

Znak sprawy OA.243.5.2017.JS

OPIS PRZEDMIOTU ZAMÓWIENIA**1. PRZEDŁUŻENIE SUBSKRYPCJI I WSPARCIA TECHNICZNEGO OPROGRAMOWANIA ANTYWIRUSOWEGO (70 SZT.)****WYMAGANIA MINIMALNE**

Zamawiający wymaga dostarczenia przedłużenia wsparcia technicznego, subskrypcji dla wykorzystywanego oprogramowania antywirusowego F-Secure Client Security o okres 12 miesięcy. Zamawiający wymaga przeprowadzenia aktualizacji posiadanego oprogramowania do najnowszej stabilnej wersji udostępnianej przez producenta oprogramowania.

Lp.	Opis/charakterystyka produktu	Ilość
1.	F-Secure Client Security	70
2.	F-Secure Policy Menager Console	1

Program antywirusowy	Program antywirusowy
Ilość	70 licencji + konsola administracyjna
Okres	Licencje mają obejmować okres 12 miesięcy licząc od daty aktywacji licencji przez Zamawiającego, z darmowymi aktualizacjami online przez cały okres ważności licencji
Istotne cechy oprogramowania	ochrona antywirusowa stacji roboczych (Windows 10 32-bit i 64-bit, Windows 8 32-bit i 64-bit, Windows 7 32-bit i 64-bit, Windows Vista 32-bit i 64-bit, Windows XP Home Edition z SP1/SP2/SP3, Windows XP Professional Edition z SP1/SP2/SP3, Windows XP Media Center Edition z SP1) ochrona antywirusowa wyżej wymienionego systemu monitorowana i zarządzana z pojedynczej, centralnej konsoli możliwość instalacji konsoli zarządzania niezależnie na kilku wybranych stacjach. polski interfejs użytkownika i dokumentacja do oprogramowania na stację roboczą

<p>Zastosowane technologie</p>	<ol style="list-style-type: none"> 1. 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. 2. Co najmniej trzy różne silniki antywirusowe, funkcjonujące jednocześnie i skanujące wszystkie dane. 3. Oddzielny silnik skanujący do wykrywania niepożądanych aplikacji takich jak oprogramowanie typu „spyware”, „adware”, „keylogger”, „dialer”, „trojan”. 4. 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. 5. 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. 6. Możliwość wywołania skanowania komputera w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera. 7. Możliwość wywołania skanowania podczas uruchamiania systemu operacyjnego lub po zalogowaniu użytkownika. 8. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie. 9. 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). 10. Możliwość pobierania aktualizacji definicji wirusów bezpośrednio z serwerów producenta, centralnej konsoli, dedykowanego proxy lub z innej stacji roboczej gdzie zainstalowane jest oprogramowanie antywirusowe. 11. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów. 12. Heurystyczna technologia do wykrywania nowych, nieznanych wirusów. 13. Wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware”, „adware”, „keylogger”, „dialer”, „trojan”, „rootkit”. 14. Możliwość umieszczenia oprogramowania typu „spyware”, „adware”, „keylogger”, „dialer”, „trojan” w kwarantannie. 15. Ochrona pliku ‘hosts’ przed niepożądanymi wpisami. 16. Mechanizm centralnego zarządzania elementami kwarantanny znajdującymi się na stacjach klienckich. 17. 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. 18. Mechanizm określania źródeł ataków prowadzonych przy użyciu zagrożeń hybrydowych, takich jak Code Red i Nimda.
--------------------------------	--

19. Obsługa plików skompresowanych obejmująca najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX.
20. Automatyczne usuwanie wirusów oraz oprogramowania typu malware i zgłaszanie alertów w przypadku wykrycia wirusa.
21. Logowanie historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów z poziomu GUI aplikacji.
22. Automatyczne uruchamianie procedur naprawczych.
23. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
24. Średni czas reakcji producenta na nowy wirus poniżej 8 godzin, 24 godziny na dobę przez cały rok (24/7/365).
25. Automatyczne powiadomienie użytkowników oraz administratora o wykrytych zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona.
26. Skanowanie przez program na komputerze klienckim przychodzącej i wychodzącej poczty elektronicznej bez konieczności instalowania dodatkowych programów/modułów.
27. Możliwość zablokowania wychodzącej wiadomości e-mail, jeżeli zostanie w niej wykryty zainfekowany załącznik.
28. Skanowanie przez program na komputerze klienckim, danych pobieranych i wysyłanych danych przy pomocy protokołu http.
29. Blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.
30. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez serwery reputacyjne producenta.
31. Automatyczna kwarantanna blokująca ruch przychodzący i wychodzący, włączająca się w momencie, gdy stacja robocza posiada stare sygnatury antywirusowe.
32. Wsparcie dla technologii Microsoft Network Access Protection (NAP).
33. Ochrona przeglądarki internetowej, w tym: blokowanie wyskakujących okienek, blokowanie ciasteczek (cookies), blokowanie możliwości zmian ustawień w IE, analiza uruchamianych skryptów ActiveX i pobieranych plików.
34. Ochrona podczas przeglądania sieci Internet na podstawie badania reputacji – moduł działający na bazie *Network Interceptor Framework* (niezależnie od rodzaju i wersji przeglądarki).
35. Możliwość zabezpieczenia połączenia do witryn skategoryzowanych przez producenta, jako 'bankowość elektroniczna' poprzez uniemożliwienie nawiązania nowych sesji do niezauważanych hostów na czas połączenia z bankiem.
36. Kontrola połączenia umożliwia zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora poprzez uniemożliwienie nawiązania nowych sesji do niezauważanych hostów na czas połączenia z daną witryną HTTPS.
37. Możliwość ręcznego aktualizowania baz definicji wirusów poprzez odrębny plik wykonywalny dostarczony przez

producenta.

38. Ochrona rejestrów systemowych, w tym odpowiedzialnych za konfigurację przeglądarki Internet Explorer, listę uruchamianych aplikacji przy starcie, przypisania rozszerzeń plików do zadanych aplikacji.

39. Kontrola oraz możliwość blokowania aplikacji próbujących uzyskać połączenie z Internetem lub siecią lokalną.

40. Osobista zaporę ogniową (tzw. personal firewall) z możliwością definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup roboczych.

41. Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.

42. Możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej)

43. Blokowanie dostępu do witryn WWW na podstawie dostarczonych przez producenta kategorii bez konieczności ręcznego wpisywania poszczególnych adresów.

44. 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.

45. Możliwość blokowania witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS.

46. Brak konieczności restartu komputera po zainstalowaniu aplikacji w środowisku Windows Vista/7/8/8.1

47. 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).

48. Moduł kontroli urządzeń zarządzany z poziomu konsoli centralnego zarządzania.

49. Moduł kontroli urządzeń umożliwia dodanie 'zaufanego urządzenia' poprzez podanie jego identyfikatora sprzętowego.

50. Moduł aktualizatora aplikacji, który okresowo skanuje i umożliwia aktualizację do najnowszych wersji aplikacji firm trzecich.

51. Aktualizator aplikacji powinien spełniać rolę programu łatającego podatności a nie tylko i wyłącznie pasywnego skanera luk w bezpieczeństwie aplikacji.

52. Administrator ma możliwość wykluczenia aplikacji, które mają nie podlegać aktualizacji poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej.

53. System raportowania powinien pokazywać status podatności aplikacji na komputerach dotyczące całej domeny lub pojedynczych komputerów.

54. Aktualizator aplikacji nie może wymagać instalowania dodatkowych agentów oprócz agenta AV.

55. Aktualizator powinien dać możliwość aktualizacji poprawek w sposób akcji wymuszonej lub reguły wykonującej się w sposób zaplanowany: dzień, godzina, opcje restartu komputera, wykluczenia aplikacji.

56. Administrator konsoli zarządzającej powinien mieć możliwość zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z

	<p>przekierowaniem na strony producenta aplikacji. 57. Aktualizator aplikacji nie wymaga uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces</p>
Zarządzanie	<ol style="list-style-type: none"> 1. System centralnego zarządzania może być zainstalowany na wersjach serwerowych Microsoft Windows oraz Linux. 2. Instalacja sytemu centralnego zarządzania dla Microsoft Windows musi wspierać następujące wersje systemów operacyjnych: <ul style="list-style-type: none"> - Windows Server 2003 SP1 32-bit: Standard, Enterprise, Web Edition, Small Business Server - Windows Server 2003 SP1 64-bit: Standard, Enterprise - Windows Server 2008 SP1 32-bit : Standard, Enterprise, Web Server - Windows Server 2008 SP1 64-bit: Standard, Enterprise, Web Server, Small Business Server, Essential Business Server - Windows Server 2008 R2: Standard, Enterprise, Web Server - Windows Server 2012: Essentials, Standard, Datacenter - Windows Server 2012 R2: Essentials, Standard, Datacenter 3. Instalacja sytemu centralnego zarządzania dla Linux musi wspierać następujące wersje systemów operacyjnych: <ul style="list-style-type: none"> - Red Hat Enterprise Linux 5 32/64-bit - Red Hat Enterprise Linux 6 32/64-bit - CentOS 6 32/64-bit - SuSE Linux Enterprise Server 10 32/64-bit - SuSE Linux Enterprise Server 11 32/64-bit - SuSE Linux Enterprise Desktop 11 32/64-bit - openSUSE 12 32/64-bit - Debian GNU Linux 6.0 (Squeeze) 32/64-bit - Debian GNU Linux 7.2 (Wheezy) 32/64-bit - Ubuntu 10.04 (Lucid Lynx) 32/64-bit - Ubuntu 12.04 (Precise Pangolin) 32/64-bit - Ubuntu 14.04 (Trusty Tahr) 32/64-bit 4. Konsola zarządzania umożliwia eksport pakietu instalacyjnego dla klienta w formacie Microsoft Installer (MSI) i JAR lub też bezpośrednią instalację zdalną nienadzorowaną. 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. 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). 7. Komunikacja pomiędzy serwerem centralnego zarządzania a stacjami roboczymi musi być zaszyfrowana lub sygnowana stosownymi kluczami prywatnymi i publicznymi. 8. Pełne centralne zarządzanie dla środowisk Windows Server 2003 (32-bit oraz 64-bit), Windows Server 2008 (32-bit oraz 64-bit), Windows Server 2008 R2, Windows Server 2012, Windows XP, Windows Vista, Windows 7, Windows 8,

Windows 8.1, Linux.

9. Scentralizowane blokowanie i odblokowywanie dostępu użytkownika do zmian konfiguracyjnych oprogramowania klienckiego, konsola pozwala na zdalne zarządzanie wszystkimi ustawieniami klienta.

10. Administratorzy muszą mieć możliwość tworzenia logicznych grup klientów i serwerów, w celu zarządzania oraz wymuszania określonych dla grupy zasad bezpieczeństwa.

11. Centralna konsola administracyjna musi umożliwiać przenoszenie klientów z jednej grupy do drugiej z możliwością zachowania ustawień lub dziedziczenia ustawień grupy.

12. Możliwość zmiany ustawień dla poszczególnych grup, umożliwienie administratorom zarządzania poszczególnymi klientami i funkcjonalnymi grupami klientów (tworzenie grup klientów).

13. Tworzenie grup, zdalne instalowanie oprogramowania oraz wymuszanie stosowania określonych zasad i ustawień na klientach.

14. Możliwość importu struktury drzewa z Microsoft Active Directory.

15. Możliwość blokowania wszystkich ustawień konfiguracyjnych stacji roboczych w celu uniemożliwienia ich modyfikacji przez użytkowników.

16. Możliwość definiowania harmonogramów lub częstotliwości automatycznego pobierania aktualizacji definicji wirusów od producenta oprogramowania przez serwer zarządzający.

17. 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.

18. Możliwość ustalenia dodatkowego harmonogramu pobierania przez serwery plików i stacje robocze aktualizacji z serwera producenta.

19. Funkcja przechowywania i przekazywania danych umożliwiająca przechowywanie przez klientów danych dotyczących zdarzeń, w sytuacji, jeśli nie mogą oni uzyskać połączenia z serwerem zarządzania.

20. Dane muszą być przesyłane do serwera zarządzania podczas kolejnego połączenia.

21. Możliwość włączania/wyłączania wyświetlania komunikatów o znalezionych wirusach na wybranych stacjach klienckich.

22. Umożliwienie administratorom na audyt sieci, polegający na wykryciu niechronionych węzłów narażonych na ataki wirusowe.

23. Automatyczne wykrywanie i usuwanie oprogramowanie innych wiodących producentów systemów antywirusowych (min. 3 inne) podczas instalacji.

24. Automatyczne uaktualnianie bazy definicji wirusów oraz mechanizmów skanujących nie rzadziej, niż co 7 dni (zalecane codzienne aktualizacje).

25. Automatyczne pobieranie przez program antywirusowy klienta zaktualizowanych definicji wirusów, jeśli aktualnie przechowywane pliki są przestarzałe.

26. Możliwość eksportu raportów z pracy systemu do pliku HTML.

	<p>27. Możliwość natychmiastowej aktualizacji przez serwer definicji wirusów na stacjach klienckich.</p> <p>28. Możliwość uruchomienia aktualizacji stacji roboczych i serwerów przez użytkowników „na żądanie”.</p> <p>29. Program musi pozwalać administratorowi na określenie reakcji w przypadku wykrycia wirusa.</p> <p>30. Program musi pozwalać na określenie obszarów skanowania, tj.: pliki, katalogi, napędy lokalne i sieciowe.</p> <p>31. Program musi pozwalać na skanowanie pojedynczych plików przez dodanie odpowiedniej opcji do menu kontekstowego (po kliknięciu prawym przyciskiem myszy).</p> <p>32. Program musi pozwalać na określenie typów skanowanych plików, momentu ich skanowania (otwarcie, modyfikacja) oraz na wykluczenie ze skanowania określonych folderów.</p> <p>33. Dedykowany system raportowania dostępny przez przeglądarkę internetową umożliwiający podgląd statystyk dotyczących wykrytych wirusów, przeprowadzonych ataków, zainstalowanego oprogramowania oraz statystyk połączenia stacji klienckich.</p> <p>34. System raportowania umożliwiający wysyłanie raportów poprzez pocztę elektroniczną zgodnie z harmonogramem określonym przez administratora.</p> <p>35. 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>36. Możliwość przekierowania alertów bezpośrednio do serwera Syslog.</p> <p>37. Możliwość tworzenia wielu kont dostępu do systemu centralnego zarządzania dla różnych użytkowników (w tym możliwość nadania danemu użytkownikowi ograniczonych praw).</p> <p>38. System umożliwiający wykonanie pełnej kopii bazy danych systemu zarządzania centralnego bez konieczności ręcznego wyłączenia programu.</p> <p>39. Pełna kopia bazy danych systemu zarządzania centralnego może być wykonywana automatycznie zgodnie z harmonogramem określonym przez administratora.</p> <p>40. Administrator ma możliwość określenia liczby kopii bazy danych, jaka będzie przetrzymywana.</p>
--	---

Cena dodatkowo powinna zawierać:

- koszt instalacji aktualizacji oprogramowania w siedzibie zamawiającego (konsola administratora + 70 komputerów Windows XP/Vista/Win7/Win10)
- opieka techniczna w okresie trwania licencji,
- szkolenie w języku polskim na w zakresie podstawowej obsługi programu w siedzibie klienta z zakresu obsługi i konfiguracji systemu w siedzibie klienta
- koszt dostawy do siedziby Zamawiającego.

Dopuszcza się stosowanie produktów równoważnych. W przypadku gdy Wykonawca oferuje produkt równoważny, musi przedłożyć informację o tym produkcie. Za równoważne zostaną uznane rozwiązania o parametrach nie gorszych niż wyżej określone.

2. PRZEDŁUŻENIE SUBSKRYPCJI I WSPARCIA TECHNICZNEGO URZĄDZEŃ FORTINET [1 SZT.]

WYMAGANIA MINIMALNE

Zamawiający wymaga dostarczenia przedłużenia wsparcia technicznego, subskrypcji dla wykorzystywanych urządzeń Fortinet o okres 12 miesięcy. Zamawiający wymaga przeprowadzenia aktualizacji posiadanych urządzeń do najnowszej stabilnej wersji udostępnianej przez producenta urządzenia.

Lp.	Opis/charakterystyka produktu	Nr seryjny	Ilość
1.	FortiGate	FG100D3G16824085	1
2.	FortiAnalyzer	FL200D3A16000742	1
3.	FortiMail	FE200E3A16000298	1

Cena dodatkowo powinna zawierać:

- aktualizacja i konfiguracja urządzenia w siedzibie klienta
- opieka techniczna w okresie trwania subskrypcji,
- serwis logistyczny na terenie Polski z dostawą urządzenia zastępczego na drugi dzień roboczy od chwili zgłoszenia awarii – 7x24;
- szkolenie w języku polskim w zakresie podstawowej konfiguracji i obsługi urządzeń w siedzibie klienta
- koszt dostawy do siedziby Zamawiającego.