Wymagania dotyczące system ochrony anty wirusowej z zaporą ogniową dla stacji roboczych.

1. Ochrona antywirusowa stacji roboczych:
   - Microsoft Windows 7 (32-bit i 64-bit)
   - Microsoft Windows 8 (32-bit i 64-bit)
   - Microsoft Windows 8.1 (32-bit i 64-bit)
   - Microsoft Windows 10 (32-bit i 64-bit)
   - macOS version 10.12 "Sierra"
   - OS X version 10.11 "El Capitan"
   - OS X version 10.10 "Yosemite"
2. Ochrona antywirusowa wyżej wymienionego systemu monitorowana i zarządzana z pojedynczej, centralnej konsoli.
3. Komunikacja ochrony antywirusowej z serwerem zarządzania musi odbywać się za pomocą protokołu HTTPS.
4. Możliwość instalacji konsoli zarządzania niezależnie na kilku wybranych stacjach.
5. Polski interfejs użytkownika aplikacji ochronnej.

Wymagania dotyczące technologii:

1. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie, jak i ściągnięcie pliku offline ze strony producenta i ręczna aktualizacja na stacjach roboczych bez dostępu do Internetu.
2. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie.
3. 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).
4. Możliwość pobierania aktualizacji definicji wirusów bezpośrednio z serwerów producenta, centralnej konsoli, dedykowanego proxy lub z innej stacji roboczej gdzie zainstalowane jest oprogramowanie antywirusowe.
5. Dedykowany protokół umożliwiający współdzielenie aktualizacji pomiędzy stacjami roboczymi znajdującymi się w sieci LAN.
6. Możliwość ręcznego aktualizowania baz definicji wirusów poprzez odrębny plik wykonywalny dostarczony przez producenta.
7. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
8. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
9. Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanowania heurystycznego, monitora poczty elektronicznej, monitora ruchu http oraz monitora kontrolującego nośniki wymienne.
10. Co najmniej trzy różne silniki antywirusowe, funkcjonujące jednocześnie i skanujące wszystkie dane.

11. Oddzielny silnik skanujący do wykrywania niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger”, „dialer”, „trojan”.
12. Możliwość umieszczenia oprogramowania typu „spyware", „adware", „keylogger”, „dialer”, „trojan” w kwarantannie.
13. Mechanizm centralnego zarządzania elementami kwarantanny znajdującymi się na stacjach klienckich.
14. Program musi pozwalać na skanowanie pojedynczych plików przez dodanie odpowiedniej opcji do menu kontekstowego (po kliknięciu prawym przyciskiem myszy).
15. Program musi pozwalać na określenie typów skanowanych plików, momentu ich skanowania (otwarcie, modyfikacja) oraz na wykluczenie ze skanowania określonych folderów.
16. Automatyczne usuwanie wirusów oraz oprogramowania typu malware i zgłaszanie alertów w przypadku wykrycia wirusa.
17. Możliwość określenia akcji automatycznie podejmowanej podczas wykrycia infekcji.
18. Obsługa plików skompresowanych obejmująca najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2.
19. Możliwość określenia poziomu zagnieżdżenia skanowanych plików skompresowanych.
20. Logowanie historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów z poziomu GUI aplikacji.
21. Automatyczne uruchamianie procedur naprawczych.
22. Automatyczne powiadomienie użytkowników oraz administratora o wykrytych zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona.
23. Ochrona pliku ‘hosts’ przed niepożądanymi wpisami.
24. Możliwość wywołania skanowania komputera na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów za pomocą centralnej konsoli lub lokalnie przez określonego klienta.
25. Możliwość wywołania skanowania komputera w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.
26. Możliwość wywołania skanowania podczas uruchamiania systemu operacyjnego lub po zalogowaniu użytkownika.
27. Heurystyczna technologia do wykrywania nowych, nieznanych wirusów.
28. Skanowanie uruchamianych procesów pod kątem podejrzanego wpływu na działanie systemu operacyjnego.
29. Ochrona rejestrów systemowych, w tym odpowiedzialnych za konfigurację przeglądarki Internet Explorer, listę uruchamianych aplikacji przy starcie, przypisania rozszerzeń plików do zadanych aplikacji.
30. Skanowanie przez program na komputerze klienckim przychodzącej i wychodzącej poczty elektronicznej bez konieczności instalowania dodatkowych programów/modułów.
31. Możliwość zablokowania wychodzącej wiadomości e-mail, jeżeli zostanie w niej wykryty zainfekowany załącznik.
32. Osobista zapora ogniowa z możliwością definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup roboczych.
33. Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.

34. Możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej)
35. Możliwość samodzielnego określenia usług działających na zdefiniowanych portach, a następnie wykorzystania usług w konfiguracji reguł zapory ogniowej.
36. Ochrona podczas przeglądania sieci Internet na podstawie badania reputacji – moduł działający na bazie *Network Interceptor Framework* (niezależnie od rodzaju i wersji przeglądarki).
37. Automatyczna kwarantanna blokująca ruch przychodzący i wychodzący, włączająca się w momencie, gdy stacja robocza posiada stare sygnatury antywirusowe lub wyłączone jest skanowanie w czasie rzeczywistym.
38. Kontrola oraz możliwość blokowania aplikacji próbujących uzyskać połączenie z siecią.
39. Możliwość określenia domyślnej akcji dla aplikacji próbujących uzyskać połączenia z siecią.
40. Wsparcie dla technologii Microsoft Network Access Protection (NAP)
41. Moduł aktualizatora aplikacji, który okresowo skanuje i umożliwia aktualizację do najnowszych wersji aplikacji firm trzecich.
42. Aktualizator aplikacji spełnia rolę programu łatającego podatności a nie tylko i wyłącznie pasywnego skanera luk w bezpieczeństwie aplikacji.
43. Możliwość pobierania instalatorów poprawek bezpośrednio z serwera zarządzającego.
44. Administrator ma możliwość wykluczenia aplikacji, które maja nie podlegać aktualizacji poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej.
45. System raportowania powinien pokazywać status podatności aplikacji na komputerach dotyczące całej domeny lub pojedynczych komputerów.
46. Aktualizator aplikacji nie może wymagać instalowania dodatkowych agentów oprócz agenta AV.
47. Aktualizator powinien dać możliwość aktualizacji poprawek w sposób akcji wymuszonej lub reguły wykonującej się w sposób zaplanowany: dzień, godzina, opcje restartu komputera, wykluczenia aplikacji.
48. Administrator konsoli zarządzającej powinien mieć możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji.
49. Aktualizator aplikacji nie wymaga uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces
50. Skanowanie przez program danych pobieranych i wysyłanych danych przy pomocy protokołu http.
51. Blokowanie przez program określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.
52. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez serwery reputacyjne producenta.
53. 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.
54. Możliwość zabezpieczenia połączenia do witryn skategoryzowanych przez producenta, jako ‘bankowość elektroniczna’ poprzez uniemożliwienie nawiązania nowych sesji do niezaufanych hostów na czas połączenia z bankiem.

55. 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.
56. Możliwość blokowania zapytań DNS do witryn sklasyfikowanych, jako niebezpieczne lub podejrzane.
57. Możliwość zezwolenia na zapytania DNS tylko do witryn sklasyfikowanych, jako zaufane.
58. Blokowanie dostępu do witryn WWW na podstawie dostarczonych przez producenta kategorii bez konieczności ręcznego wpisywanie poszczególnych adresów.
59. Możliwość blokowania witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS.
60. Moduł kontroli urządzeń zapewniający możliwość zezwolenia lub zablokowania dostępu do urządzeń zewnętrznych (np. napędy USB, urządzenia bluetooth, czytniki kart pamięci, napędy CD/DVD, stacje dyskietek).
61. Moduł kontroli urządzeń zarządzany z poziomu konsoli centralnego zarządzania.
62. Moduł kontroli urządzeń umożliwia dodanie ‘zaufanego urządzenia’ poprzez podanie jego identyfikatora sprzętu.
63. Możliwość określenia hasła zabezpieczającego przed odinstalowaniem aplikacji.
64. Brak konieczności restartu komputera po zainstalowaniu aplikacji w środowisku Windows Vista/7/8/8.1/10

Wymagania dotyczące systemu zarządzania centralnego:

1. System centralnego zarządzania może być zainstalowany na wersjach serwerowych Microsoft Windows oraz Linux.
2. Instalacja sytemu centralnego zarządzania dla Microsoft Windows musi wspierać następujące wersje systemów operacyjnych:
    - Microsoft Windows Server 2008 SP1: Standard, Enterprise, Web Server, Small Business Server, Essential Business Server
    - Microsoft Windows Server 2008 R2: Standard, Enterprise, Web Server
    - Microsoft Windows Server 2012: Essentials, Standard, Datacenter
    - Microsoft Windows Server 2012 R2: Essentials, Standard, Datacenter
    - Microsoft Windows Server 2016: Essentials, Standard, Datacenter
3. Instalacja sytemu centralnego zarządzania dla Linux musi wspierać następujące wersje systemów operacyjnych:
    - Red Hat Enterprise Linux 5, 6, 7
    - CentOS 6, 7
    - SuSE Linux Enterprise Server 10, 11
    - SuSE Linux Enterprise Desktop 11
    - openSUSE 13.2
    - Debian GNU Linux 7 (Wheezy)
    - Debian GNU Linux 8 (Jessie)
    - Ubuntu 12.04 (Precise Pangolin)
    - Ubuntu 14.04 (Trusty Tahr)
    - Ubuntu 16.04 (Xenial Xerus)

4. Konsola zarządzania umożliwia eksport pakietu instalacyjnego dla klienta w formacie Microsoft Installer (MSI) i JAR lub też bezpośrednią instalację zdalną nienadzorowaną.
5. Narzędzie instalacyjne musi sprawdzać istnienie poprzednich wersji oprogramowania. W przypadku znalezienia poprzedniej wersji instalator powinien pozostawić ustawienia użytkownika, usunąć starsze oprogramowanie z klienta lub serwera i instalować nowe wersję.
6. Pełna administracja konfiguracją i monitorowanie stacji roboczych i serwerów plików za pomocą konsoli administracyjnej (centralna instalacja, konfiguracja w czasie rzeczywistym, zarządzanie, raportowanie i administrowanie oprogramowaniem).
7. Komunikacja pomiędzy serwerem centralnego zarządzania a stacjami roboczymi musi być zaszyfrowana lub sygnowana stosownymi kluczami prywatnymi i publicznymi.
8. Scentralizowane blokowanie i odblokowywanie dostępu użytkownika do zmian konfiguracyjnych oprogramowania klienckiego, konsola pozwala na zdalne zarządzanie wszystkimi ustawieniami klienta.
9. Administratorzy muszą mieć możliwość tworzenia logicznych grup klientów i serwerów, w celu zarządzania oraz wymuszania określonych dla grupy zasad bezpieczeństwa.
10. Centralna konsola administracyjna musi umożliwiać przenoszenie klientów z jednej grupy do drugiej z możliwością zachowania ustawień lub dziedziczenia ustawień grupy.
11. Możliwość zmiany ustawień dla poszczególnych grup, umożliwienie administratorom zarządzania poszczególnymi klientami i funkcjonalnymi grupami klientów (tworzenie grup klientów).
12. Tworzenie grup, zdalne instalowanie oprogramowania oraz wymuszanie stosowania określonych zasad i ustawień na klientach.
13. Możliwość importu struktury drzewa z Microsoft Active Directory.
14. Możliwość tworzenia reguł synchronizacji z Microsoft Active Directory umożliwiających automatyczną synchronizację klientów z aktualnie istniejącymi grupami komputerów
15. Możliwość tworzenia reguł powiadamiania o nowych, niezarządzanych klientach w Microsoft Active Directory.
16. Możliwość blokowania wszystkich ustawień konfiguracyjnych stacji roboczych w celu uniemożliwienia ich modyfikacji przez użytkowników.
17. Możliwość zdefiniowania hasła do odinstalowania aplikacji.
18. Możliwość definiowania harmonogramów lub częstotliwości automatycznego pobierania aktualizacji definicji wirusów od producenta oprogramowania przez serwer zarządzający.
19. 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.
20. Możliwość ustalenia dodatkowego harmonogramu pobierania przez serwery plików i stacje robocze aktualizacji z serwera producenta.
21. 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.

22. Możliwość włączania/wyłączania wyświetlania komunikatów o znalezionych wirusach na wybranych stacjach klienckich.
23. Umożliwienie administratorom na audyt sieci, polegający na wykryciu niechronionych węzłów narażonych na ataki wirusowe.
24. Automatyczne wykrywanie i usuwanie oprogramowania konfliktowego podczas instalacji.
25. Automatyczne uaktualnianie bazy definicji wirusów oraz mechanizmów skanujących nie rzadziej, niż co 7 dni (zalecane codzienne aktualizacje).
26. Automatyczne pobieranie przez program antywirusowy klienta zaktualizowanych definicji wirusów, jeśli aktualnie przechowywane pliki są przestarzałe.
27. Możliwość eksportu raportów z pracy systemu do pliku HTML.
28. Możliwość natychmiastowej aktualizacji przez serwer definicji wirusów na stacjach klienckich.
29. Możliwość uruchomienia aktualizacji stacji roboczych i serwerów przez użytkowników „na żądanie”.
30. Dedykowany system raportowania dostępny przez przeglądarkę internetową umożliwiający podgląd statystyk dotyczących wykrytych wirusów, przeprowadzonych ataków, zainstalowanego oprogramowania oraz statystyk połączenia stacji klienckich.
31. System raportowania umożliwiający wysyłanie raportów poprzez pocztę elektroniczną zgodnie z harmonogramem określonym przez administratora.
32. 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.
33. Możliwość przekierowania alertów bezpośrednio do serwera Syslog.
34. Możliwość wysyłania alertów w postaci wiadomości e-mail do zdefiniowanych odbiorców.
35. Możliwość określenia rodzaju alertów jakie zostaną wysłane w postaci wiadomości e-mail.
36. Możliwość tworzenia wielu kont dostępu do systemu centralnego zarządzania dla różnych użytkowników (w tym możliwość nadaniu danemu użytkownikowi ograniczonych praw).
37. Możliwość wykorzystywania wbudowanej bazy danych lub zewnętrznej MySQL.
38. System umożliwiający wykonanie pełnej kopii bazy danych systemu zarządzania centralnego bez konieczności ręcznego wyłączania programu.
39. Pełna kopia bazy danych systemu zarządzania centralnego może być wykonywana automatycznie zgodnie z harmonogramem określonym przez administratora.
40. Administrator ma możliwość określenia liczby kopii bazy danych, jaka będzie przetrzymywana.
41. Możliwość wygenerowania danych diagnostycznych z podpiętych komputerów za pomocą konsoli zarządzającej.
42. Możliwość bezpośredniego pobrania z komputera danych diagnostycznych z poziomu konsoli zarządzającej.

43. Możliwość opisywania wprowadzonej konfiguracji za pomocą notatek umieszczonych w interfejsie graficznym konsoli zarządzającej.
44. Automatyczne powiadamianie o dostępności nowej wersji aplikacji ochronnych lub środowiska centralnego zarządzania.

Wymagania dotyczące oprogramowania antywirusowego dla systemów typu Windows serwer:

1. Ochrona serwerów:
   - Microsoft Windows Server 2008
   - Microsoft Windows Server 2008 R2
   - Microsoft Small Business Server 2008
   - 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 (SS/ESS only)
2. Ochrona całego systemu monitorowana i zarządzana z pojedynczej konsoli.
3. Zarządzanie aplikacją poprzez interfejs dostępny przez protokół HTTPS.
4. Możliwość określenia adresów sieciowych, z których można zarządzać aplikacją.
5. Możliwość określenia portu, na którym dostępny będzie interfejs zarządzający aplikacją.
6. Integracja z systemem antywirusowym dla serwerów MS Exchange dostarczanym przez producenta poprzez wspólny lokalny interfejs zarządzający.
7. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie, jak i ściągnięcie pliku offline ze strony producenta i ręczna aktualizacja na stacjach roboczych bez dostępu do Internetu.
8. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie.
9. Mikrodefinicje wirusów – przyrostowe (inkrementalne) - pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).
10. Możliwość pobierania aktualizacji definicji wirusów bezpośrednio z serwerów producenta, centralnej konsoli, dedykowanego proxy lub z innej stacji roboczej gdzie zainstalowane jest oprogramowanie antywirusowe.
11. Dedykowany protokół umożliwiający współdzielenie aktualizacji pomiędzy stacjami roboczymi znajdującymi się w sieci LAN.

12. Możliwość ręcznego aktualizowania baz definicji wirusów poprzez odrębny plik wykonywalny dostarczony przez producenta.
13. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
14. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
15. Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanowania heurystycznego oraz monitora ruchu http
16. Co najmniej trzy różne silniki antywirusowe, funkcjonujące jednocześnie i skanujące wszystkie dane.
17. Oddzielny silnik skanujący do wykrywania niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan".
18. Możliwość umieszczenia oprogramowania typu „spyware", „adware", „keylogger", „dialer", „trojan" w kwarantannie.
19. Mechanizm centralnego zarządzania elementami kwarantanny znajdującymi się na stacjach klienckich.
20. Program musi pozwalać na skanowanie pojedynczych plików przez dodanie odpowiedniej opcji do menu kontekstowego (po kliknięciu prawym przyciskiem myszy).
21. Program musi pozwalać na określenie typów skanowanych plików, momentu ich skanowania (otwarcie, modyfikacja) oraz na wykluczenie ze skanowania określonych folderów.
22. Automatyczne usuwanie wirusów oraz oprogramowania typu malware i zgłaszanie alertów w przypadku wykrycia wirusa.
23. Możliwość określenia akcji automatycznie podejmowanej podczas wykrycia infekcji.
24. Obsługa plików skompresowanych obejmująca najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2.
25. Możliwość określenia poziomu zagnieżdżenia skanowanych plików skompresowanych.
26. Logowanie historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów z poziomu GUI aplikacji.
27. Automatyczne uruchamianie procedur naprawczych.
28. Automatyczne powiadomienie użytkowników oraz administratora o wykrytych zagrożeniach wraz z określeniem czy stacja jest odpowiednio zabezpieczona.
29. Ochrona pliku 'hosts' przed niepożądanymi wpisami.
30. Możliwość wywołania skanowania komputera na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów za pomocą centralnej konsoli lub lokalnie przez określonego klienta.
31. Możliwość wywołania skanowania komputera w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.
32. Możliwość wywołania skanowania podczas uruchamiania systemu operacyjnego lub po zalogowaniu użytkownika.
33. Heurystyczna technologia do wykrywania nowych, nieznanych wirusów.
34. Skanowanie uruchamianych procesów pod kątem podejrzanego wpływu na działanie systemu operacyjnego.
35. Ochrona rejestrów systemowych, w tym odpowiedzialnych za konfigurację przeglądarki Internet Explorer, listę uruchamianych aplikacji przy starcie, przypisania rozszerzeń plików do zadanych aplikacji.

36. Moduł aktualizatora aplikacji, który okresowo skanuje i umożliwia aktualizację do najnowszych wersji aplikacji firm trzecich.
37. Aktualizator aplikacji spełnia rolę programu łatającego podatności a nie tylko i wyłącznie pasywnego skanera luk w bezpieczeństwie aplikacji.
38. Możliwość pobierania instalatorów poprawek bezpośrednio z serwera zarządzającego.
39. Administrator ma możliwość wykluczenia aplikacji, które maja nie podlegać aktualizacji poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej.
40. System raportowania powinien pokazywać status podatności aplikacji na komputerach dotyczące całej domeny lub pojedynczych komputerów.
41. Aktualizator aplikacji nie może wymagać instalowania dodatkowych agentów oprócz agenta AV.
42. Aktualizator powinien dać możliwość aktualizacji poprawek w sposób akcji wymuszonej lub reguły wykonującej się w sposób zaplanowany: dzień, godzina, opcje restartu komputera, wykluczenia aplikacji.
43. Administrator konsoli zarządzającej powinien mieć możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji.
44. Aktualizator aplikacji nie wymaga uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces
45. Ochrona podczas przeglądania sieci Internet na podstawie badania reputacji – moduł działający na bazie *Network Interceptor Framework* (niezależnie od rodzaju i wersji przeglądarki).
46. Skanowanie przez program danych pobieranych i wysyłanych danych przy pomocy protokołu http.
47. Blokowanie przez program określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.
48. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez serwery reputacyjne producenta.
49. Możliwość blokowania zapytań DNS do witryn sklasyfikowanych, jako niebezpieczne lub podejrzane.
50. Możliwość zezwolenia na zapytania DNS tylko do witryn sklasyfikowanych, jako zaufane.
51. Możliwość określenia hasła zabezpieczającego przed odinstalowaniem aplikacji.