opis wymagań technicznych
1	F-Secure Policy Manager lub równoważny	<p>F-Secure Policy Manager w wersji min. 15.21 lub równoważny</p> <p>Oferowane oprogramowanie antywirusowe musi spełniać następujące wymagania:</p> <ol style="list-style-type: none"> <li>1. System centralnego zarządzania może być zainstalowany na wersjach serwerowych Microsoft Windows oraz Linux.</li> <li>2. Instalacja sytemu centralnego zarządzania dla Microsoft Windows musi wspierać następujące wersje systemów operacyjnych: <ul style="list-style-type: none"> <li>· Windows Server 2012 R2: Essentials, Standard, Datacenter</li> <li>· Windows Server 2016 : Essentials, Standard, Datacenter</li> <li>· Windows Server 2019: Essentials, Standard, Datacenter</li> <li>· Windows Server 2022: Essentials, Standard, Datacenter</li> </ul> </li> <li>3. Instalacja sytemu centralnego zarządzania dla Linux musi wspierać następujące wersje systemów operacyjnych: <ul style="list-style-type: none"> <li>· Debian 10.x</li> <li>· Debian 11.x</li> <li>· Debian 12.x</li> </ul> </li> <li>4. Konsola zarządzania umożliwia eksport pakietu instalacyjnego dla klienta w formacie Microsoft Installer (MSI) i JAR lub też bezpośrednią instalację zdalną nienadzorowaną.</li> <li>5. Narzędzie instalacyjne musi sprawdzać istnienie poprzednich wersji oprogramowania. W przypadku znalezienia poprzedniej wersji instalator powinien pozostawić ustawienia użytkownika, usunąć starsze oprogramowanie z klienta lub serwera i instalować nową wersję.</li> <li>6. Pełna administracja konfiguracją i monitorowanie stacji roboczych i serwerów plików za pomocą konsoli administracyjnej (centralna instalacja, konfiguracja w czasie rzeczywistym, zarządzanie, raportowanie i administrowanie oprogramowaniem).</li> <li>7. Komunikacja pomiędzy serwerem centralnego zarządzania a stacjami roboczymi musi być</li> </ol>



		<p>zaszyfrowana lub sygnowana stosownymi kluczami prywatnymi i publicznymi.</p> <ol style="list-style-type: none"><li>8. Scentralizowane blokowanie i odblokowywanie dostępu użytkownika do zmian konfiguracyjnych oprogramowania klienckiego, konsola pozwala na zdalne zarządzanie wszystkimi ustawieniami klienta.</li><li>9. Administratorzy muszą mieć możliwość tworzenia logicznych grup klientów i serwerów, w celu zarządzania oraz wymuszania określonych dla grupy zasad bezpieczeństwa.</li><li>10. Centralna konsola administracyjna musi umożliwiać przenoszenie klientów z jednej grupy do drugiej z możliwością zachowania ustawień lub dziedziczenia ustawień grupy.</li><li>11. Możliwość zmiany ustawień dla poszczególnych grup, umożliwienie administratorom zarządzania poszczególnymi klientami i funkcjonalnymi grupami klientów (tworzenie grup klientów).</li><li>12. Tworzenie grup, zdalne instalowanie oprogramowania oraz wymuszanie stosowania określonych zasad i ustawień na klientach.</li><li>13. Możliwość importu struktury drzewa z Microsoft Active Directory.</li><li>14. Możliwość tworzenia reguł synchronizacji z Microsoft Active Directory umożliwiających automatyczną synchronizację klientów z aktualnie istniejącymi grupami komputerów</li><li>15. Możliwość tworzenia reguł powiadamiania o nowych, niezarządzanych klientach w Microsoft Active Directory.</li><li>16. Możliwość blokowania wszystkich ustawień konfiguracyjnych stacji roboczych w celu uniemożliwienia ich modyfikacji przez użytkowników.</li><li>17. Możliwość zdefiniowania hasła do odinstalowania aplikacji.</li><li>18. Możliwość definiowania harmonogramów lub częstotliwości automatycznego pobierania aktualizacji definicji wirusów od producenta oprogramowania przez serwer zarządzający.</li><li>19. Możliwość instalacji i konfiguracji wewnętrznego serwera aktualizacji, łączącego się z serwerem aktualizacji producenta i aktualizacja serwerów, serwera zarządzającego oraz stacji roboczych z wewnętrznego serwera aktualizacji.</li><li>20. Możliwość ustalenia dodatkowego harmonogramu pobierania przez serwery plików i stacje robocze aktualizacji z serwera producenta.</li></ol>
--	--	--



		<ol style="list-style-type: none"><li>21. Funkcja przechowywania i przekazywania danych umożliwiającą przechowywanie przez klientów danych dotyczących zdarzeń, w sytuacji, jeśli nie mogą oni uzyskać połączenia z serwerem zarządzania. Dane muszą być przesyłane do serwera zarządzania podczas kolejnego połączenia.</li><li>22. Możliwość włączania/wyłączania wyświetlania komunikatów o znalezionych wirusach na wybranych stacjach klienckich.</li><li>23. Umożliwienie administratorom na audyt sieci, polegający na wykryciu niechronionych węzłów narażonych na ataki wirusowe.</li><li>24. Automatyczne wykrywanie i usuwanie oprogramowanie innych wiodących producentów systemów antywirusowych podczas instalacji.</li><li>25. Automatyczne uaktualnianie bazy definicji wirusów oraz mechanizmów skanujących nie rzadziej, niż co 7 dni (zalecane codzienne aktualizacje).</li><li>26. Automatyczne pobieranie przez program antywirusowy klienta zaktualizowanych definicji wirusów, jeśli aktualnie przechowywane pliki są przestarzałe.</li><li>27. Możliwość eksportu raportów z pracy systemu do pliku HTML.</li><li>28. Możliwość natychmiastowej aktualizacji przez serwer definicji wirusów na stacjach klienckich.</li><li>29. Możliwość uruchomienia aktualizacji stacji roboczych i serwerów przez użytkowników „na żądanie”.</li><li>30. Program musi pozwalać administratorowi na określenie reakcji w przypadku wykrycia wirusa.</li><li>31. Program musi pozwalać na określenie obszarów skanowania, tj.: pliki, katalogi, napędy lokalne i sieciowe.</li><li>32. Program musi pozwalać na skanowanie pojedynczych plików przez dodanie odpowiedniej opcji do menu kontekstowego (po kliknięciu prawym przyciskiem myszy).</li><li>33. Program musi pozwalać na określenie typów skanowanych plików, momentu ich skanowania (otwarcie, modyfikacja) oraz na wykluczenie ze skanowania określonych folderów.</li><li>34. Dedykowany system raportowania dostępny przez przeglądarkę internetową umożliwiający podgląd statystyk dotyczących wykrytych wirusów, przeprowadzonych ataków, zainstalowanego oprogramowania oraz statystyk połączenia stacji klienckich.</li></ol>
--	--	---





		<p>35. System raportowania umożliwiający wysyłanie raportów poprzez pocztę elektroniczną zgodnie z harmonogramem określonym przez administratora.</p> <p>36. Zarządzanie zdarzeniami i raportowanie – natychmiastowe alarmowanie o aktywności wirusów w administrowanej sieci na kilka sposobów: poczta elektroniczna, powiadomienia przez SNMP, raportowanie do dziennika systemowego, raportowanie do systemu centralnego zarządzania.</p> <p>37. Możliwość przekierowania alertów bezpośrednio do serwera Syslog.</p> <p>38. Możliwość tworzenia wielu kont dostępu do systemu centralnego zarządzania dla różnych użytkowników (w tym możliwość nadaniu danemu użytkownikowi ograniczonych praw).</p> <p>39. System umożliwiający wykonanie pełnej kopii bazy danych systemu zarządzania centralnego bez konieczności ręcznego wyłączenia programu.</p> <p>40. Pełna kopia bazy danych systemu zarządzania centralnego może być wykonywana automatycznie zgodnie z harmonogramem określonym przez administratora.</p> <p>41. Administrator ma możliwość określenia liczby kopii bazy danych, jaka będzie przetrzymywana.</p> <p>42. Możliwość wygenerowania danych diagnostycznych z podpiętych komputerów za pomocą konsoli zarządzającej.</p> <p>43. Możliwość bezpośredniego pobrania z komputera danych diagnostycznych z poziomu konsoli zarządzającej.</p> <p>44. Możliwość opisywania wprowadzonej konfiguracji za pomocą notatek umieszczonych w interfejsie graficznym konsoli zarządzającej.</p>
--	--	--

## II. Prawo opcji

6. Licencja na oprogramowanie antywirusowe na stacje robocze - 30 szt.

L.p.	Nazwa Oprogramowania	Opis wymagań technicznych
1	F-Secure Client Security lub równoważny	<p>Oferowane oprogramowanie antywirusowe musi spełniać następujące wymagania:</p> <ol style="list-style-type: none"> <li>Ochrona stacji klienckich z systemem: <ul style="list-style-type: none"> <li>Windows 10 (64 bit)</li> <li>Windows 11 (64 bit)</li> </ul> </li> <li>Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanowania heurystycznego, modułu skanującego nośniki</li> </ol>



		<p>i monitora poczty elektronicznej, monitora ruchu http oraz moduł antyrootkitowy.</p> <ol style="list-style-type: none"> <li>3. Co najmniej trzy różne silniki antywirusowe, funkcjonujące jednocześnie i skanujące wszystkie dane.</li> <li>4. Oddzielny silnik skanujący do wykrywania niepożądanych aplikacji takich jak oprogramowanie typu „spyware”, „adware”, „keylogger”, „dialer”, „trojan”.</li> <li>5. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie, jak i ściągnięcie pliku offline ze strony producenta i ręczna aktualizacja na stacjach roboczych bez dostępu do Internetu.</li> <li>6. Możliwość wywołania skanowania komputera na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów za pomocą centralnej konsoli lub lokalnie przez określonego klienta.</li> <li>7. Możliwość wywołania skanowania komputera w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.</li> <li>8. Możliwość wywołania skanowania podczas uruchamiania systemu operacyjnego lub po zalogowaniu użytkownika.</li> <li>9. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie.</li> <li>10. Mikrodefinicje wirusów – przyrostowe (inkrementalne) - pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).</li> <li>11. Możliwość pobierania aktualizacji definicji wirusów bezpośrednio z serwerów producenta, centralnej konsoli, dedykowanego proxy lub z innej stacji roboczej gdzie zainstalowane jest oprogramowanie antywirusowe.</li> <li>12. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.</li> </ol>
--	--	---



		<ol style="list-style-type: none"> <li>13. Heurystyczna technologia do wykrywania nowych, nieznanych wirusów.</li> <li>14. Wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware”, „adware”, „keylogger”, „dialer”, „trojan”, „rootkit” oraz ataki typu 0-day</li> <li>15. Możliwość umieszczenia oprogramowania typu „spyware”, „adware”, „keylogger”, „dialer”, „trojan” w kwarantannie.</li> <li>16. Ochrona pliku 'hosts' przed niepożądanymi wpisami.</li> <li>17. Mechanizm centralnego zarządzania elementami kwarantanny znajdującymi się na stacjach klienckich.</li> <li>18. Mechanizm określania źródeł ataków prowadzonych przy użyciu zagrożeń hybrydowych, takich jak Code Red i Nimda.</li> <li>19. Obsługa plików skompresowanych obejmująca najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2</li> <li>20. Automatyczne usuwanie wirusów oraz oprogramowania typu malware i zgłaszanie alertów w przypadku wykrycia wirusa.</li> <li>21. Logowanie historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów z poziomu GUI aplikacji.</li> <li>22. Automatyczne uruchamianie procedur naprawczych.</li> <li>23. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.</li> <li>24. Średni czas reakcji producenta na nowy wirus poniżej 8 godzin, 24 godziny na dobę przez cały rok (24/7/365).</li> <li>25. Automatyczne powiadomienie użytkowników oraz administratora o wykrytych zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona.</li> <li>26. Skanowanie przez program na komputerze klienckim, danych pobieranych i wysyłanych danych przy pomocy protokołu http.</li> <li>27. Blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.</li> <li>28. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla</li> </ol>
--	--	---



		<p>witryn określonych, jako zaufane przez serwery reputacyjne producenta.</p> <p>29. Automatyczna kwarantanna blokująca ruch przychodzący i wychodzący, włączająca się w momencie, gdy stacja robocza posiada stare sygnatury antywirusowe.</p> <p>30. Wsparcie dla technologii Microsoft Network Access Protection (NAP).</p> <p>31. Ochrona podczas przeglądania sieci Internet na podstawie badania reputacji – moduł działający na bazie Network Interceptor Framework (niezależnie od rodzaju i wersji przeglądarki).</p> <p>32. Możliwość ręcznego aktualizowania baz definicji wirusów poprzez odrębny plik wykonywalny dostarczony przez producenta.</p> <p>33. Ochrona rejestrów systemowych, w tym odpowiedzialnych za konfigurację przeglądarki Internet Explorer, listę uruchamianych aplikacji przy starcie, przypisania rozszerzeń plików do zadanych aplikacji.</p> <p>34. Kontrola oraz możliwość blokowania aplikacji próbujących uzyskać połączenie z Internetem lub siecią lokalną.</p> <p>35. Osobista zaporę ogniową (tzw. personal firewall) z możliwością definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup roboczych.</p> <p>36. Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.</p> <p>37. Możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej)</p> <p>38. Użytkownik podczas próby przejścia na witrynę znajdująca się w zablokowanej przez Administratora kategorii musi zostać powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej.</p> <p>39. Możliwość blokowania witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS.</p> <p>40. Możliwość blokowania zapytań DNS do witryn sklasyfikowanych, jako niebezpieczne lub podejrzane.</p>
--	--	---



Fundusze  
Europejskie



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



cupt  
CENTRUM UNIJNYCH  
PROJEKTÓW TRANSPORTOWYCH

		<ol style="list-style-type: none"> <li>41. Możliwość zezwolenia na zapytania DNS tylko do witryn sklasyfikowanych, jako zaufane.</li> <li>42. Brak konieczności restartu komputera po zainstalowaniu aplikacji w środowisku Windows 7/8/8.1, 10, 11.</li> <li>43. Możliwość automatycznego odinstalowania innego oprogramowania AV.</li> <li>44. Moduł kontroli urządzeń zapewniający możliwość zezwolenia lub zablokowania dostępu do urządzeń zewnętrznych (np. napędy USB, urządzenia bluetooth, czytniki kart pamięci, napędy CD/DVD, stacje dyskiety).</li> <li>45. Moduł kontroli urządzeń zarządzany z poziomu konsoli centralnego zarządzania.</li> <li>46. Moduł kontroli urządzeń umożliwia dodanie 'zaufanego urządzenia' poprzez podanie jego identyfikatora sprzętu.</li> <li>47. Blokowanie aktywności sieciowej związanej ze znanymi botnetami włączając w to ataki ransomware i ataki ukierunkowane</li> </ol>
--	--	--

7. Licencja na oprogramowanie antywirusowe na urządzenia mobilne - 32 szt.

L.p.	Nazwa Oprogramowania	Opis wymagań technicznych
1	F-Secure Elements EPP for Mobiles lub równoważne	<ol style="list-style-type: none"> <li>1. Dostarczone licencje muszą być w pełni kompatybilne z posiadanym przez Zamawiającego systemem F-Secure Protection Service for Business. Możliwość wdrożenia oraz aktualizacji i usuwania oprogramowania za pośrednictwem rozwiązania MDM VMware Workspace One Advanced.</li> <li>2. Licencje muszą zapewniać ochronę i wsparcie dla urządzeń mobilnych z systemami operacyjnymi: <ul style="list-style-type: none"> <li>· Android (min. w wersji 8.x i wyższych),</li> </ul> </li> <li>3. Możliwość centralnego zarządzania chronionymi urządzeniami mobilnymi, z opcją zmiany zasad bezpieczeństwa.</li> <li>4. Możliwość monitorowania stanu zabezpieczeń chronionych urządzeń, w tym dostęp do szczegółowych informacji takich jak numer telefonu czy wersja systemu operacyjnego.</li> <li>5. Możliwość automatycznego szyfrowania ruchu sieciowego podczas korzystania z publicznych sieci Wi-Fi i sieci komórkowych.</li> <li>6. Możliwość ukrycia lub zmiany wirtualnej lokalizacji urządzenia.</li> <li>7. Możliwość anonimowego połączenia internetowego przez ukrycie adresu IP urządzenia.</li> <li>8. Możliwość blokowania reklam internetowych.</li> </ol>



Fundusze  
Europejskie



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



cupt  
CENTRUM UNIJNYCH  
PROJEKTÓW TRANSPORTOWYCH

		<p>9. Możliwość chmurowej analizy zagrożeń pojawiających się na urządzeniach np. z wykorzystaniem algorytmów Big Data.</p> <p>10. Funkcja sprawdzania reputacji plików i aplikacji w czasie rzeczywistym.</p> <p>11. Funkcje ochrony przed przeglądaniem złośliwych witryn internetowych.</p> <p>12. Licencja powinna zapewniać wysoki poziom ochrony przeglądania niezależnie od rodzaju przeglądarki internetowej.</p> <p>13. Licencja powinna zapewniać ochronę przed śledzeniem użytkownika (ochrona przed zbieraniem informacji o wyszukiwanych hasłach, odwiedzanych stronach i klikniętych banerach, ochrona przed zbieraniem informacji o lokalizacji geograficznej, ochrona przed zbieraniem informacji przez pliki cookie, skrypty lub śledzenie pikseli).</p> <p>14. Możliwość zmniejszenia zużycia transferu danych dzięki blokowaniu zbędnego ruchu sieciowego, takiego jak reklamy oraz metody śledzenia użytkownika.</p> <p>16. Możliwość wdrożenia, w przypadku systemu Android, programu klienckiego za pomocą Google Play lub instalację pakietu APK.</p> <p>17. Możliwość wdrożenia, w przypadku systemu iOS, programu klienckiego za pomocą Apple App Store.</p> <p>18. Interfejs użytkownika w języku polskim.</p>
--	--	---

#### 8. Subskrypcja i wsparcie techniczne dla licencji

1. Wymagany okres subskrypcji i wsparcia technicznego dla licencji z pozycji 1-5 OPZ wynosi 36 miesięcy od dnia 12 kwietnia 2025r.. Wymagany okres subskrypcji i wsparcia technicznego dla licencji dostarczonych w ramach prawa opcji z pozycji 6-7 OPZ obowiązuje od daty udzielenia licencji do upływu ważności licencji, który nastąpi wraz z upływem ważności licencji nabytych w ramach zamówienia podstawowego.
2. Prawo do subskrypcji i usługa wsparcia technicznego, o którym mowa powyżej obejmuje:
  - a) prawo do otrzymywania aktualnych wersji Oprogramowania oraz publikowanych poprawek,
  - b) prawo do otrzymywania aktualizacji bazy sygnatur antywirusowych on-line w trybie 24 godziny na dobę przez 7 dni w tygodniu,
  - c) udzielanie niezwłocznie konsultacji i wyjaśnień telefonicznie lub drogą poczty elektronicznej w dni robocze,
  - d) internetowy dostęp do dokumentacji i bazy wiedzy oraz zdalne wsparcie, w trybie nie mniej niż 8 godzin na dobę od poniedziałku do piątku w godzinach 8.15 -16.15



Fundusze  
Europejskie



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



cupt  
CENTRUM UNIJNYCH  
PROJEKTÓW TRANSPORTOWYCH

3. W przypadku realizacji usługi wsparcia technicznego poprzez zdalny dostęp, sesja zdalna musi odbywać się za pomocą posiadanego przez Zamawiającego systemu klasy PAM (ang. Privileged Access Management), umożliwiającemu m.in. nagrywanie sesji.

#### 9. Instruktaż dla administratorów Zamawiającego

- Wykonawca przeprowadzi instruktaż omawiający wszystkie komponenty, który będzie dotyczył konfiguracji oraz administracji dostarczonego oprogramowania dla administratorów Zamawiającego.
- Instruktaż poprowadzi pracownik Wykonawcy, który brał aktywny udział w projekcie wdrożeniowym.
- Instruktaż odbędzie się w postaci spotkań online.
- o terminie realizacji Instruktażu Wykonawca poinformuje Zamawiającego z co najmniej siedmiodniowym wyprzedzeniem.
- Wykonawca zapewni uczestnikom odpowiednie materiały szkoleniowe w formie elektronicznej.
- Program Instruktażu powinien obejmować zagadnienia związane z czynnościami konfiguracyjnymi i administracyjnymi wdrożonego systemu.
- Instruktaż musi być przeprowadzony w języku polskim.
- W instruktażu będzie uczestniczyć maksymalnie 7 osób

W przypadku zaoferowania licencji równoważnych, wykonawca jest zobowiązany:

1. Do wdrożenia w środowisku informatycznym (serwery, stacje robocze, urządzenia mobilne w ilości określonej licencji) zaoferowanego rozwiązania (instalacja, konfiguracja)
2. Przygotowanie dokumentacji powdrożeniowej:

Wykonawca zapewni i dostarczy w formacie DOC/DOCX dokumentację powykonawczą, która będzie:

- Sporządzona w języku polskim;
- Zawierać nazwę dokumentu;
- Zawierać metrykę dokumentu (data, numer wersji, historia zmian, autor);
- Zawierać spis treści;
- Zawierać słownik pojęć;
- Zawartość merytoryczna.