Załącznik nr 4 do SWZ - Opis Przedmiotu zamówienia

Dotyczy postępowania o udzielenie zamówienia publicznego prowadzonego w trybie podstawowym zgodnie z art. 275 pkt 1 ustawy PZP**, na zakup, dostawę, instalację oraz wdrożenie systemu ochrony antywirusowej dla Szpitala Wojewódzkiego im. Kardynała Stefana Wyszyńskiego w Łomży, znak sprawy: ZT-SZP-226/01/61/2022.**

Opis Przedmiotu zamówienia

Opis systemu ochrony antywirusowej z zaporą ogniową **dla 755 szt**. stacji roboczych, urządzeń mobilnych oraz serwerów wraz z centralną konsolą zarządzającą.

1. Ochrona antywirusowa stacji roboczych:
   - Microsoft Windows 7 (32/64-bit);
   - Microsoft Windows 8.1 (32/64-bit);
   - Microsoft Windows 10 (32/ 64-bit);
   - Microsoft Windows 11 (32/ 64-bit).

2. Ochrona antywirusowa serwerów:
   - Microsoft Windows Server 2008 R2;
   - Microsoft Small Business Server 2011, Standard Edition;
   - Microsoft Small Business Server 2011, Essentials;
   - Microsoft Windows Server 2012;
   - Microsoft Windows Server 2012 Essentials;
   - Microsoft Windows Server 2012 R2;
   - Microsoft Windows Server 2012 R2 Essentials;
   - Microsoft Windows Server 2012 R2 Foundation;
   - Microsoft Windows Server 2016 Standard;
   - Microsoft Windows Server 2016 Essentials;
   - Microsoft Windows Server 2016 Datacenter;
   - Microsoft Windows Server 2016 Core;
   - Microsoft Windows Server 2019 Standard;
   - Microsoft Windows Server 2019 Essentials;
   - Microsoft Windows Server 2019 Datacenter;
   - Microsoft Windows Server 2019 Core;
   - Microsoft Windows Server 2022 Standard;
   - Microsoft Windows Server 2022 Essentials;
   - Microsoft Windows Server 2022 Datacenter;
   - Microsoft Windows Server 2022 Core.

   Dodatkowo wspierane serwery terminalowe:
   - Microsoft Windows Terminal/RDP Services;
   - Citrix XenApp 5.0;

- Citrix XenApp 6.0;
- Citrix XenApp 6.5;
- Citrix XenApp 7.0 - 7.15.

3. Ochrona antywirusowa wyżej wymienionego systemu monitorowana i zarządzana z pojedynczej, centralnej konsoli.
4. Komunikacja ochrony antywirusowej z serwerem zarządzania musi odbywać się za pomocą protokołu HTTPS.
5. Możliwość instalacji konsoli zarządzania niezależnie na kilku wybranych stacjach.
6. Polski interfejs użytkownika aplikacji ochronnej.

Opis technologii:

1. Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanowania heurystycznego, modułu skanującego nośniki i monitora poczty elektronicznej, monitora ruchu http oraz modułu antyrootkit i modułu antyransonmware.
2. Co najmniej trzy różne silniki antywirusowe, funkcjonujące jednocześnie i skanujące wszystkie dane.
3. Oddzielny silnik skanujący do wykrywania niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan".
4. Instalator oprogramowania na stacji końcowej musi sprawdzać istnienie poprzednich wersji oprogramowania oraz oprogramowania uniemożliwiającego poprawne działanie klienta.
5. W przypadku znalezienia poprzedniej wersji oprogramowania antywirusowego instalator powinien pozostawić ustawienia użytkownika, usunąć starsze oprogramowanie klienta stacji końcowej lub serwera zarządzania i instalować nowe wersję.
6. W przypadku znalezienia oprogramowania uniemożliwiającego poprawne działanie klienta, instalator powinien poinformować o tym użytkownika i w razie akceptacji usunąć takie oprogramowanie.
7. Możliwość zdefiniowania automatycznego procesu usuwania oprogramowania uniemożliwiającego poprawne działanie klienta, bez informowania użytkownika końcowego.
8. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa musi być zarówno aktualizacja automatyczna programu oraz na żądanie przez wywołanie funkcji w interfejsie lokalnym oprogramowania.
9. Możliwość dystrybuowania aktualizacji baz definicji wirusów, aktualizacji oprogramowania zainstalowanego na stacji końcowej, oraz polityk bezpieczeństwa za pomocą serwera pośredniczącego. Serwer pośredniczący pobiera aktualizacje oprogramowania, jak i bazy antywirusowe, z serwerów producenta, a następnie dystrybuuje je w sieci lokalnej.
10. Możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli lub lokalnie przez określonego klienta.

11. Możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.
12. Możliwość wywołania skanowania po uruchomieniu systemu operacyjnego, oraz po zalogowaniu użytkownika.
13. Możliwość wywołania procesu skanowania z niskim priorytetem, co pozwala na skanowanie z użyciem mniejszej ilości zasobów systemowych.
14. Możliwość wywołania skanowania uwzględnionych rozszerzeń a także ich wykluczanie.
15. Możliwość skanowania dysków przenośnych takich jak dyski USB, dyski zewnętrzne, drukarki czy dyski sieciowe.
16. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie.
17. Skanowanie na żądanie pojedynczych plików, katalogów, napędów przy pomocy skrótu w menu kontekstowym.
18. Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).
19. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
20. Heurystyczna technologia do wykrywania nowych, nieznanych wirusów.
21. Wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan", „rootkit" oraz ataki typu 0-day.
22. Mechanizm wykrywania nowych i nieznanych zagrożeń (0-day), bazujący na technologii chmurowej, analizującej podejrzane pliki wykonywalne (przez pliki wykonywalne rozumie się co najmniej: aplikacje, interpretowalną zawartość Flash, Sliverlight, skrypty oraz makra dokumentów pakietu Office).
23. Technologia wykrywania nowych i nieznanych zagrożeń typu 0-day, powinna w głównej mierze bazować na metadanych na temat analizowanego pliku. Pliki sklasyfikowane jako bezpieczne, nie mogą być wysyłane do analizy w infrastrukturze producenta.
24. Technologia wykrywania nowych i nieznanych zagrożeń, powinna w przypadku podejrzanych plików umożliwiać automatyczne ładowanie ich do systemu sandbox, utrzymywanego w infrastrukturze dostawcy oprogramowania antywirusowego w celu przeprowadzenia dodatkowej strukturalnej i behawioralnej analizy podejrzanego pliku.
25. Możliwość wyłączenia mechanizmu automatycznego przesyłania podejrzanych plików do dodatkowej analizy przez producenta.
26. Możliwość umieszczenia oprogramowania typu „spyware", „adware", „keylogger", „dialer", „trojan" w kwarantannie.
27. Mechanizm określania źródeł ataków prowadzonych przy użyciu zagrożeń hybrydowych, takich jak Code Red i Nimda.
28. Obsługa plików skompresowanych obejmująca najpopularniejsze formaty w tym, co najmniej: ZIP, JAR, ARJ, LZH, TAR, TGZ, GZ, CAB, RAR, BZ2, HQX.

29. Automatyczne usuwanie wirusów oraz oprogramowania typu malware i zgłaszanie alertów w przypadku wykrycia wirusa.
30. Logowanie historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów z poziomu GUI aplikacji.
31. Automatyczne uruchamianie procedur naprawczych.
32. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
33. Automatyczne powiadomienie użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem stacja robocza jest odpowiednio zabezpieczona.
34. Możliwość wyłączenia powiadomień dla użytkowników stacji końcowej o wykrytych zagrożeniach.
35. Skanowanie przez program na komputerze klienckim, danych pobieranych i wysyłanych danych przy pomocy protokołu http.
36. Blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.
37. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez system reputacyjny producenta.
38. Ochrona przeglądarki internetowej, w tym: analiza uruchamianych skryptów ActiveX i pobieranych plików.
39. Ochrona podczas przeglądania sieci Internet na podstawie badania reputacji – moduł działający na bazie *Network Interceptor Framework* (niezależnie od rodzaju i wersji przeglądarki).
40. Możliwość zabezpieczenia połączenia do witryn skategoryzowanych przez producenta, jako ‘bankowość elektroniczna’ poprzez uniemożliwienie nawiązania nowych sesji do niezaufanych hostów na czas połączenia z bankiem.
41. Kontrola połączenia umożliwia zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora poprzez uniemożliwienie nawiązania nowych sesji do niezaufanych hostów na czas połączenia z daną witryną HTTPS.
42. Możliwość blokowania uruchomienia aplikacji na stacji końcowej.
43. Blokowanie możliwości uruchomienia aplikacji na stacji końcowej musi umożliwiać identyfikację aplikacji, co najmniej na podstawie identyfikatora SHA1.
44. Możliwość zarządzania zaporą ogniową (tzw. personal firewall) wbudowaną w system Windows, z możliwością definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup roboczych.
45. Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.
46. Możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej).
47. Blokowanie dostępu do kategorii witryn WWW skatalogowanych przez systemy reputacyjne producenta. Brak konieczności ręcznego wpisywania poszczególnych adresów.

48. Oprogramowanie musi zapewnić co najmniej 30 kategorii klasyfikacji witryn WWW.
49. Użytkownik podczas próby przejścia na witrynę znajdująca się w zablokowanej przez Administratora kategorii, musi zostać powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej.
50. Możliwość blokowania witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS.
51. Brak konieczności restartu systemu operacyjnego po zainstalowaniu aplikacji w środowisku Windows 7/8/8.1/10/11.
52. Komunikacja pomiędzy serwerem centralnego zarządzania a stacjami roboczymi musi odbywać się w formie zaszyfrowanej.
53. Moduł aktualizatora aplikacji, który okresowo skanuje aplikacje zainstalowane na stacji roboczej i umożliwia ich aktualizację do najnowszych wersji.
54. Aktualizator aplikacji musi spełniać role programu łatającego podatności i instalującego aktualizacje oprogramowania, a nie tylko i wyłącznie pasywnego skanera luk w bezpieczeństwie aplikacji.
55. Administrator ma możliwość zdefiniowania aplikacji, które nie podlegają aktualizacji, poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej.
56. System centralnego zarządzania musi prezentować niezaktualizowane aplikacje na komputerach dotyczące całej domeny lub listę nieaktualizowane oprogramowania dla pojedynczej stacji końcowej.
57. Aktualizator aplikacji nie może wymagać instalowania dodatkowych agentów oprócz agenta AV (systemu antywirusowego).
58. Aktualizator powinien dać możliwość wymuszenia instalacji aktualizacji w sposób akcji wymuszonej z poziomu interfejsu zarządzania lub reguły wykonującej się w sposób zaplanowany: dzień, godzina, opcje restartu komputera, wykluczenia aplikacji.
59. Administrator konsoli zarządzającej musi mieć możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji.
60. Aktualizator aplikacji nie wymaga uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces.
61. Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.
62. Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej.
63. Istnieje możliwość blokady zapisywania plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta musi umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach.
64. Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.

65. Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.
66. Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.
67. Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną antyransomware.
68. Wsparcie Antimalware Scan Interface (AMSI).
69. Możliwość ukrycia programu z zasobnika systemowego dla użytkowników końcowych.
70. Ochrona plików programu przed naruszeniem
71. Możliwość ustalenia hasła, które umożliwia zwolnienie plików z kwarantanny przez użytkownika, bądź całkowite zakazanie zwolnienia z kwarantanny.

Ochrona urządzeń Mac

1. Ochrona antywirusowa komputerów musi komunikować się z systemem centralnego zarządzania oprogramowaniem AV.
2. Oprogramowanie musi być kompatybilne z następującymi systemami operacyjnymi:
    - mac OS 10.15 Catalina
    - mac OS 10.14 Mojave
    - mac OS 10.13 High Sierra
    - mac OS 11.0 Big Sur

Ochrona urządzeń mobilnych z systemami Android, iOS i iPadOS

1. Ochrona antywirusowa urządzeń mobilnych musi komunikować się z systemem centralnego zarządzania oprogramowaniem AV.
2. Oprogramowanie musi być kompatybilne z następującymi systemami operacyjnymi:
    - Android 7.0 i wyższe wersje
    - iOS 12.1 i wyższe wersje
    - iPadOS 13 i wyższe wersje.
3. **W ramach oferowanych 755 szt. licencji na urządzenia, 55 szt. licencji musi być dedykowanych dla urządzeń mobilnych z systemami opisanymi w ust. 2.**
4. Aplikacja na urządzenia mobilne musi wspierać działanie z rozwiązaniami MDM co najmniej: AirWatch, IBM MaaS360, Google MDM, Microsoft Intune, Miradore, MobileIron.
5. Wdrożenie oprogramowania ma działać na zasadzie zaproszeń e-mail wysyłanych do użytkowników końcowych.
6. Program musi zawierać funkcjonalność ochrony przeglądania zapobiegającą odwiedzaniu szkodliwych stron internetowych, także z wsparciem HTTPS.
7. Aplikacja musi posiadać funkcjonalność VPN z możliwością wyboru wirtualnej lokalizacji sieciowej z możliwością ograniczenia listy lokacji przez administratora.

8. Wspierane lokacje VPN to co najmniej: Espoo, Sztokhol, Oslo, Kopenhaga, Madryt, Warszawa, Paryż, Bruksela, Amsterdam, Milan, Falkenstein, Londyn, Wschodnie wybrzeżę USA, Zachodnie wybrzeże USA, Montreal, Tokyo, Melborune.
9. Administrator musi posiadać możliwość wybrania aplikacji które pomijają VPN.
10. Dla systemów firmy Apple administrator musi posiadać możliwość wyboru protokołu VPN między IKEv1, IKEv2 bądź wybór automatyczny.
11. Produkt musi zawierać funkcjonalność Anti-Tracking, która zapobiega śledzeniu przez reklamodawców, oraz przez pliki cookie.
12. Dla systemu Android produkt musi zawierać lekki moduł ochrony przed złośliwym oprogramowaniem, który blokuje wirusy, malware oraz wykrywa ransomware.
13. Administrator musi posiadać możliwość regulowania skanowania w wypadku połączenia sieciowego z limitem użycia danych.
14. Administrator musi posiadać możliwość zaplanowania skanowania antywirusowego w czasie codziennym, co tydzień, co cztery tygodnie bądź miesięcznie.
15. Administrator musi posiadać możliwość zablokowania każdej opcji konfiguracyjnej przed modyfikacją przez użytkownika.

Opis systemu centralnego zarządzania:

1. System centralnego zarządzania w języku polskim.
2. System centralnego zarządzania może być zainstalowany na wersjach serwerowych Microsoft Windows lub Linux.
3. Instalacja sytemu centralnego zarządzania dla Microsoft Windows musi wspierać następujące wersje systemów operacyjnych:
   - Windows Server 2008 SP1 64-bit: Standard, Enterprise, Web Server, Small Business Server, Essential Business Server;
   - Windows Server 2008 R2: Standard, Enterprise, Web Server;
   - Windows Server 2012: Essentials, Standard, Datacenter;
   - Windows Server 2012 R2: Essentials, Standard, Datacenter;
   - Windows Server 2016 Essentials, Standard, Datacenter;
   - Windows 2019 Essentials, Standard, Datacenter;
   - Windows 2022 Essentials, Standard, Datacenter.

4. Instalacja sytemu centralnego zarządzania dla Linux musi wspierać następujące wersje systemów operacyjnych:
   - Red Hat Enterprise Linux 6 32/64-bit;
   - Red Hat Enterprise Linux 7 32/64-bit;
   - Red Hat Enterprise Linux 8 32/64-bit;
   - CentOS 6 32/64-bit;
   - CentOS 7 32/64-bit;
   - CentOS 8 32/64-bit;

- SuSE Linux Enterprise Server 11 32/64-bit;
- SuSE Linux Enterprise Server 12 32/64-bit;
- SuSE Linux Enterprise Server 15 32/64-bit;
- SuSE Linux Enterprise Desktop 11, 12, 15 32/64-bit;
- openSUSE Leap 43.15 32/64-bit;
- Debian GNU Linux 8 (Jessie) 32/64-bit;
- Debian GNU Linux 9 (Stretch) 32/64-bit;
- Ubuntu 14.04 (Trusty Tahr) 32/64-bit;
- Ubuntu 16.04 (Xenial Xerus) 32/64-bit;
- Ubuntu 18.04 (Bionic Beaver) 32/64-bit;
- Ubuntu 20.04 (Focal Fossa) 32/64-bit;
- Oracle Linux 8.

5. System centralnego zarządzania musi wspierać następujące przeglądarki internetowe do obsługi konsoli zarządzającej:
   - Microsoft Edge
   - Mozilla Firefox
   - Google Chrome
   - Safari.
6. Interfejs zarządzania posiada funkcję wyświetlania monitów o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.
7. Interfejs jest wyposażony w panel kontrolny zawierający podsumowanie stanu bezpieczeństwa organizacji w postaci graficznych wykresów.
8. Wykresy są interaktywne, tzn. że po wybraniu interesującego elementu, następuje przekierowanie do zawierającego bardziej szczegółowe dane menu.
9. Rozwiązanie posiada dedykowaną zakładkę zawierającą informację o wszystkich hostach posiadających zainstalowane oprogramowanie do ochrony, w tym: ich nazwy, status ochrony, przypisany profil bezpieczeństwa.
10. Istnieje możliwość eksportu listy wszystkich hostów do pliku CSV.
11. Administrator ma możliwość wglądu w szczegóły zgłaszającego się hosta, w których zawarte są informacje dotyczące: ostatniego podłączenia do konsoli zarządzającej, wersji zainstalowanego produktu, systemu operacyjnego, stanu ochrony, akcji związanych z wykrytymi zagrożeniami i skanowaniami.
12. Pełna administracja konfiguracją i monitorowanie stacji roboczych i serwerów plików za pomocą konsoli administracyjnej (centralna instalacja, konfiguracja w czasie rzeczywistym, zarządzanie, raportowanie i administrowanie oprogramowaniem).
13. Komunikacja pomiędzy serwerem centralnego zarządzania a stacjami roboczymi musi być zaszyfrowana lub sygnowana stosownymi kluczami prywatnymi i publicznymi.
14. Scentralizowane blokowanie i odblokowywanie dostępu użytkownika do zmian konfiguracyjnych oprogramowania klienckiego, konsola pozwala na zdalne zarządzanie wszystkimi ustawieniami klienta.

15. Administratorzy muszą mieć możliwość tworzenia logicznych grup klientów i serwerów, w celu zarządzania oraz wymuszania określonych dla grupy zasad bezpieczeństwa.
16. Centralna konsola administracyjna musi umożliwiać przenoszenie klientów z jednej grupy do drugiej z możliwością zachowania ustawień lub dziedziczenia ustawień grupy.
17. Możliwość zmiany ustawień dla poszczególnych grup, umożliwienie administratorom zarządzania poszczególnymi klientami i funkcjonalnymi grupami klientów (tworzenie grup klientów).
18. Tworzenie grup, zdalne instalowanie oprogramowania oraz wymuszanie stosowania określonych zasad i ustawień na klientach.
19. Możliwość importu struktury drzewa z Microsoft Active Directory.
20. Możliwość tworzenia reguł synchronizacji z Microsoft Active Directory umożliwiających automatyczną synchronizację klientów z aktualnie istniejącymi grupami komputerów.
21. Możliwość tworzenia reguł powiadamiania o nowych, niezarządzanych klientach w Microsoft Active Directory.
22. Możliwość blokowania wszystkich ustawień konfiguracyjnych stacji roboczych w celu uniemożliwienia ich modyfikacji przez użytkowników.
23. Możliwość zdefiniowania hasła do odinstalowania aplikacji.
24. Możliwość definiowania harmonogramów lub częstotliwości automatycznego pobierania aktualizacji definicji wirusów od producenta oprogramowania przez serwer zarządzający.
25. Możliwość instalacji i konfiguracji wewnętrznego serwera aktualizacji, łączącego się z serwerem aktualizacji producenta i aktualizacja serwerów, serwera zarządzającego oraz stacji roboczych z wewnętrznego serwera aktualizacji.
26. Możliwość ustalenia dodatkowego harmonogramu pobierania przez serwery plików i stacje robocze aktualizacji z serwera producenta.
27. Funkcja przechowywania i przekazywania danych umożliwiająca przechowywanie przez klientów danych dotyczących zdarzeń, w sytuacji, jeśli nie mogą oni uzyskać połączenia z serwerem zarządzania. Dane muszą być przesyłane do serwera zarządzania podczas kolejnego połączenia.
28. Możliwość włączania/wyłączania wyświetlania komunikatów o znalezionych wirusach na wybranych stacjach klienckich.
29. Rozwiązanie ma możliwość definiowania różnych profili ustawień dla chronionych urządzeń z poziomu portalu zarządzającego.
30. Profile mogą być przypisane do pojedynczych hostów lub do grup.
31. Rozwiązanie pozwala administratorowi podczas tworzenia profili wskazanie funkcjonalności, które mogą być zmieniane przez użytkownika od strony chronionego hosta – możliwość wprowadzanych zmian jest do określenia dla poszczególnych funkcji programu oraz całości konfiguracji.
32. Tworzone profile muszą dawać administratorowi możliwość blokowania ustawień konfiguracyjnych aplikacji zainstalowanych od strony stacji roboczych w celu uniemożliwienia ich modyfikacji przez lokalnego użytkownika.

33. W ramach posiadanych licencji istnieje możliwość przenoszenia oprogramowania w ramach danego klucza subskrypcji z jednej stacji roboczej na inną.
34. Umożliwienie administratorom na audyt sieci, polegający na wykryciu niechronionych węzłów narażonych na ataki wirusowe.
35. Automatyczne uaktualnianie bazy definicji wirusów oraz mechanizmów skanujących nie rzadziej, niż co 7 dni (zalecane codzienne aktualizacje).
36. Automatyczne pobieranie przez program antywirusowy klienta zaktualizowanych definicji wirusów, jeśli aktualnie przechowywane pliki są przestarzałe.
37. Możliwość eksportu raportów z pracy systemu do pliku HTML.
38. Możliwość natychmiastowej aktualizacji przez serwer definicji wirusów na stacjach klienckich.
39. Możliwość uruchomienia aktualizacji stacji roboczych i serwerów przez użytkowników „na żądanie”.
40. Program musi pozwalać administratorowi na określenie reakcji w przypadku wykrycia wirusa.
41. Program musi pozwalać na określenie obszarów skanowania, tj.: pliki, katalogi, napędy lokalne i sieciowe.
42. Dedykowany system raportowania dostępny przez przeglądarkę internetową umożliwiający podgląd statystyk dotyczących wykrytych wirusów, przeprowadzonych ataków, zainstalowanego oprogramowania oraz statystyk połączenia stacji klienckich.
43. System raportowania umożliwiający wysyłanie raportów poprzez pocztę elektroniczną zgodnie z harmonogramem określonym przez administratora.
44. Zarządzanie zdarzeniami i raportowanie – natychmiastowe alarmowanie o aktywności wirusów w administrowanej sieci na kilka sposobów: poczta elektroniczna, powiadomienia przez SNMP, raportowanie do dziennika systemowego, raportowanie do systemu centralnego zarządzania.
45. Możliwość przekierowania alertów bezpośrednio do serwera Syslog.
46. Możliwość tworzenia wielu kont dostępu do systemu centralnego zarządzania dla różnych użytkowników (w tym możliwość nadaniu danemu użytkownikowi ograniczonych praw).
47. System umożliwiający wykonanie pełnej kopii bazy danych systemu zarządzania centralnego bez konieczności ręcznego wyłączania programu.
48. Możliwość wykonywania automatycznej kopii bazy danych systemu zarządzania centralnego zgodnie z harmonogramem określonym przez administratora.
49. Możliwość określenia liczby kopii bazy danych, jaka będzie przetrzymywana przez automatyczny system tworzenia kopii zapasowej.
50. Możliwość wygenerowania danych diagnostycznych z podpiętych komputerów za pomocą konsoli zarządzającej.
51. Możliwość bezpośredniego pobrania z komputera danych diagnostycznych z poziomu konsoli zarządzającej.
52. Możliwość komentowania stosowanej konfiguracji stacji końcowych za pomocą notatek umieszczonych w interfejsie graficznym konsoli zarządzającej.
53. Wsparcie REST API dla integracji z rozwiązaniami monitorowania i raportowania.