Załącznik nr 1

OPIS PRZEDMIOTU ZAMÓWIENIA

Cel zamówienia:
zapewnienie bezpieczeństwa oprogramowania i danych na stacjach roboczych w sieci komputerowej Mazowieckiego Urzędu Wojewódzkiego w Warszawie.

Realizacja zamówienia - miejsce dostawy:
siedziba Zamawiającego w Warszawie przy Placu Bankowym 3/5.

Przedmiotem zamówienia jest:
odnowienie 2200 licencji na oprogramowanie antywirusowe ESET Secure Enterprise na okres 36 miesięcy, od 01.07.2018 r.

Obecnie Mazowiecki Urząd Wojewódzki w Warszawie posiada 2200 licencji na oprogramowanie antywirusowe ESET Secure Enterprise. Optymalnym rozwiązaniem byłoby przedłużenie posiadanych licencji, jednak Zamawiający dopuszcza możliwość zaoferowania produktów równoważnych w zakresie nowych licencji na oprogramowanie antywirusowe (oprogramowanie równoważne).

Oprogramowanie antywirusowe musi zapewniać poniższe funkcje:

I. Ochrona urządzeń mobilnych opartych o system Android:

1. Wspierany system co najmniej Android 4.0 (Ice Cream Sandwich).
2. Rozdzielczość wyświetlacza urządzenia 480x800px lub wyższa.
3. Procesor: ARM (minimum ARMv7).
4. Pamięć wewnętrzna: 20 MB.
5. Połączenie z siecią Internet dla celów aktualizacji sygnatur i aktywacji licencji.

Ochrona antywirusowa:
1. Ochrona plików w czasie rzeczywistym.
2. Ochrona przed atakami typu „phishing”.
3. Skanowanie rozszerzeń DEX, bibliotek SO plików archiwum oraz innych.
4. Skanowanie dostępnego w urządzeniu nośnika pamięci SD.
5. Aplikacja musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
6. Ochrona proaktywna wykrywająca nieznane zagrożenia.
7. Aplikacja ma mieć możliwość określenia poziomu głębokości skanowania plików archiwum.
8. Aplikacja ma mieć możliwość określenia domyślnej akcji podejmowanej w przypadku wykrycia zagrożenia: przeniesienia do kwarantanny, usunięcia lub zignorowania.
9. W przypadku wykrycia zagrożenia użytkownik ma otrzymać odpowiednie powiadomienie.
10. Aplikacja musi umożliwiać zdefiniowanie harmonogramu dla pełnego skanowania urządzenia.

11. Aplikacja musi umożliwiać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności, w pełni naładowane i podłączone do ładowarki.

Skanowanie na żądanie:

1. Aplikacja ma mieć możliwość skanowania zainstalowanych aplikacji.
2. Aplikacja ma wykorzystywać do celu skanowania metody heurystyczne wykrywające nieznane zagrożenia.
3. Informacje o skanowaniu mają być przechowywane w plikach dziennika.
4. Użytkownik ma mieć możliwość wskazania akcji jaka ma być podjęta w przypadku wykrycia zagrożenia: poddania kwarantannie, usunięcia lub zignorowania.
5. Użytkownik ma mieć możliwość wymuszenia przeskanowania całego urządzenia, lub wskazania folderu, który ma być przeskanowany.
6. Aplikacja ma posiadać osobne dzienniki skanowania dla ochrony plików w czasie rzeczywistym, oraz skanowania na żądanie.

Filtr SMS/MMS i połączeń (jeśli system zezwala):
Użytkownik musi mieć możliwość definiowania własnych reguł dotyczących połączeń oraz wiadomości SMS/MMS bez konieczności podawania hasła administratora.

1. Reguły zdefiniowane przez administratora (w trybie administratora) muszą mieć wyższy priorytet niż reguły zdefiniowane przez użytkownika.
2. Użytkownik i administrator ma mieć możliwość tworzenia białej i czarnej listy numerów telefonów.
3. Użytkownik i administrator ma mieć możliwość dodania numeru telefonu, dla którego można określić akcje dla:
   a) przychodzącej wiadomości SMS,
   b) przychodzącej wiadomości MMS,
   c) połączenia wychodzącego,
   d) połączenia przychodzącego.
4. Aplikacja ma mieć możliwość aktywacji blokady dla wszystkich połączeń oraz wiadomości SMS/MMS dla znanych kontaktów znajdujących się w książce telefonicznej urządzenia.
5. Aplikacja ma mieć możliwość blokady połączeń telefonicznych oraz wiadomości SMS/MMS dla nieznanych kontaktów (nieznajdujących się w książce telefonicznej urządzenia).
6. Aplikacja ma mieć możliwość blokowania anonimowych połączeń przychodzących (pochodzących z ukrytych ID).
7. Aplikacja ma być wyposażona w dziennik modułu antyspamowego zawierający informacje odnośnie filtrowania modułu.

Ochrona przed kradzieżą:

1. Użytkownik ma mieć możliwość wprowadzenia zaufanej karty SIM.
2. Dodanie zaufanej karty SIM ma się odbyć się w oparciu o kartę wprowadzoną w danym urządzeniu lub w oparciu o dane wprowadzone ręcznie.
3. Wprowadzenie danych ręcznie dotyczących zaufanej karty SIM ma się odbywać w oparciu o numer IMSI karty SIM.
4. Aplikacja ma mieć możliwość wprowadzenia zaufanych odbiorców wiadomości, do których zostanie przesłana informacja w przypadku umieszczenia w urządzeniu innej niż zaufana karty SIM.

5. Aplikacja ma mieć możliwość włączenia opcji ignorowania niedopasowania kart SIM.
6. Użytkownik ma mieć możliwość edycji treści wiadomości SMS wysyłanej na zaufane numery telefonów w przypadku nie dopasowania karty SIM.
7. W przypadku kradzieży urządzenia, prawowity użytkownik ma mieć możliwość wysłania na urządzenie komendy która umożliwi:
   a) usunięcie zawartości urządzenia,
   b) zablokowania urządzenia,
   c) przesłania na zaufany numer telefonu lokalizacji GPS w której skradzione urządzenie się znajduje.
8. Administrator musi mieć możliwość wysyłania powyższych komend bezpośrednio z poziomu konsoli centralnego zarządzania.
9. Możliwość zdalnego zresetowania hasła ma być możliwa tylko w przypadku wysłania odpowiedniego polecenia z zaufanego urządzenia.

Polityka ustawień:
Aplikacja musi posiadać funkcjonalność pozwalającą administratorowi na monitorowanie ustawień urządzenia w celu weryfikacji czy są one zgodne z polityką.

1. Administrator musi mieć wgląd w podstawowe ustawienia urządzenia:
   a) połączenie Wi-Fi,
   b) satelity GPS,
   c) usługi lokalizacyjne,
   d) pamięć,
   e) roaming danych,
   f) roaming połączeń,
   g) nieznane źródła,
   h) tryb debugowania,
   i) komunikacja NFC,
   j) szyfrowanie pamięci masowej.
2. Administrator ma mieć możliwość wyboru powyższych elementów.

Kontrola aplikacji:

1. Rozwiązanie musi umożliwiać administratorowi podejrzenie listy zainstalowanych aplikacji.
2. Administrator musi mieć możliwość blokowania zdefiniowanych aplikacji i poprosić użytkownika o odinstalowanie blokowanej aplikacji.
3. Blokowanie aplikacji musi być umożliwione co najmniej za pomocą polityk:
   a) manualnego zdefiniowania listy blokowanych aplikacji na podstawie nazwy,
   b) blokowanie na podstawie kategorii (np. kategorii Gry lub Społecznościowe),
   c) blokowanie na podstawie uprawnień aplikacji (np. aplikacji, które korzystają z modułu GPS do odczytania lokalizacji),
   d) blokowanie na podstawie źródła (np. aplikacje instalowane z innych źródeł niż sklep Google Play).
4. Administrator musi mieć możliwość monitorowania czasu, jaki użytkownik spędza na korzystaniu z poszczególnych aplikacji i sprawdzenia z jakich aplikacji użytkownik korzystał w ciągu ostatnich 30 dni, 7 dni oraz 24 godzin.

Zabezpieczenia urządzenia:

1. W ramach zabezpieczeń administrator musi mieć możliwość uruchomienia polityki zabezpieczeń, w której może określić co najmniej:
   a) minimalny poziom zabezpieczeń i złożoność blokady ekranu,
   b) maksymalną dopuszczaną liczbę błędnych prób odblokowania,
   c) odstęp czasu po którym użytkownik musi zmienić kod odblokowujący urządzenie,
   d) czas przeznaczony na odblokowanie urządzenia,
   e) ograniczyć dostęp do kamery wbudowanej w urządzenie.

Aktualizacje sygnatur:

1. Wymuszenie pobrania aktualizacji na żądanie ma być dostępne z poziomu interfejsu aplikacji.
2. Aplikacja ma mieć możliwość określenia harmonogramu zgodnie, z którym pobierane będą aktualizacje sygnatur co najmniej: raz dziennie, co 6 godzin, co 3 dni, co tydzień.
3. Aplikacja ma mieć funkcjonalność ochrony hasłem wybranych modułów ochrony, w tym co najmniej dostępu do ustawień ochrony antywirusowej, ustawień modułu antyspamowego, ochrony przed kradzieżą, uruchamiania zadań audytu zabezpieczeń oraz przed deinstalacją.
4. Aplikacja ma mieć możliwość ukrycia ikony powiadomień.

Konfiguracja i zdalne zarządzanie:

1. Administrator musi mieć możliwość eksportu/importu ustawień z/do pliku w celu przeniesienia konfiguracji na inne urządzenie mobilne.
2. Administrator musi mieć możliwość zabezpieczenia ustawień aplikacji hasłem przed ich modyfikacją.
3. Administrator musi mieć możliwość zdalnego wysyłania komunikatów z poziomu konsoli centralnego zarządzania do użytkowników urządzeń mobilnych.
4. Przesłana wiadomość musi wyświetlać się w formie wyskakującego okna, aby użytkownik ich nie przeoczył.
5. Administrator musi mieć możliwość kontrolowania mechanizmu aktualizacji oprogramowania.

II. ESET Endpoint Security Suite:

1. Pełne wsparcie dla systemu Windows XP SP3/Vista/Windows 7/Windows8/Windows 8.1/Windows 8.1 Update/10.
2. Wsparcie dla 32- i 64-bitowej wersji systemu Windows.
3. Wersja programu dla stacji roboczych Windows dostępna zarówno w języku polskim jak i angielskim.
4. Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim.
5. Skuteczność programu potwierdzona nagrodami VB100 i AV-comparatives

Ochrona antywirusowa i antyspyware

1. Pełna 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 (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
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. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min 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. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
22. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego).

23. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
24. 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).
25. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
26. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
27. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
28. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Program musi umożliwić blokowanie danej strony internetowej po podaniu na liście całej nazwy strony lub tylko wybranego słowa występującego w nazwie strony.
29. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora.
30. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
31. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
32. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
33. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta.
34. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
35. Program musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
36. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym.
37. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
38. 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.
39. 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.
40. 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.

41. Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika.
42. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
43. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
44. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
45. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła.
46. 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.
47. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.
48. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i administratora wraz z listą niezainstalowanych aktualizacji.
49. Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.
50. 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.
51. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
52. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.
53. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM , urządzeń przenośnych oraz urządzeń dowolnego typu.
54. Funkcja blokowania nośników wymiennych bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model.
55. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia, dana funkcjonalność musi pozwalać na automatyczne wypełnienie właściwości urządzenia dla tworzonej reguły.

56. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie brak dostępu do podłączanego urządzenia.
57. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
58. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
59. Użytkownik ma posiadać możliwość takiej konfiguracji programu aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika.
60. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
61. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    a) tryb automatyczny z regułami gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    b) tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
    c) tryb oparty na regułach gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
    d) tryb uczenia się, w którym program uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
    e) tryb inteligentny – w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach.
62. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
63. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
64. Oprogramowanie musi posiadać zaawansowany skaner pamięci.
65. Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp.
66. 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.
67. 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.
68. 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.
69. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.

70. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami.
71. Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji program zgłosi posiadanie nieaktualnej bazy sygnatur.
72. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji.
73. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http
74. Program musi być wyposażony w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback).
75. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa).
76. Program ma być w pełni zgodny z technologią CISCO Network Access Control.
77. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełno ekranowym.
78. W momencie wykrycia trybu pełno ekranowego aplikacja ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań aplikacji.
79. Użytkownik ma mieć możliwość skonfigurowania programu tak aby automatycznie program włączał powiadomienia oraz zadania pomimo pracy w trybie pełnoekranowym po określonym przez użytkownika czasie.
80. 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.
81. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
82. Program musi posiadać możliwość utworzenia z poziomu interfejsu aplikacji dziennika diagnostycznego na potrzeby pomocy technicznej.
83. Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline.
84. Możliwość podejrzenia licencji za pomocą, której program został aktywowany.
85. 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, kontrola dostępu do stron internetowych, , Obsługa technologii Microsoft NAP.
86. W programie musi istnieć możliwość tymczasowego wstrzymania polityk wysłanych z poziomu serwera zdalnej administracji.
87. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej.
88. Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas po którym automatycznie zostają przywrócone dotychczasowe ustawienia.

89. Administrator ma możliwość wstrzymania polityk na 10 min, 30 min, 1 godzinę i 4 godziny.
90. Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika.
91. Program musi posiadać opcję automatycznego skanowania komputera po dokonaniu zmian z użyciem opcji wstrzymania polityki.
92. Aplikacja musi posiadać funkcję ręcznej aktualizacji komponentów programu.
93. 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.
94. Program musi posiadać możliwość definiowana stanów aplikacji, jakie będą wyświetlane użytkownikowi np. powiadomień o wyłączonych mechanizmach ochrony czy stanie licencji.
95. Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie.

Ochrona przed spamem

1. Ochrona antyspamowa dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail.
2. Program ma umożliwiać uaktywnienie funkcji wyłączenia skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej.
3. Pełna integracja z programami pocztowymi MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail – antyspamowe funkcje programu dostępne są bezpośrednio z paska menu programu pocztowego.
4. Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego.
5. Możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną wiadomość i odwrotnie oraz ręcznego dodania wiadomości do białej i czarnej listy z wykorzystaniem funkcji programu zintegrowanych z programem pocztowym.
6. Możliwość definiowania swoich własnych folderów, gdzie program pocztowy będzie umieszczać spam.
7. Możliwość zdefiniowania dowolnego Tag-u dodawanego do tematu wiadomości zakwalifikowanej jako spam.
8. Program ma umożliwiać współpracę w swojej domyślnej konfiguracji z folderem „Wiadomości śmieci” obecnym w programie Microsoft Outlook.
9. Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną zmieni jej właściwość jako „nieprzeczytana” oraz w momencie zaklasyfikowania wiadomości jako spam na automatyczne ustawienie jej właściwości jako „przeczytana”.
10. Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.

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.

Kontrola dostępu do stron internetowych

1. Aplikacja musi być wyposażony w zintegrowany moduł kontroli odwiedzanych stron internetowych.
2. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane zdefiniowane reguły.
3. Dodawanie użytkowników musi być możliwe w oparciu o już istniejące konta użytkowników systemu operacyjnego.
4. Profile mają być automatycznie aktywowane w zależności od zalogowanego użytkownika.
5. Aplikacja musi posiadać możliwość filtrowania url w oparciu o co najmniej 140 kategorii i pod kategorii.
6. Podstawowe kategorie w jakie aplikacja musi być wyposażony to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii.
7. Moduł musi posiadać także możliwość grupowania kategorii już istniejących.
8. Lista adresów url znajdujących się w poszczególnych kategoriach musi być na bieżąco aktualizowana przez producenta.
9. Użytkownik musi posiadać możliwość wyłączenia integracji modułu kontroli dostępu do stron internetowych.
10. Aplikacja musi posiadać możliwość określenia uprawnień dla dostępu do kategorii url – zezwól, zezwól i ostrzeż, blokuj.
11. Program musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania określonej w regułach witryny.

Ochrona serwera plików Windows

1. Wsparcie dla systemów: Microsoft Windows Server 2003, 2008, 2008 R2, 2012, 2012 R2, 2016, SBS 2003, SBS 2003 R2, SBS 2008, SBS 2011, Microsoft MultiPoint Server 2010, Microsoft MultiPoint Server 2011, Windows MultiPoint Server 2012.
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 powinna wspierać mechanizm klastrowania.
17. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
18. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS.
19. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
20. Program ma umożliwiać użytkownikowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: pamięci masowych, płyt CD/DVD i pamięci masowych FireWire.

21. Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia.
22. Aplikacja musi posiadać funkcjonalność, która automatycznie uzupełni elementy wymagane dla tworzenia reguł w oparciu o informacje dostępne z aktualnie podłączonego nośnika.
23. Aplikacja ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, brak dostępu do podłączanego urządzenia.
24. Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
25. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
26. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
27. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony.
28. Dodanie automatycznych wyłączeń nie wymaga restartu serwera.
29. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych.
30. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji.
31. W przypadku restartu serwera – usunięte z listy wyłączeń elementy mają być automatycznie uzupełnione.
32. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego.
33. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line).
34. 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.
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 skanowania wyłącznie z zastosowaniem algorytmów heurystycznych tj. wyłączenie skanowania przy pomocy sygnatur baz wirusów.
37. Aktualizacje modułów analizy heurystycznej.
38. 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.

39. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
40. Wysyłanie zagrożeń do laboratorium ma być możliwe z serwera zdalnego zarządzania i lokalnie z każdej stacji roboczej w przypadku komputerów mobilnych.
41. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
42. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
43. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail.
44. 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.
45. 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.
46. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji ma być takie samo.
47. System antywirusowy ma być w pełni zgodny z technologią CISCO NAC.
48. System antywirusowy ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji.
49. System antywirusowy 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 ma także posiadać opcję dezaktywacji tego mechanizmu.
50. 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.
51. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
52. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.
53. Program powinien umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: nośników CD/DVD oraz urządzeń USB.
54. System antywirusowy 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.

55. 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.
56. 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.
57. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
58. 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).
59. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
60. 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).
61. 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.
62. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
63. Aplikacja musi wspierać skanowanie magazynu Hyper-V
64. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów
65. Wykluczenie ze skanowania musi odbywać się nie tylko po nazwie procesu ale również ma umożliwiać użycie symbolu wieloznacznego „*” zastępującego inne znaki.
66. Administrator ma możliwość dodania wykluczenia po tzw. HASH’u zagrożenia, wskazującego bezpośrednio na określoną infekcję a nie konkretny plik.
67. Praca programu musi być niezauważalna dla użytkownika.
68. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania.
69. 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 2003, 2008, 2012 oraz systemach Linux.
2. Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance).
3. Serwer administracyjny musi wspierać instalację w oparciu o co najmniej bazy danych MS SQL i MySQL.

4. Serwer administracyjny musi oferować możliwość wykorzystania już istniejącej bazy danych MS SQL lub MySQL użytkownika.
5. 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.
6. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej.
7. Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy występujące w sieci.
8. Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6.
9. Podczas logowania administrator musi mieć możliwość wyboru języka w jakim zostanie wyświetlony panel zarządzający.
10. Zmiana języka panelu administracyjnego nie może wymagać zatrzymania lub reinstalacji oprogramowania zarządzającego.
11. Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL.
12. Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.
13. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.
14. Jeden centralny serwer centralnego zarządzania bez względu na wielkość sieci.
15. Instalacja serwera administracyjnego powinna oferować wybór trybu pracy serwera w sieci w przypadku rozproszonych sieci –serwer pośredniczący (proxy) lub serwer centralny.
16. Serwer proxy musi pełnić funkcję pośrednika pomiędzy lokalizacjami zdalnymi a serwerem centralnym.
17. Serwer proxy musi być wyposażony we własną bazę danych, w której będą przechowywane dane z agentów na wypadek braku połączenia z serwerem centralnym.
18. Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM.
19. 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.
20. Serwer http proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) najczęściej pobieranych elementów.
21. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.
22. Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy.
23. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na stacjach roboczych z systemami Windows, Mac OS X oraz Linux oraz serwerach Windows.

24. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na urządzeniach mobilnych z systemem Android.
25. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci.
26. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.
27. Administrator musi posiadać możliwość zarządzania za pomocą dedykowanego agenta stacjami nie posiadającymi zainstalowanego programu zabezpieczającego.
28. Agent musi przekazywać informacje na temat stanu systemu operacyjnego do serwera administracji zdalnej.
29. Agent musi posiadać możliwość pobrania listy zainstalowanego oprogramowania firm trzecich na stacji roboczej z możliwością jego odinstalowania.
30. Serwer administracyjny musi oferować możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.
31. Instalacja agenta musi odbywać się przy wykorzystaniu repozytorium producenta. Repozytorium powinno zawierać aktualne wersje agentów bez względu na rodzaj systemu operacyjnego.
32. 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.
33. Instalacja klienta na urządzeniach mobilnych musi być dostępna za pośrednictwem portalu WWW udostępnionego przez moduł MDM z poziomu urządzenia użytkownika.
34. W przypadku braku zainstalowanego klienta na urządzeniu mobilnym musi istnieć możliwość jego pobrania ze sklepu Google Play.
35. Administrator musi posiadać możliwość utworzenia listy zautoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.
36. 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.
37. Serwer administracyjny musi oferować możliwość utworzenia polityk konfiguracji dla aplikacji zabezpieczającej na urządzeniu mobilnym.
38. Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi.
39. Administrator musi posiadać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli zarządzającej

40. Dwu fazowa autoryzacja musi się odbywać za pomocą wiadomości SMS lub haseł jednorazowych generowanych na urządzeniu mobilnym za pomocą dedykowanej aplikacji.
41. Administrator musi posiadać możliwość utworzenia użytkownika wbudowanego lub zintegrowanego z grupą z usługi Active Directory.
42. Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp.
43. Administrator musi posiadać możliwość nadania dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko do odczytu, odczyt/zapis.
44. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.
45. Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta bez konieczności logowania się do panelu administracyjnego.
46. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności po jakim użytkownik zostanie automatycznie wylogowany.
47. Dostępne zadania muszą być podzielone na dwie grupy: zadania klienta oraz zadania serwera.
48. Zadania serwera obejmujące zadanie instalacji agenta, generowania raportów oraz synchronizacji grup.
49. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej.
50. 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.
51. 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.
52. Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym.
53. Serwer administracyjny musi oferować możliwość wyboru parametrów pakietu instalacyjnego zależnych od systemu operacyjnego oraz licencji na program zabezpieczający.
54. Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu.
55. Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką.
56. Serwer administracyjny musi oferować możliwość utworzenia jednego zadania dla kilku klientów lub grupy.
57. Serwer administracyjny musi oferować możliwość uruchomienia zadania automatycznie zgodnie z harmonogramem, po wystąpieniu nowego dziennika zdarzeń lub umieszczeniu nowego klienta w grupie dynamicznej.

58. Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów.
59. 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.
60. Serwer administracyjny musi oferować możliwość utworzenia polityk dla programów zabezpieczających i modułów serwera centralnego zarządzania.
61. 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.
62. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej.
63. 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.
64. Serwer administracyjny musi oferować możliwość ukrycia graficznego interfejsu użytkownika na stacji klienckiej i jego uruchomienia tylko przez administratora.
65. Serwer administracyjny musi umożliwiać wyświetlenie polityk do których przynależy dana stacja robocza oraz ich edycję z poziomu właściwości samego klienta
66. Serwer administracyjny musi oferować możliwość utworzenia własnych raportów lub skorzystanie z predefiniowanych wzorów.
67. Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania.
68. Serwer administracyjny musi oferować możliwość wyboru formy przedstawienia danych w raporcie w postaci tabeli, wykresu lub obu elementów jednocześnie.
69. Serwer administracyjny musi oferować możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy, itp.
70. Serwer administracyjny musi oferować możliwość określenia danych jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na elementach wykresu oraz ich odfiltrowania i posortowania.
71. Serwer administracyjny musi być wyposażony w mechanizm importu oraz eksportu szablonów raportów.
72. 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.
73. Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym dostępnym z poziomu interfejsu konsoli WWW.

74. Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub PS.
75. Serwer administracyjny musi oferować możliwość skonfigurowania czasu automatycznego odświeżania raportu na panelu kontrolnym oraz umożliwiać jego odświeżenie na żądanie.
76. Serwer administracyjny musi oferować możliwość tworzenia wielu zakładek panelu, w których będą widoczne wybrane przez administratora elementy monitorujące.
77. Serwer administracyjny musi oferować możliwość maksymalizacji wybranego elementu monitorującego.
78. Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.
79. Serwer administracyjny musi oferować możliwość utworzenia własnych powiadomień lub skorzystanie z predefiniowanych wzorów.
80. 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.
81. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP.
82. Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu.
83. Serwer administracyjny musi oferować możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu.
84. Serwer administracyjny musi oferować możliwość podłączenia serwera administracji zdalnej do portalu zarządzania licencjami dostępnego na serwerze producenta.
85. Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji.
86. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty.
87. Serwer administracyjny musi oferować możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela.
88. 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.
89. Serwer administracyjny musi być wyposażony w machizm autodopasowania kolumn w zależności od rozdzielczości urządzenia na jakim jest wyświetlana.
90. 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.
91. Konfiguracja zestawów uprawnień musi umożliwiać przypisanie praw tylko do odczytu, odczytu i użycia, oraz prawo do zapisania zmian w ramach danego zadania lub polityki w konsoli ERA.

92. Konsola webowa musi umożliwiać stronicowanie w widoku komputerów w celu ograniczenia liczby wyświetlanych maszyn na jednej stronie.
93. Administrator musi mieć możliwość podłączenia do stacji roboczej z użyciem protokołu RDP bezpośrednio z poziomu konsoli ERA.
94. Serwer musi wspierać wysyłanie logów do systemu SIEM IBM qRadar
95. Musi istnieć mechanizm, umożliwiający dodawanie reguł do istniejących już w module firewalla lub harmonogramie. Takie reguły można umieścić na początku lub końcu istniejącej listy.
96. Konsola administracyjna musi umożliwiać dodanie własnego logotypu do interfejsu webowego.

III. Ochrona serwera plików Windows

1. Wsparcie dla systemów: Microsoft Windows Server 2003, 2008, 2008 R2, 2012, 2012 R2, SBS 2003, SBS 2003 R2, SBS 2008, SBS 2011, Microsoft MultiPoint Server 2010, Microsoft MultiPoint Server 2011, Windows MultiPoint Server 2012.
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 powinna wspierać mechanizm klastrowania.
17. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).

18. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS.
19. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
20. Program ma umożliwiać użytkownikowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: pamięci masowych, płyt CD/DVD i pamięci masowych FireWire.
21. Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia.
22. Aplikacja musi posiadać funkcjonalność, która automatycznie uzupełni elementy wymagane dla tworzenia reguł w oparciu o informacje dostępne z aktualnie podłączonego nośnika.
23. Aplikacja ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, brak dostępu do podłączanego urządzenia.
24. Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
25. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
26. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
27. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony.
28. Dodanie automatycznych wyłączeń nie wymaga restartu serwera.
29. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych.
30. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji.
31. W przypadku restartu serwera – usunięte z listy wyłączeń elementy mają być automatycznie uzupełnione.
32. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego.
33. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line).
34. 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.
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 skanowania wyłącznie z zastosowaniem algorytmów heurystycznych tj. wyłączenie skanowania przy pomocy sygnatur baz wirusów.
37. Aktualizacje modułów analizy heurystycznej.
38. 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.

39. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
40. Wysyłanie zagrożeń do laboratorium ma być możliwe z serwera zdalnego zarządzania i lokalnie z każdej stacji roboczej w przypadku komputerów mobilnych.
41. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
42. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
43. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail.
44. 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.
45. 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.
46. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji ma być takie samo.
47. System antywirusowy ma być w pełni zgodny z technologią CISCO NAC.
48. System antywirusowy ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji.
49. System antywirusowy 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 ma także posiadać opcję dezaktywacji tego mechanizmu.
50. 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.
51. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
52. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.
53. Program powinien umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: nośników CD/DVD oraz pamięci USB.
54. System antywirusowy 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.

55. 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.
56. 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.
57. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
58. 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).
59. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
60. 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).
61. 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.
62. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
63. Aplikacja musi wspierać skanowanie magazynu Hyper-V.
64. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów.
65. Praca programu musi być niezauważalna dla użytkownika.
66. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania.
67. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

IV. Ochrona poczty MS Exchange

1. Musi zapewniać wsparcie dla systemów poczty Microsoft Exchange 2003/2007/2010/2013/2016
2. Musi zapewniać wsparcie dla ról Mailbox, Edge, Hub.
3. Aplikacja musi umożliwiać Administratorowi na etapie instalacji wybór komponentów jakie mają być zainstalowane.
4. Aplikacja musi skanować pocztę przychodzącą i wychodzącą na serwerze MS Exchange.
5. Program ma zapewnić skanowanie bezpośrednio w storach Exchange przy pomocy VSAPI.
6. Program musi mieć możliwość zdefiniowania kilku wątków skanujących w celu optymalizacji pracy serwera.
7. Program ma zapewnić skanowanie przed zapisaniem wiadomości w storze przy pomocy transport agenta.
8. W przypadku wykrycia wirusa/blokowania wiadomości system musi umożliwić usunięcie wiadomości/ załącznika, podmianę załącznika na czysty plik zawierający jedynie informację o infekcji.

9. Możliwość tworzenia różnych reguł blokowania wiadomości w tym co najmniej po zdefiniowanym nadawcy, odbiorcy, temacie wiadomości, typie załącznika, rozmiarze załącznika, rozmiarze wiadomości, nagłówku wiadomości, na podstawie uzyskanego wyniku skanowania antyspamowego i antywirusowego, godzinie odbioru, obecności załącznika chronionego hasłem lub uszkodzonego archiwum.
10. Program musi posiadać możliwość tworzenia białych i czarnych list domen/adresów IP, adresów e-mail.
11. Aplikacja musi posiadać możliwość akceptacji białych list stworzonych na poziomie serwera MS Exchange.
12. Program musi posiadać wbudowany w oprogramowanie filtr antyspamowy odpowiedzialny za filtrowanie niechcianej poczty.
13. System antyspamowy ma być wyposażony przynajmniej w możliwość sprawdzania list RBL, DNSBL oraz mechanizm reputacji poczty.
14. Administrator musi mieć możliwość dodania własnych adresów list RBL oraz DSBL z których będzie korzystać aplikacja.
15. Program ma posiadać mechanizmy greylistingu (szare listy).
16. Aplikacja musi posiadać możliwość tworzenia wyjątków dla mechanizmu greylistingu.
17. Program ma posiadać możliwość stworzenia End User Quarantine.
18. Kwarantanna musi być dostępna dla użytkownika końcowego za pośrednictwem przeglądarki www.
19. Użytkownik końcowy musi posiadać możliwość zarządzania wiadomościami znajdującymi się w kwarantannie w tym co najmniej, mieć możliwość uwolnienia wiadomości z kwarantanny, jej usunięcia lub pozostawienia w kwarantannie.
20. Administrator musi mieć możliwość wglądu w globalną kwarantannę z poziomu interfejsu aplikacji oraz przeglądarki www.
21. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików serwera "na żądanie" lub według harmonogramu.
22. Wykrywanie niebezpiecznych aplikacji typu Adware, Spyware, Dialer itp.
23. Wbudowana technologia do ochrony przed rootkitami.
24. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
25. Skanowanie plików spakowanych i skompresowanych.
26. Aplikacja musi w momencie instalacji na serwerze wykrywać usługi jakie są zainstalowane i tworzyć odpowiednie wyjątki dla nich.
27. Zainstalowana aplikacja musi wykorzystywać technologię chmury w celu przyśpieszenia reakcji na nowe zagrożenia oraz optymalizacji samego procesu skanowania.
28. Aplikacja musi być wyposażona w mechanizm chroniący serwer przed exploitami i atakami typu 0-day.
29. Aplikacja musi posiadać zaawansowany skaner pamięci umożliwiający wykrywanie zagrożeń próbujących działać na poziomie pamięci operacyjnej serwera.
30. Zainstalowany system ochrony musi być wyposażony w system HIPS.
31. Aplikacja musi w natywny sposób wspierać środowiska klastrowe.
32. System musi umożliwiać wskazanie zewnętrznych lokalizacji w których przechowywane będą moduły i aktualizacje programu.

33. Aplikacja musi wspierać WMI za pomocą których może przekazywać podstawowe informacje na temat swojej pracy do zewnętrznych systemów np. SIEM.
34. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail, Windows Live Mail zainstalowanego lokalnie na serwerze pocztowym.
35. Możliwość utworzenia kilku zadań skanowania (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (metody skanowania, obiekty skanowania, czynności) .
36. Pliki zapisywane w katalogu kwarantanny powinny być szyfrowane.
37. Aplikacja musi umożliwiać aktualizację modułów ochrony bez konieczności reinstalacji całego programu.
38. Aplikacja musi być wyposażona w dwa niezależnie pracujące mechanizmy analizy heurystycznej (standardowa i zaawansowana heurystyka).
39. Administrator musi posiadać możliwość używania jednego poziomu analizy heurystycznej lub obu poziomów jednocześnie.
40. Aplikacja musi umożliwiać automatyczne wysyłanie nowych zagrożeń (wykrytych przez heurystykę) do laboratorium producenta przez program antywirusowy – nie wymaga ingerencji użytkownika.
41. Wysyłanie nowych zagrożeń musi być możliwe za pomocą interfejsu aplikacji i nie może do tego celu wykorzystywać klienta pocztowego zainstalowanego w systemie.
42. Program musi umożliwiać wysyłanie wraz z próbką adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
43. W przypadku wykrycia wirusa, ostrzeżenie może zostać wysłane do administratora poprzez e-mail.
44. Aplikacja musi posiadać wbudowany dziennik zdarzeń rejestrujący informacje na temat znalezionych wirusów, dokonanych aktualizacji baz wirusów i wersji oprogramowania.
45. Administrator musi mieć możliwość zabezpieczenia hasłem dostępu do opcji konfiguracyjnych programu.
46. Możliwość zabezpieczenia hasłem musi obejmować wyłączenie programu antywirusowego oraz jego odinstalowanie.
47. Aplikacja musi w sposób automatyczny i przyrostowy dokonywać aktualizacji baz sygnatur wirusów.
48. Aktualizacja musi być 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).
49. Aplikacja musi posiadać możliwość automatycznego ściągania oraz udostępniania zbiorów aktualizacyjnych
50. Aplikacja musi wspierać aktualizacje za pośrednictwem serwera Proxy.
51. Administrator musi posiadać możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami.
52. Program musi uruchamiać jeden skaner uruchamiany w pamięci, do którego odnoszą się wszystkie monitory skanujące i skanery na żądanie.

53. Aplikacja musi posiadać możliwość zdalnej administracji za pomocą konsoli administracji zdalnej.
54. Aplikacja musi posiadać wbudowany, dedykowany moduł command line umożliwiający konfigurację oraz uruchamianie zadań zainstalowanej aplikacji.
55. Aplikacja musi być wyposażona w narzędzie umożliwiające wygenerowanie raportu dotyczącego stanu komputera, w tym co najmniej zainstalowanych aplikacji, uruchomionych procesów, ważnych wpisów w rejestrze i uruchomionych usług.
56. Musi istnieć możliwość zdalnej administracji programem za pomocą konsoli administracji zdalnej.
57. Do administracji zdalnej musi być wykorzystywany dedykowany agent.
58. Agent musi komunikować się z serwerem administracji zdalnej w bezpieczny sposób uniemożliwiający podsłuch komunikacji.
59. Skuteczność programu ma być potwierdzona nagrodami niezależnych organizacji (np. VB100, ISCA labs, Check Mark).
60. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

Rozwiązanie równoważne (oprogramowanie równoważne):

1. Zaoferowane produkty równoważne muszą integrować się z posiadaną przez Zamawiającego infrastrukturą systemową:
   a). serwera pocztowego - system operacyjny Windows Server 2016 oraz oprogramowanie aplikacyjne Microsoft Exchange 2016,
   b). stanowiska komputerowe – system operacyjny Windows XP, Windows 8.1, Windows 10.
2. Zaoferowane produkty równoważne muszą zapewniać pełną ochronę antywirusową, antyspamową, antyhakerską, dla stacji roboczych, serwerów Zamawiającego oraz placówek podległych wojewodzie przez okres 36 miesięcy.
3. Zaoferowane produkty równoważne muszą zapewniać funkcjonalności na poziomie opisanym w punktach I-IV powyżej.
4. W przypadku zaoferowania rozwiązania równoważnego, Wykonawca będzie również zobowiązany do przeprowadzenia szkolenia dla sześciu wskazanych pracowników Mazowieckiego Urzędu Wojewódzkiego w Warszawie z obsługi równoważnego oprogramowania w terminie uzgodnionym z Zamawiającym jednak nie później niż do 10 dni roboczych od dnia podpisania umowy,
5. W przypadku zaoferowania rozwiązań równoważnych Wykonawca, zgodnie z przepisem art. 30 ust. 5 ustawy Prawo zamówień publicznych, obowiązany jest wykazać, że oferowane przez niego rozwiązanie spełnia wymagania określone przez Zamawiającego w niniejszym OPZ.
6. 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.