Nr postępowania: ZO/KŁ/4/2022

Pruszków, dn. 01.02.2022 r.

ZAPYTANIE OFERTOWE

w ramach zakupu dostaw, usług lub robót budowlanych
których wartość nie przekracza kwoty 130.000,00 zł

1. **Zamawiający: Mazowieckie Specjalistyczne Centrum Zdrowia im. prof. Jana Mazurkiewicza w Pruszkowie** zaprasza do złożenia oferty na:**Przedmiot zamówienia: Przedłużenie obecnie posiadanych licencji oprogramowania antywirusowego ESET, na okres 24 m-cy.**
3. **Krótki opis przedmiotu zamówienia:** Przedłużenie obecnie posiadanych licencji oprogramowania antywirusowego ESET. Zamówienie dotyczy 350 licencji, które pozwalają na aktualizację oprogramowania do najnowszej wersji oraz utrzymują ciągłość ochrony przed wirusami. Szczegółowy opis przedmiotu zamówienia stanowi Załącznik nr 2 do niniejszego postępowania.
4. **Termin realizacji zamówienia:** 24 m-ce od dnia zawarcia umowy.
5. **Miejsce lub sposób uzyskania informacji dotyczących przedmiotu zamówienia:** W niniejszym postępowaniu o udzielenie zamówienia oświadczenia, wnioski, zawiadomienia oraz informacje Zamawiający i Wykonawcy przekazują drogą elektroniczną. Adres poczty elektronicznej Zamawiającego: zp@mscz.pl.

   Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści Zapytania Ofertowego wraz z załącznikami. Zamawiający jest zobowiązany udzielić wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przed upływem terminu składania ofert – pod warunkiem, że wniosek o wyjaśnienie treści Zapytania Ofertowego wpłynął do Zamawiającego nie później niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert. Jeśli wniosek o wyjaśnienie treści Zapytania Ofertowego wpłynął po terminie składania wniosku albo dotyczy udzielonych wyjaśnień, Zamawiający może udzielić wyjaśnień albo pozostawić wniosek bez rozpoznania. Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosku o wyjaśnienie.

   Osoby do kontaktu: Karol Łosin – GŁ. Specjalista w Zespole Obsługi Informatycznej,
   tel. 22/ 739 12 63, e-mail: karol.losin@mscz.pl
6. **Kryteria oceny ofert: Cena /koszt/ – 100%**
7. **Oferta musi zawierać:**

   a) wypełniony Formularz oferty – Załącznik nr 1 do Zapytania Ofertowego;

   b) zaakceptowany oraz parafowany Opis Przedmiotu Zamówienia – Załącznik 2 do Zapytania Ofertowego;

   c) odpis z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej.
8. Sposób przygotowania oferty: ofertę z podaniem ceny w PLN (z VAT) należy sporządzić w języku polskim, w następujący sposób: nazwa i adres Zamawiającego, nazwa i adres Wykonawcy, z adnotacją ***„Zapytanie Ofertowe – nr postępowania ZO/KŁ/4/2022”***.
9. Miejsce i termin złożenia ofert: ***ofertę należy złożyć do dnia 08.02.2022 r. do godziny 10:00***:
   - pisemnie na adres: Mazowieckie Specjalistyczne Centrum Zdrowia im. prof. Jana Mazurkiewicza, 05-802 Pruszków, ul. Partyzantów 2/4, Kancelaria (budynek Dyrekcji, parter, hol główny);
   - drogą elektroniczną na adres e-mail: zp@mscz.pl

DYREKTOR

.....

Podpis Dyrektora

..... dn. ..... r.

Zamawiający:
Mazowieckie Specjalistyczne Centrum Zdrowia
im. prof. Jana Mazurkiewicza w Pruszkowie
ul. Partyzantów 2/4
05-802 Pruszków

FORMULARZ OFERTY

Ja (my),

_____

Imiona i nazwiska osób reprezentujących Wykonawcę

działając w imieniu i na rzecz Wykonawcy:

Rodzaj informacji	**Dane Wykonawcy**
Pełna nazwa firmy lub imię i nazwisko Wykonawcy	
REGON	
NIP	
Adres siedziby Wykonawcy nr telefonu adres e-mail	

1. Odpowiadając na ogłoszenie o zamówieniu publicznym w postępowaniu prowadzonym w trybie Zapytania Ofertowego, którego przedmiotem jest **przedłużenie obecnie posiadanych licencji oprogramowania antywirusowego ESET, na okres 24 m-cy**, oświadczamy, że oferujemy spełnienie przedmiotu zamówienia zgodnie z warunkami i postanowieniami zawartymi w Zapytaniu Ofertowym wraz ze wszystkimi załącznikami, *za **całkowitą cenę brutto (z podatkiem VAT):***
   ……
   (słownie: ……)

   *w tym: **wartość netto:** ……zł*

   podatek VAT (……%): ……*zł*
2. **Termin realizacji zamówienia: 24 miesiące od dnia zawarcia umowy.**
3. Oświadczamy, że w cenie oferty zostały uwzględnione wszystkie koszty wykonania zamówienia i realizacji przyszłego świadczenia umownego.
4. Zapoznaliśmy się z warunkami umowy i nie wnosimy w stosunku do niej żadnych uwag, a w przypadku wyboru naszej oferty podpiszemy umowę na warunkach w niej zawartych, w miejscu oraz terminie wskazanym przez Zamawiającego.

5. Oświadczamy, że wypełniliśmy obowiązki informacyjne, przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskaliśmy w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postepowaniu.

6. Wszelką korespondencję w sprawie niniejszego postępowania należy kierować na adres:

.....

osoba do kontaktu: .....

e-mail: .....tel. .....

7. Informacje do zawarcia umowy, w przypadku dokonania wyboru naszej oferty:

osoba upoważniona do podpisania umowy: .....

osoba upoważniona do kontaktów z Zamawiającym, w sprawach dotyczących realizacji umowy:

.....

e-mail: .....tel. .....

(podpis Wykonawcy lub upoważnionego przedstawiciela)

1. Administratorem danych osobowych jest Mazowieckie Specjalistyczne Centrum Zdrowia im. prof. Jana Mazurkiewicza w Pruszkowie, adres: ul. Partyzantów 2/4, 05-802 Pruszków.

2. Pana/Pani dane osobowe przetwarzane będą w trybie art. 6 ust. 1 lit. b (przetwarzanie jest niezbędne do realizacji zamówienia publicznego) Rozporządzenia 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. U. UE. L. 2016.119.1 z dnia 4 maja 2016 r.

3. Z pełną Informacją Administratora dotyczącą przetwarzania danych osobowych w celu realizacji zamówienia publicznego, można zapoznać się w siedzibie administratora.

OPIS PRZEDMIOTU ZAMÓWIENIA

Cel zamówienia: zapewnienie bezpieczeństwa oprogramowania i danych na stacjach roboczych i serwerach w sieci komputerowej Mazowieckiego Specjalistycznego Centrum Zdrowia im. prof. Jana Mazurkiewicza w Pruszkowie, zwanego dalej Zamawiającym.

Realizacja zamówienia/miejsce dostawy: ul. Partyzantów 2/4, 05-802 Pruszków

Przedmiotem zamówienia jest:

odnowienie Licencji dla 350 stacji roboczych, urządzeń mobilnych, w tym dla minimum 35 serwerów na oprogramowanie antywirusowe **ESET PROTECT Entry ON-PREM**, na okres 24 miesięcy.

Obecnie Zamawiający posiada oprogramowanie antywirusowe **ESET PROTECT Entry ON-PREM** 350 licencji. Zamawiający dopuszcza możliwość zaoferowania produktów równoważnych w zakresie nowych licencji na oprogramowanie antywirusowe (oprogramowanie równoważne).

Oprogramowanie antywirusowe musi zapewniać poniższe funkcje:

I. ESET PROTECT Entry ON-PREM:

1. Pełne wsparcie dla systemów Windows7/ Windows8/ Windows 8.1/Windows 10 dla 32- i 64-bitowej wersji systemu.
2. Wersja programu dostępna zarówno w języku polskim, jak i angielskim.
3. Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim.

Ochrona antywirusowa i antyspyware:

1. Ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor itp.
3. Wbudowana technologia do ochrony przed rootkitami.
4. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
6. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików „na żądanie" lub według harmonogramu.
7. System ma oferować administratorowi możliwość definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało, czy komputer pracuje na zasilaniu bateryjnym i jeśli tak - nie wykonywało danego zadania.
8. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu. Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
9. Skanowanie „na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
10. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie" i według harmonogramu.
11. Możliwość skanowania dysków sieciowych i dysków przenośnych.
12. Skanowanie plików spakowanych i skompresowanych.
13. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
14. Wykluczenie ze skanowania musi odbywać się nie tylko po nazwie pliku, ale również ma być możliwe użycie symbolu wieloznacznego „*" zastępującego dowolne znaki w ścieżce.
15. Administrator ma możliwość dodania wykluczenia po tzw. HASH'u zagrożenia, wskazującego bezpośrednio na określoną infekcję, a nie konkretny plik.
16. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
17. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.

18. Możliwość tymczasowego wyłączenia ochrony na określony czas lub do ponownego uruchomienia komputera.
19. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
20. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
21. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli.
22. 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).
23. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
24. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
25. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie.
26. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
27. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
28. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji, takich jak przeglądarki Web lub programy pocztowe.
29. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta.
30. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
31. Program musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
32. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym.
33. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
34. 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.
35. Wbudowane dwa niezależne moduły heurystyczne - jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie - z użyciem jednej i/lub obu metod jednocześnie.
36. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie oraz, czy próbki zagrożeń mają być wysyłane w pełni automatycznie, czy też po dodatkowym potwierdzeniu przez użytkownika.
37. Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika.
38. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
39. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
40. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
41. Możliwość zabezpieczenia konfiguracji programu hasłem w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła.

42. 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.
43. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.
44. 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. Program musi umożliwiać dezaktywację tego mechanizmu.
45. 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 wirusów.
46. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
47. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.
48. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
49. Użytkownik ma posiadać możliwość takiej konfiguracji programu, aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika.
50. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście.
51. Moduł zapobiegania włamaniom 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 tworzonych 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.
52. Tworzenie reguł dla modułu zapobiegania włamaniom musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
53. Użytkownik na etapie tworzenia reguł dla modułu zapobiegania włamaniom musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
54. Oprogramowanie musi posiadać zaawansowany skaner pamięci.
55. Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach, np. czytnikach PDF, aplikacjach JAVA itp.
56. 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 procesach i połączeniach.
57. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa.
58. Program ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.
59. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.
60. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami.
61. Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji program zgłosi posiadanie nieaktualnej bazy sygnatur.
62. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji.
63. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http

64. Program musi być wyposażony w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback).
65. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa).
66. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym.
67. W momencie wykrycia trybu pełnoekranowego aplikacja ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań aplikacji.
68. Użytkownik ma mieć możliwość skonfigurowania programu tak, aby automatycznie program włączał powiadomienia oraz zadania pomimo pracy w trybie pełnoekranowym po określonym przez użytkownika czasie.
69. 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.
70. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego przez producenta programu.
71. Program musi posiadać możliwość utworzenia z poziomu interfejsu aplikacji dziennika diagnostycznego na potrzeby pomocy technicznej.
72. Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline.
73. Możliwość podejrzenia licencji, za pomocą której program został aktywowany.
74. W trakcie instalacji program ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór co najmniej następujących modułów do instalacji: ochrona antywirusowa i antyspyware, kontrola dostępu do urządzeń, zapora osobista, ochrona poczty, ochrona protokołów.
75. W programie musi istnieć możliwość tymczasowego wstrzymania polityk wysłanych z poziomu serwera zdalnej administracji.
76. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej.
77. Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas, po którym automatycznie zostają przywrócone dotychczasowe ustawienia.
78. Administrator ma możliwość wstrzymania polityk na wskazany przez Administratora okres czasu, np. 10 min., 30 min., 1 godzinę, 4 godziny.
79. Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika.
80. Program musi posiadać opcję automatycznego skanowania komputera po dokonaniu zmian z użyciem opcji wstrzymania polityki.
81. Aplikacja musi posiadać funkcję ręcznej aktualizacji komponentów programu.
82. 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.
83. Program musi posiadać możliwość definiowania stanów aplikacji, jakie będą wyświetlane użytkownikowi, np. powiadomień o wyłączonych mechanizmach ochrony czy stanie licencji.
84. Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie.

Zapora osobista (personal firewall)

1. Zapora osobista ma pracować jednym z 4 trybów:
   a) tryb automatyczny - program blokuje cały ruch przychodzący i zezwala tylko na znane, bezpieczne połączenia wychodzące, jednocześnie umożliwia utworzenie dodatkowych reguł przez administratora;
   b) tryb interaktywny - program pyta się o każde nowe nawiązywane połączenie i automatycznie tworzy dla niego regułę (na stałe lub tymczasowo);

c) tryb oparty na regułach - użytkownik/administrator musi ręcznie zdefiniować reguły określające, jaki ruch jest blokowany, a jaki przepuszczany;

d) tryb uczenia się - umożliwia zdefiniowanie przez administratora określonego okresu czasu, w którym oprogramowanie samo tworzy odpowiednie reguły zapory, analizując aktywność sieciową danej stacji.

2. Program musi akceptować istniejące reguły w zaporze systemu Windows, zezwalające na ruch przychodzący.
3. Możliwość tworzenia list sieci zaufanych.
4. Możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie
5. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego.
6. Możliwość wyboru jednej z 3 akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj o decyzję.
7. Możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń.
8. Możliwość zapisywania w dzienniku zdarzeń związanych z zezwoleniem lub zablokowaniem danego typu ruchu.
9. Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer w tym minimum dla strefy zaufanej i sieci Internet.
10. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
11. Program musi umożliwiać ochronę przed przyłączeniem komputera do sieci botnet.
12. Wykrywanie zmian w aplikacjach korzystających z sieci i monitorowanie o tym zdarzeniu.
13. Program ma oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.
14. Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.
15. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci
16. Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora.
17. Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowaniu sieci bezprzewodowej lub jego braku, aktywności połączenia bezprzewodowego lub jego braku, konkretny interfejs sieciowy w systemie.
18. Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS, zarówno z wykorzystaniem adresów IPv4, jak i IPv6.
19. Opcje związane z autoryzacją stref mają oferować opcje łączenia (np. lokalny adres IP i adres serwera DNS) w dowolnej kombinacji, celem zwiększenia dokładności identyfikacji danej sieci.
20. Program musi możliwość ustalenia tymczasowej czarnej listy adresów IP, które będą blokowane podczas próby połączenia.
21. Program musi posiadać kreator, który umożliwia rozwiązać problemy z połączeniem. Musi on działać w oparciu o:
    a) rozwiązanie problemów z aplikacją lokalną, którą wskazujemy z listy;
    b) rozwiązywanie problemów z połączeniem z urządzeniem zdalnym na podstawie adresu IP.

Ochrona serwera plików Windows

1. Wsparcie dla systemów: Microsoft Windows Server 2008, 2008R2, 2012, 2012R2, 2016.
2. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor itp.
4. Wbudowana technologia do ochrony przed rootkitami i exploitami.
5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.

6. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików „na żądanie" lub według harmonogramu.
7. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu. Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
8. Skanowanie na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
9. System antywirusowy ma mieć możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie" i według harmonogramu.
10. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych.
11. Użytkownik ma mieć możliwość zmiany ilości wątków skanowania w ustawieniach systemu antywirusowego.
12. Możliwość skanowania dysków sieciowych i dysków przenośnych.
13. Skanowanie plików spakowanych i skompresowanych.
14. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
15. Program musi posiadać funkcjonalność pozwalającą na ograniczenie wielokrotnego skanowania plików w środowisku wirtualnym, za pomocą mechanizmu przechowującego informacje o przeskanowanym już obiekcie i współdzieleniu tych informacji z innymi maszynami wirtualnymi.
16. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
17. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
18. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony.
19. Dodanie automatycznych wyłączeń nie wymaga restartu serwera.
20. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych.
21. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji.
22. W przypadku restartu serwera - usunięte z listy wyłączeń elementy mają być automatycznie uzupełnione.
23. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego.
24. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line).
25. Możliwość przeniesienia zainfekowanych plików w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
26. Wbudowane dwa niezależne moduły heurystyczne - jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie - z użyciem jednej i/lub obu metod jednocześnie.
27. Możliwość skanowania wyłącznie z zastosowaniem algorytmów heurystycznych, tj. wyłączenie skanowania przy pomocy sygnatur baz wirusów.
28. Aktualizacje modułów analizy heurystycznej.
29. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie oraz czy próbki zagrożeń będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.
30. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
31. Wysyłanie zagrożeń do laboratorium ma być możliwe z serwera zdalnego zarządzania.
32. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.

33. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
34. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail.
35. Możliwość zabezpieczenia konfiguracji programu hasłem w taki sposób, aby użytkownik siedzący przy serwerze przy próbie dostępu do konfiguracji systemu antywirusowego był proszony o podanie hasła.
36. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program ma pytać o hasło.
37. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji ma być takie samo.
38. Po instalacji systemu antywirusowego 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 wirusów.
39. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
40. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.
41. System antywirusowy ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.
42. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
43. Aktualizacja dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP).
44. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
45. Możliwość utworzenia kilku zadań aktualizacji (np. co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja).
46. Do każdego zadania aktualizacji można przypisać dwa różne profile z innym ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja). Przykładowo, domyślny profil aktualizuje z sieci lokalnej, a w przypadku jego niedostępności wybierany jest profil rezerwowy, pobierający aktualizację z Internetu.
47. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
48. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów.
49. Wykluczenie ze skanowania musi odbywać się nie tylko po nazwie procesu, ale również ma umożliwiać użycie symbolu wieloznacznego „*", zastępującego inne znaki.
50. Administrator ma możliwość dodania wykluczenia po tzw. HASH'u zagrożenia, wskazującego bezpośrednio na określoną infekcję, a nie konkretny plik.
51. Praca programu musi być niezauważalna dla użytkownika.
52. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania.
53. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

Administracja zdalna

1. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2008,2008R2, 2012, 2012R2.
2. Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance).
3. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji i konsoli w postaci jednego pakietu instalacyjnego lub każdego z modułów oddzielnie bezpośrednio ze strony producenta.

4. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW, niezależnie od platformy sprzętowej i programowej.
5. Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy występujące w sieci.
6. Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6.
7. Podczas logowania administrator musi mieć możliwość wyboru języka, w jakim zostanie wyświetlony panel zarządzający.
8. Zmiana języka panelu administracyjnego nie może wymagać zatrzymania lub reinstalacji oprogramowania zarządzającego.
9. Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL.
10. Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.
11. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.
12. Jeden centralny serwer centralnego zarządzania dla minimum 1000 stacji/serwerów.
13. Serwer proxy musi pełnić funkcję pośrednika pomiędzy lokalizacjami zdalnymi, a serwerem centralnym.
14. Serwer proxy musi być wyposażony we własną bazę danych, w której będą przechowywane dane z agentów, na wypadek braku połączenia z serwerem centralnym.
15. Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi - MDM.
16. Serwer administracyjny musi oferować możliwość instalacji serwera http proxy, pozwalającego na pobieranie aktualizacji baz sygnatur oraz pakietów instalacyjnych na stacjach roboczych bez dostępu do Internetu.
17. Serwer http proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) najczęściej pobieranych elementów.
18. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.
19. Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy.
20. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na stacjach roboczych z systemami Windows, Linux oraz serwerach Windows.
21. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na urządzeniach mobilnych z systemem Android.
22. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci.
23. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.
24. Administrator musi posiadać możliwość zarządzania za pomocą dedykowanego agenta stacjami, nie posiadającymi zainstalowanego programu zabezpieczającego.
25. Agent musi przekazywać informacje na temat stanu systemu operacyjnego do serwera administracji zdalnej.
26. Agent musi posiadać możliwość pobrania listy zainstalowanego oprogramowania firm trzecich na stacji roboczej, z możliwością jego odinstalowania.
27. Serwer administracyjny musi oferować możliwość wymuszenia połączenia agenta do serwera administracyjnego, z pominięciem domyślnego czasu oczekiwania na połączenie.
28. Instalacja agenta musi odbywać się przy wykorzystaniu repozytorium producenta. Repozytorium powinno zawierać aktualne wersje agentów, bez względu na rodzaj systemu operacyjnego.
29. Instalacja agenta nie może wymagać określenia typu systemu (32 lub 64 -bitowy) oraz jego rodzaju (Windows, Mac, itp), a dobór odpowiedniego pakietu musi być w pełni automatyczny.
30. Instalacja klienta na urządzeniach mobilnych musi być dostępna za pośrednictwem portalu WWW udostępnionego przez moduł MDM z poziomu urządzenia użytkownika.
31. W przypadku braku zainstalowanego klienta na urządzeniu mobilnym musi istnieć możliwość jego pobrania ze sklepu Google Play.

32. Administrator musi posiadać możliwość utworzenia listy zautoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.
33. Serwer administracyjny musi oferować możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, nie komunikację za pośrednictwem wiadomości SMS.
34. Serwer administracyjny musi oferować możliwość utworzenia polityk konfiguracji dla aplikacji zabezpieczającej na urządzeniu mobilnym.
35. Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów. Serwer centralnego zarządzania do zarządzania stacjami roboczymi.
36. Administrator musi posiadać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli zarządzającej
37. Dwufazowa autoryzacja musi się odbywać za pomocą wiadomości SMS lub haseł jednorazowych, generowanych na urządzeniu mobilnym za pomocą dedykowanej aplikacji.
38. Administrator musi posiadać możliwość utworzenia użytkownika wbudowanego lub zintegrowanego z grupą z usługi Active Directory.
39. Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami itp.
40. Administrator musi posiadać możliwość nadania dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko do odczytu, odczyt/zapis.
41. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.
42. Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta bez konieczności logowania się do panelu administracyjnego.
43. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności, po jakim użytkownik zostanie automatycznie wylogowany.
44. Dostępne zadania muszą być podzielone na dwie grupy: zadania klienta oraz zadania serwera.
45. Zadania serwera obejmujące zadanie instalacji agenta, generowania raportów oraz synchronizacji grup.
46. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej.
47. 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.
48. Serwer administracyjny musi w przejrzysty sposób informować administratora o elementach zadań, jakie są wymagane do jego uruchomienia, a w przypadku jego braku wskazywać brakujące elementy konfiguracji.
49. Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym.
50. Serwer administracyjny musi oferować możliwość wyboru parametrów pakietu instalacyjnego zależnych od systemu operacyjnego oraz licencji na program zabezpieczający.
51. Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu.
52. Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stację kliencką.
53. Serwer administracyjny musi oferować możliwość utworzenia jednego zadania dla kilku klientów lub grupy.
54. Serwer administracyjny musi oferować możliwość uruchomienia zadania automatycznie zgodnie z harmonogramem, po wystąpieniu nowego dziennika zdarzeń lub umieszczeniu nowego klienta w grupie dynamicznej.
55. Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów.
56. Grupy dynamiczne tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby zostać umieszczony w danej grupie. Przykładowe warunki: Adresy sieciowe IP, Aktywne zagrożenia, Stan funkcjonowania/ochrony, Wersja systemu operacyjnego itp.

57. Serwer administracyjny musi oferować możliwość utworzenia polityk dla programów zabezpieczających i modułów serwera centralnego zarządzania.
58. Serwer administracyjny musi oferować możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów. Serwer administracyjny musi oferować możliwość przypisania kilku polityk z innymi priorytetami dla jednego klienta.
59. Edytor konfiguracji polityki musi być identyczny, jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej.
60. Serwer administracyjny musi oferować możliwość nadania priorytetu „Wymuś" dla konkretnej opcji w konfiguracji klienta. Opcja ta nie będzie mogła być zmieniona na stacji klienckiej, bez względu na zabezpieczenie całej konfiguracji hasłem lub w przypadku jego braku.
61. Serwer administracyjny musi oferować możliwość ukrycia graficznego interfejsu użytkownika na stacji klienckiej i jego uruchomienia tylko przez administratora.
62. Serwer administracyjny musi umożliwiać wyświetlenie polityk, do których przynależy dana stacja robocza oraz ich edycję z poziomu właściwości samego klienta
63. Serwer administracyjny musi oferować możliwość utworzenia własnych raportów lub skorzystanie z predefiniowanych wzorów.
64. Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania.
65. Serwer administracyjny musi oferować możliwość wyboru formy przedstawienia danych w raporcie w postaci tabeli, wykresu lub obu elementów jednocześnie.
66. Serwer administracyjny musi oferować możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy itp.
67. Serwer administracyjny musi oferować możliwość określenia danych, jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na elementach wykresu oraz ich odfiltrowania i posortowania.
68. Serwer administracyjny musi być wyposażony w mechanizm importu oraz eksportu szablonów raportów.
69. Serwer administracyjny powinien posiadać Panel kontrolny z raportami administratora, pozwalający na szybki dostępu do najbardziej interesujących go danych. Panel ten musi oferować możliwość modyfikacji jego elementów.
70. Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym, dostępnym z poziomu interfejsu konsoli WWW.
71. Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości e-mail lub zapisany do pliku w formacie PDF, CSV lub PS.
72. Serwer administracyjny musi oferować możliwość skonfigurowania czasu automatycznego odświeżania raportu na panelu kontrolnym oraz umożliwiać jego odświeżenie na żądanie.
73. Serwer administracyjny musi oferować możliwość tworzenia wielu zakładek panelu, w których będą widoczne wybrane przez administratora elementy monitorujące.
74. Serwer administracyjny musi oferować możliwość maksymalizacji wybranego elementu monitorującego.
75. Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.
76. Serwer administracyjny musi oferować możliwość utworzenia własnych powiadomień lub skorzystanie z predefiniowanych wzorów.
77. Powiadomienia muszą dotyczyć zmiany ilości klientów danej grupy dynamicznej, wzrostu liczby grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń lub skanowania lub stanu obiektu serwer centralnego zarządzania.
78. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP.
79. Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu.
80. Serwer administracyjny musi oferować możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu.
81. Serwer administracyjny musi oferować możliwość podłączenia serwera administracji zdalnej do portalu zarządzania licencjami dostępnego na serwerze producenta.

82. Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji.
83. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty.
84. Serwer administracyjny musi oferować możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela.
85. 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.
86. Serwer administracyjny musi być wyposażony w machizm autodopasowania kolumn, w zależności od rozdzielczości urządzenia, na jakim jest wyświetlana.
87. Serwer administracji musi umożliwić granulację uprawnień dla Administratorów w taki sposób, aby każdemu z nich możliwe było przyznanie oddzielnych uprawnień do poszczególnych grup komputerów, polityk lub zadań.
88. Konsola webowa musi umożliwiać stronicowanie w widoku komputerów, w celu ograniczenia liczby wyświetlanych maszyn na jednej stronie.
89. Musi istnieć mechanizm, umożliwiający dodawanie reguł do istniejących już w module firewalla lub harmonogramie. Takie reguły można umieścić na początku lub końcu istniejącej listy.

II. Rozwiązanie równoważne (oprogramowanie równoważne):

1. Zaoferowane produkty równoważne muszą integrować się z posiadaną przez Zamawiającego infrastrukturą systemową:
   a) serwery - system operacyjny Windows Server 2008, 2008R2,2012, 2012R2 ;
   b) stanowiska komputerowe - system operacyjny Windows 7, Windows 10.
2. Zaoferowane produkty równoważne muszą zapewniać pełną ochronę antywirusową, firewall, dla stacji roboczych, serwerów Zamawiającego przez okres 12 miesięcy.
3. Zaoferowane produkty równoważne muszą zapewniać funkcjonalności na poziomie opisanym w punkcie I powyżej.
4. W przypadku zaoferowania rozwiązań równoważnych Wykonawca obowiązany jest wykazać, że oferowane przez niego rozwiązanie spełnia wymagania określone przez Zamawiającego w niniejszym OPZ.
5. Zamawiający wymaga złożenia w ofercie szczegółowego opisu rozwiązania równoważnego wraz z podaniem funkcjonalności proponowanego rozwiązania (pełna dokumentacja w języku polskim), w celu potwierdzenia równoważności funkcjonalności zaoferowanego rozwiązania.