

Załącznik nr 6

Wymagania jakie musi spełniać oprogramowanie w zakresie pozycji nr 1 - 350 sztuk licencji - specyfikacja na stacje robocze i serwery wraz z konsolą do centralnej administracji (w przypadku oferty równoważnej)

Stacje robocze i serwery Windows

1. Pełne wsparcie dla systemu Windows 2000/XP/Vista/Windows 7/Windows 8/Windows 8.1
2. Wsparcie dla 32- i 64-bitowej wersji systemu Windows.
3. Wersja programu dla stacji roboczych Windows dostępna w języku polskim.
4. Skuteczność programu potwierdzona w testach VB100 i co najmniej jedną inną niezależną organizacją taką jak ICSA labs lub Check Mark.

Ochrona antywirusowa i antyspyware

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakierskich, backdoor, itp.
2. Wbudowana technologia do ochrony przed rootkitami.
3. Możliwość skanowania "na żądanie" lub według harmonogramu.
4. System ma oferować administratorowi możliwość wstrzymania zadań w harmonogramie w przypadku pracy komputera na baterii.
5. Skanowanie "na żądanie" pojedynczych plików lub katalogów
6. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
8. Możliwość skanowania dysków sieciowych i dysków przenośnych.
9. Skanowanie plików spakowanych i skompresowanych.
10. Możliwość definiowania listy rozszerzeń plików, które mają być skanowane (w tym z uwzględnieniem plików bez rozszerzeń).
11. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
12. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
13. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
14. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny)
15. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail, Mozilla Thunderbird.
16. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail, Mozilla Thunderbird.

17. 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).
18. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym.
19. Możliwość definiowania różnych portów dla POP3 i IMAP, na których ma odbywać się skanowanie.
20. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
21. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora.
22. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
23. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
24. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
25. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
26. Aplikacja musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
27. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym.
28. 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.
29. Wbudowane dwa niezależne moduły heurystyczne
30. Interfejs programu ma mieć możliwość automatycznego aktywowania trybu bez grafiki w momencie, gdy użytkownik przełączy system Windows w tryb wysokiego kontrastu.
31. Możliwość zabezpieczenia konfiguracji programu oraz możliwości deinstalacji hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji lub deinstalacji programu był proszony o podanie hasła.
32. 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.
33. System antywirusowy uruchomiony z płyty bootowalnej musi pracować w trybie graficznym i musi umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
34. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart, modemów, portów LPT/COM oraz urządzeń przenośnych
35. Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń np. w oparciu o typ urządzenia, numer seryjny urządzenia.
36. 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.
37. Użytkownik ma posiadać możliwość takiej konfiguracji aplikacji aby skanowanie całego podłączonego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika
38. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
39. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego oraz wybór akcji: pytaj, blokuj, zezwól.

40. 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.
41. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.
42. Możliwość utworzenia kilku zadań aktualizacji gdzie każde zadanie może być uruchomione z własnymi ustawieniami.
43. Aplikacja musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http
44. Aplikacja musi być wyposażona w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback).
45. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
46. 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.
47. Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania.
48. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

Ochrona systemu plików Linux

1. Skaner antywirusowy, antyspyware
2. Możliwość skanowania wszystkimi modułami programu (heurystyka, sygnatury, adware/spyware, aplikacje niepożądane, aplikacje niebezpieczne)
3. Skanowanie plików, plików spakowanych, archiwów samorozpakowujących, plików wiadomości e-mail
4. Konfiguracja wszystkich modułów oprogramowania ma być możliwa poprzez edycję jednego pliku konfiguracyjnego
5. Możliwość ustawień limitów dla modułu skanującego względem maksymalnego rozmiaru pliku, maksymalnej liczby warstw kompresji, maksymalnego rozmiaru archiwum, maksymalnego czasu skanowania, maksymalnego rozmiaru archiwum samorozpakowującego, rozszerzenia skanowanego pliku
6. Możliwość skanowania podkatalogów oraz podążania za łańcuchami symbolicznymi (symlinkami) w systemie
7. Możliwość definicji maksymalnego poziomu głębokości skanowanych podkatalogów
8. Możliwość tworzenia kwarantanny dla plików zainfekowanych w dowolnej lokalizacji w systemie plików
9. Możliwość zdefiniowania częstotliwości aktualizacji programu.
10. Brak potrzeby instalacji dodatkowych zależności do systemu oprócz biblioteki LIBC, oprogramowanie po instalacji jest od razu gotowe do pracy
11. Wbudowany bezpośrednio w program system obsługi plików spakowanych niewymagający zewnętrznych komponentów zainstalowanych w systemie
12. Brak potrzeby instalacji źródeł jądra systemu oraz kompilacji jakichkolwiek modułów jądra do skanowania plików na żądanie
13. Możliwość tworzenia przynajmniej pięciu poziomów dokładności czyszczenia zainfekowanych plików
14. Możliwość skanowania alternatywnych strumieni danych (ADS) obecnych w systemie plików NTFS
15. Wsparcie dla skanowania za pośrednictwem biblioteki współdzielonej LIBC, która umożliwia skanowanie plików które są otwierane, zamykane lub wykonywane przez serwery plików (ftp, Samba) które wykorzystują zapytania do biblioteki LIBC

16. Możliwość zdefiniowania liczby wątków oraz liczby procesów dla każdego z modułów skanujących
17. Możliwość tworzenia różnych akcji w zależności od typu zdarzenia (w przypadku pliku nie przeskanowanego, pliku przeskanowanego, pliku zainfekowanego).
18. Wsparcie dla zewnętrznego serwera logującego syslog, możliwość definiowania dowolnego pliku logu (np. daemon, mail, user itp.)
19. Możliwość zdefiniowania kilku poziomów logowania programu
20. Możliwość zdalnego zarządzania z wykorzystaniem serwera zdalnego zarządzania instalowanego na systemach Windows 8, 7, Vista, XP, 2000; Windows Server 2012/2012 R2, 2008 R2, 2008, 2003
21. Możliwość łatwej konfiguracji produktu za pomocą prostej w użyciu konsoli administracyjnej spod systemów Windows 8, 7, Vista, XP, 2000; Windows Server 2012/2012 R2, 2008 R2, 2008, 2003
22. Możliwość zdefiniowania hasła zabezpieczającego służącego zabezpieczeniu podłączenia do serwera zdalnego zarządzania
23. Możliwość uruchomienia interfejsu programu dostępnego przez przeglądarkę Web
24. Interfejs ma umożliwiać modyfikację ustawień programu oraz jego aktualizację i przeskanowanie dowolnego obszaru systemu plików a także przegląd statystyk dotychczas przeskanowanych plików
25. Interfejs programu dostępny przez przeglądarkę Web wykorzystuje wbudowany w program serwer http
26. Możliwość uruchomienia interfejsu Web na dowolnym porcie TCP
27. Możliwość uruchomienia interfejsu Web na dowolnym interfejsie sieciowym
28. Możliwość zabezpieczenia dostępu do interfejsu Web poprzez zdefiniowanie nazwy użytkownika i hasła
29. Interfejs Web ma przedstawić administratorowi dokładny wynik skanowania poszczególnych plików w systemie wraz z możliwością pobrania tych wyników w postaci pliku tekstowego celem późniejszej analizy
30. Możliwość podglądu informacji o licencji bezpośrednio z poziomu interfejsu Web która zawiera przynajmniej informacje o liczbie dni do wygaśnięcia licencji, nazwę użytkownika licencji oraz nazwę produktu którego dotyczy licencja
31. Program ma być wyposażony w graficzny menadżer kwarantanny dostępny z poziomu interfejsu Web. Menadżer ma oferować administratorowi możliwość przeglądu, pobrania, dodania i usunięcia plików w kwarantannie
32. Menadżer kwarantanny ma posiadać możliwość wyszukiwania plików znajdujących się w kwarantannie przynajmniej po nazwie pliku, dacie dodania pliku (możliwość definiowania przedziałów czasowych), rozmiarze (możliwość definiowania minimalnej i maksymalnej wielkości) oraz ilości plików (możliwość definiowania minimalnej i maksymalnej ilości)
33. Interfejs Web do zarządzania produktem ma opierać się o wbudowane w program biblioteki PHP w wersji nie niższej niż 5.2.8
34. Interfejs dostępny poprzez przeglądarkę Web ma umożliwiać zarządzanie programem również wtedy, gdy przeglądarka nie obsługuje kodu JavaScript
35. Możliwość stworzenia lokalnego repozytorium aktualizacji dla przynajmniej dwóch różnych produktów antywirusowych instalowanych na stacjach Windows
36. Możliwość tworzenia osobnych ustawień skanowania dla poszczególnych użytkowników w systemie
37. Możliwość definicji użytkownika systemowego z prawami którego zostanie uruchomiony demon skanujący
38. Współpraca z mechanizmem automatycznej wysyłki podejrzanych plików do laboratorium producenta
39. Wysyłka podejrzanych plików ma być możliwa bezpośrednio do producenta lub za pośrednictwem serwera zdalnego zarządzania
40. Możliwość uaktywnienia dodatkowych funkcjonalności programu (moduł skanujący pocztę e-mail oraz moduł skanujący dla bramek sieciowych) które nie wymagają od użytkownika instalacji dodatkowych zależności ani modułów a jedynie załadowanie dodatkowych plików licencji
41. Możliwość instalacji na dowolnym systemie Linux 2.2.x, 2.4.x, 2.6.x
42. Producent ma dostarczyć pakiety instalacyjne w formacie RPM (dla dystrybucji Red Hat Mandriva, Suse oraz innych z nimi zgodnych), DEB (dla dystrybucji Debian, Ubuntu oraz innych z nimi zgodnych) oraz archiwum TGZ dla wszystkich pozostałych

43. Możliwość instalacji na systemie FreeBSD 5.x, 6.x i 7.x
44. Możliwość instalacji na systemach NetBSD.
45. Wsparcie dla platform 32 oraz 64 bitowych
46. Architektura programu umożliwia jego uruchomienie i optymalizację zarówno dla systemów jedno jak i wieloprocesorowych
47. System ma mieć możliwość powiadomienia administratora o wykryciu infekcji oraz powiadomienia o zbliżającym się terminie wygaśnięcia licencji za pośrednictwem poczty e-mail.
48. Możliwość szybkiej konfiguracji oprogramowania poprzez skrypt powłoki. Skrypt umożliwia prostą konfigurację oprogramowania stosownie do wykrytego systemu operacyjnego w jakim oprogramowanie zostało zainstalowane.
49. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

Ochrona serwera plików Windows

1. Wsparcie dla systemów: Microsoft Windows Server 2003, 2008, 2008 R2, 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.
5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
6. 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).
7. System antywirusowy ma mieć możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
8. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych.
9. Możliwość skanowania dysków sieciowych i dysków przenośnych.
10. Skanowanie plików spakowanych i skompresowanych.
11. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
12. System antywirusowy ma automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
13. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony.
14. Dodanie automatycznych wyłączeń nie wymaga restartu serwera.
15. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych.
16. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji.
17. W przypadku restartu serwera – usunięte z listy wyłączeń elementy mają być automatycznie uzupełnione.
18. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego.
19. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line).
20. 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.
21. Wbudowane dwa niezależne moduły heurystyczne.
22. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
23. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
24. Możliwość automatycznego wysyłania powiadomienia o wykrytych zagrożeniach do dowolnej stacji roboczej w sieci lokalnej.
25. Interfejs programu ma oferować funkcję pracy w trybie bez grafiki gdzie cały interfejs wyświetlany jest w formie formatek i tekstu.

26. 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.
27. 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.
28. 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.
29. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku i pracować w trybie graficznym
30. 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.
31. Funkcja generująca taki log ma oferować kilka poziomów filtrowania wyników
32. 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.
33. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
34. 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).
35. Do każdego zadania aktualizacji można przypisać dwa różne profile z innym ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja).
36. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
37. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania.
38. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

Konsola zdalnej administracji

1. Centralna instalacja i zarządzanie programami służącymi do ochrony stacji roboczych Windows/Linux desktop
2. Do instalacji centralnej i zarządzania centralnego nie jest wymagany dodatkowy agent. Na końcówkach zainstalowany jest sam program antywirusowy
3. Kreator konfiguracji zapory osobistej stacji klienckich pracujących w sieci, umożliwiający podgląd i utworzenie globalnych reguł w oparciu o reguły odczytane ze wszystkich lub z wybranych komputerów lub ich grup.
4. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej
5. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu.
6. Możliwość skanowania sieci z centralnego serwera zarządzającego w poszukiwaniu niezabezpieczonych stacji roboczych.
7. Możliwość importowania konfiguracji programu z wybranej stacji roboczej a następnie przesłanie (skopiowanie) jej na inną stację lub grupę stacji roboczych w sieci.
8. Możliwość zmiany konfiguracji na stacjach z centralnej konsoli zarządzającej lub lokalnie (lokalnie tylko, jeżeli ustawienia programu nie są zabezpieczone hasłem lub użytkownik/administrator zna hasło zabezpieczające ustawienia konfiguracyjne).
9. Możliwość uruchomienia serwera centralnej administracji i konsoli zarządzającej na stacjach Windows Microsoft Windows 8 / 7 / Vista / XP / 2000, Windows Server 2003, 2008, 2008 R2, 2012.
10. Możliwość wymuszenia konieczności uwierzytelniania stacji roboczych przed połączeniem się z serwerem zarządzającym. Uwierzytelnianie przy pomocy zdefiniowanego na serwerze hasła.

11. Do instalacji serwera centralnej administracji nie jest wymagane zainstalowanie żadnych dodatkowych baz typu MSDE lub MS SQL. Serwer centralnej administracji musi mieć własną wbudowaną bazę w pełni kompatybilną z formatem bazy danych programu Microsoft Access.
12. Serwer centralnej administracji ma oferować administratorowi możliwość współpracy przynajmniej z trzema zewnętrznymi motorami baz danych w tym minimum z: Microsoft SQL Server, MySQL Server oraz Oracle.
13. Do instalacji serwera centralnej administracji nie jest wymagane zainstalowanie dodatkowych aplikacji takich jak Internet Information Service (IIS) czy Apache.
14. Aplikacja musi posiadać funkcjonalność, generowania raportów oraz umożliwiać ich przesłanie na wskazany adres email.
15. Do wysłania raportów aplikacja nie może wykorzystywać klienta pocztowego zainstalowanego na stacji gdzie jest uruchomiona usługa serwera.
16. Możliwość tworzenia hierarchicznej struktury serwerów zarządzających i replikowania informacji pomiędzy nimi w taki sposób, aby nadrzędny serwer miał wgląd w swoje stacje robocze i we wszystkie stacje robocze serwerów podrzędnych (struktura drzewiasta).
17. Serwer centralnej administracji ma umożliwiać definiowanie różnych kryteriów wobec podłączonych do niego klientów (w tym minimum przynależność do grupy roboczej, przynależność do domeny, adres IP, adres sieci/podsieci, zakres adresów IP, nazwa hosta, przynależność do grupy, brak przynależności do grupy). Po spełnieniu zadanego kryterium lub kilku z nich stacja ma otrzymać odpowiednią konfigurację.
18. Serwer centralnej administracji ma być wyposażony w wygodny mechanizm zarządzania licencjami, który umożliwi sumowanie liczby licencji nabytych przez użytkownika oraz poinformuje administratora w przypadku wykorzystania wszystkich licencji.
19. Aplikacja musi posiadać funkcjonalność, która umożliwi dystrybucję aktualizacji za pośrednictwem protokołu http oraz https.
20. Do celu aktualizacji za pośrednictwem protokołu https nie jest wymagane instalowanie dodatkowych zewnętrznych usług jak IIS lub Apache zarówno od strony serwera aktualizacji jak i klienta.
21. Dostęp do kwarantanny klienta ma być możliwy z poziomu systemu centralnego zarządzania.
22. Administrator ma mieć możliwość przywrócenia i wyłączenia ze skanowania pliku pobranego z kwarantanny stacji klienckiej.
23. Podczas przywracania pliku, administrator ma mieć możliwość zdefiniowania kryteriów dla plików, które zostaną przywrócone w tym minimum: zakres czasu z dokładnością co do minuty kiedy wykryto daną infekcję, nazwa danego zagrożenia, dokładna nazwa wykrytego obiektu oraz zakres minimalnej i maksymalnej wielkości pliku z dokładnością do jednego bajta.
24. W przypadku tworzenia administratora z niestandardowymi uprawnieniami możliwość wyboru modułów, do których ma mieć uprawnienia.
25. Wszystkie działania administratorów zalogowanych do serwera administracji centralnej mają być logowane.
26. Możliwość uruchomienia panelu kontrolnego dostępnego za pomocą przeglądarki internetowej.
27. Panel kontrolny musi umożliwiać administratorowi wybór elementów monitorujących, które mają być widoczne.
28. Możliwość włączenia opcji pobierania aktualizacji z serwerów producenta z opóźnieniem.
29. Możliwość przywrócenia baz sygnatur wirusów wstecz (tzw. Rollback).
30. Aplikacja musi mieć możliwość przygotowania paczki instalacyjnej dla stacji klienckiej, która będzie pozbawiona wybranej funkcjonalności.