Zał A do siwz

Specyfikacja wymaganego oprogramowania antywirusowego - stacje robocze

I. Program antywirusowy

A. Wymagania ogólne

1) Pełne wsparcie w najnowszej wersji dla systemu Windows 7/Windows 8/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) Instalator musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji.
5) Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim.
6) Skuteczność programu potwierdzona nagrodami VB100 i AV-comparatives

B. Zakres funkcjonalny programu:

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. Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania).
9. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
10. Możliwość skanowania dysków sieciowych i dysków przenośnych.
11. Skanowanie plików spakowanych i skompresowanych.
12. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
13. Wykluczenie ze skanowania musi odbywać się nie tylko po nazwie pliku ale również ma być możliwe użycie symbolu wieloznacznego „*” zastępującego dowolne znaki w ścieżce.
14. Administrator ma możliwość dodania wykluczenia po tzw. HASH’u zagrożenia, wskazującego bezpośrednio na określoną infekcję a nie konkretny plik.
15. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
16. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
17. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera.
18. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
19. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
20. 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.
21. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
22. Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
23. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
24. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
25. 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.
26. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora.
27. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
28. Program musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
29. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
30. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
31. 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.
32. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.
33. 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.
34. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
35. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.
36. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM , urządzeń przenośnych.
37. 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.
38. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia, dana funkcjonalność musi pozwalać na automatyczne wypełnienie właściwości urządzenia dla tworzonej reguły.
39. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, brak dostępu do podłączanego urządzenia.
40. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
41. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
42. Użytkownik ma posiadać możliwość takiej konfiguracji programu aby skanowanie całego nośnika odbywało się automatycznie.
43. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
44. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
45. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
46. Oprogramowanie musi posiadać zaawansowany skaner pamięci.
47. Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp.
48. 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.
49. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.
50. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami.
51. Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji program zgłosi posiadanie nieaktualnej bazy sygnatur.
52. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji.
53. Program musi być wyposażony w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback).
54. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
55. Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, kontroli stron Internetowych i kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania.
56. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
57. Program musi posiadać możliwość utworzenia z poziomu interfejsu aplikacji dziennika diagnostycznego na potrzeby pomocy technicznej.
58. Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji lub podanie klucza licencyjnego oraz możliwość aktywacji programu offline.
59. Możliwość podejrzenia licencji za pomocą, której program został aktywowany.
60. W programie musi istnieć możliwość tymczasowego wstrzymania polityk wysłanych z poziomu serwera zdalnej administracji.
61. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej.
62. Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika.
63. Aplikacja musi posiadać funkcję ręcznej aktualizacji komponentów programu.
64. 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.
65. Program musi posiadać możliwość definiowana stanów aplikacji, jakie będą wyświetlane użytkownikowi np. powiadomień o wyłączonych mechanizmach ochrony czy stanie licencji.
66. Aplikacja musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.
67. Administrator ma możliwość dodania wykluczenia na podstawie procesu, wskazującego bezpośrednio na określony plik wykonywalny.
68. Program musi oferować możliwość umieszczenia na liście wyłączeń ze skanowania wybranej ścieżki, w której znajdują się pliki i foldery, które mają zostać wyłączone ze skanowania.
69. Program musi oferować możliwość umieszczenia na liście wyłączeń ze skanowania obiektu co najmniej w oparciu o nazwę zagrożenia oraz jego lokalizację.
70. Program musi oferować możliwość umieszczenia na liście wyłączeń ze skanowania pliku, wskazując sumę kontrolną pliku (jego HASH).
71. Program musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.
72. Program musi posiadać system ochrony przed atakami sieciowymi (IDS).
73. Administrator musi posiadać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o adres IP.

II. Konsola administracyjna – zakres funkcjonalny:

1. Serwer administracyjny musi być dostarczony jako obraz maszyny wirtualnej. Wszelkie licencje wymagane do uruchomienia i użytkowania obrazu muszą być dostarczone w ramach dostawy serwera administracyjnego. Konfiguracje serwera administracyjnego wykonuje Wykonawca, dostosowując ją do potrzeb zamawiającego.
2. Serwer administracyjny musi wspierać instalację w oparciu o co najmniej bazy danych MS SQL i MySQL.
3. Konsola administracyjna musi umożliwiać podgląd szczegółów dotyczących bazy danych takich jak serwer Bazy danych, nazwę bazy danych, aktualny rozmiar bazy danych, nazwę hosta bazy danych
4. Serwer administracyjny musi oferować możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych
5. Serwer administracyjny musi oferować możliwość wykorzystania już istniejącej bazy danych MS SQL lub MySQL użytkownika.
6. Rozwiązanie ma być w pełni zgodne z rozporządzeniem RODO
7. 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.

8. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej.
9. Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy występujące w sieci.
10. Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6.
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. Serwer administracyjny musi oferować natywne wsparcie dla „VDI".
15. Jeden centralny serwer centralnego zarządzania bez względu na wielkość sieci.
16. Instalacja serwera administracyjnego powinna oferować możliwość pracy w sieci rozproszonej nie wymagając dodatkowego serwera proxy.
17. Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM.
18. Serwer administracyjny musi oferować możliwość sprawdzenia lokalizacji dla urządzeń z systemami iOS
19. Serwer administracyjny musi oferować możliwość wdrożenia urządzenia z iOS z wykorzystaniem programu DEP
20. Serwer administracyjny musi oferować możliwość konfiguracji polityk zabezpieczeń takich jak ograniczenia funkcjonalności urządzenia, blokadę usuwania aplikacji, konfigurację usługi Airprint, konfigurację ustawień Bluetooth, Wi-Fi, VPN dla urządzeń z systemem iOS 10 oraz 11
21. Serwer administracyjny musi oferować możliwość lokalizacji urządzeń mobilnych przy wykorzystaniu Map Google
22. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.
23. Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority)
24. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na stacjach roboczych z systemami Windows, Mac OS X oraz Linux oraz serwerach Windows.
25. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na urządzeniach mobilnych z systemem Android.
26. Centralna administracja musi pozwalać na zarządzanie urządzeniami mobilnymi z systemem iOS
27. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci.
28. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.
29. Administrator musi posiadać możliwość zarządzania za pomocą dedykowanego agenta stacjami nie posiadającymi zainstalowanego programu zabezpieczającego.
30. Agent musi przekazywać informacje na temat stanu systemu operacyjnego do serwera administracji zdalnej.
31. Z poziomu konsoli zarządzania administrator ma mieć możliwość weryfikacji podzespołów bazowych zarządzanego komputera oraz weryfikację zainstalowanego oprogramowania firm trzecich na stacji dla systemów Windows.
32. Serwer administracyjny musi oferować możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.
33. Konsola ma oferować możliwość aktywacji oraz wdrożenie elementów systemu EDR producenta.
34. Instalacja agenta nie może wymagać określenia typu systemu (32 lub 64 – bitowy)
35. Instalacja klienta na urządzeniach mobilnych musi być dostępna za pośrednictwem portalu WWW udostępnionego przez moduł MDM z poziomu urządzenia użytkownika.
36. W przypadku braku zainstalowanego klienta na urządzeniu mobilnym musi istnieć możliwość jego pobrania ze sklepu Google Play.
37. 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.
38. Serwer administracyjny musi oferować możliwość utworzenia polityk konfiguracji dla aplikacji zabezpieczającej na urządzeniu mobilnym.
39. Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi.
40. Administrator musi posiadać możliwość utworzenia użytkownika wbudowanego lub zintegrowanego z grupą z usługi Active Directory.
41. Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp.
42. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.
43. Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta bez konieczności logowania się do panelu administracyjnego.
44. Dostępne zadania muszą być podzielone na dwie grupy: zadania klienta oraz zadania serwera.
45. Zadania serwera obejmujące zadanie instalacji agenta, generowania raportów oraz synchronizacji grup.
46. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej.
47. Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji.
48. Serwer administracyjny musi w przejrzysty sposób informować administratora o elementach zadań jakie są wymagane do jego uruchomienia a w przypadku jego braku wskazywać brakujące elementy konfiguracji.
49. Serwer administracyjny musi oferować możliwość wyboru parametrów pakietu instalacyjnego zależnych od systemu operacyjnego oraz licencji na program zabezpieczający.
50. Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu.
51. Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką.
52. Serwer administracyjny musi oferować możliwość utworzenia jednego zadania dla kilku klientów lub grupy.
53. Serwer administracyjny musi oferować możliwość uruchomienia zadania automatycznie zgodnie z harmonogramem lub po umieszczeniu nowego klienta w grupie dynamicznej.
54. Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów.
55. Serwer administracyjny musi oferować możliwość utworzenia polityk dla programów zabezpieczających i modułów serwera centralnego zarządzania.
56. Serwer administracyjny musi oferować możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów.
57. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej.

58. 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.
59. Serwer administracyjny musi oferować możliwość ukrycia graficznego interfejsu użytkownika na stacji klienckiej.
60. Serwer administracyjny musi umożliwiać wyświetlenie polityk do których przynależy dana stacja robocza
61. Serwer administracyjny musi posiadać minimum 40 szablonów raportów przygotowanych przez producenta
62. Serwer administracyjny musi oferować możliwość utworzenia własnych raportów lub skorzystanie z predefiniowanych wzorów.
63. Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania.
64. Serwer administracyjny musi oferować możliwość wyboru formy przedstawienia danych w raporcie w postaci tabeli, wykresu lub obu elementów jednocześnie.
65. Serwer administracyjny musi oferować możliwość wyboru jednego z kilku typów wykresów: kołowy, liniowy, słupkowy, punktowy, itp.
66. Serwer administracyjny musi oferować możliwość określenia danych jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na elementach wykresu oraz ich odfiltrowania i posortowania oraz zapisania szablonów stworzonych filtrów
67. 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.
68. Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, lub zgodnie z harmonogramem
69. Serwer administracyjny musi oferować możliwość wygenerowania raportu na podstawie informacje o zainstalowanych podzespołów w stacjach roboczych
70. Serwer administracyjny musi oferować możliwość tworzenia wielu zakładek panelu, w których będą widoczne wybrane przez administratora elementy monitorujące.
71. Serwer administracyjny musi oferować możliwość maksymalizacji wybranego elementu monitorującego.
72. Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.
73. Serwer administracyjny musi oferować możliwość utworzenia własnych powiadomień lub skorzystanie z predefiniowanych wzorów.
74. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP.
75. Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu.
76. Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji.
77. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty.
78. W przypadku posiadania tylko jednej dodanej licencji do konsoli zarządzania ma być ona wybierana automatycznie podczas konfiguracji zadania.
79. Rozwiązanie ma oferować weryfikacji zainstalowanych komponentów bazowych urządzenia takich jak: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, karty sieciowe, urządzenia masowe, etc.
80. Serwer administracyjny musi oferować możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela.
81. Narzędzie administracyjne musi być wyposażone w mechanizm wyszukiwania zarządzanych komputerów na podstawie co najmniej nazwy komputera, adresu IPv4 i IPv6
82. Serwer administracyjny oferować łatwy dostęp do zadań z poziomu menu kontekstowego w zależności od rodzaju urządzenia.
83. Serwer administracyjny musi oferować WOL.
84. Serwer administracji musi umożliwić granulację uprawnień dla Administratorów w taki sposób, aby każdemu z nich możliwe było przyznanie oddzielnych uprawnień do poszczególnych grup komputerów.
85. 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.
86. Konsola administracyjna musi oferować możliwość weryfikacji zmian w produktach wprowadzanych przez producenta (Release notes dostępne bezpośrednio z konsoli zarządzania).
87. Serwer musi wspierać wysyłanie logów do systemu SIEM IBM qRadar
88. Musi istnieć mechanizm, umożliwiający dodawanie reguł do istniejących już w module firewalla. Takie reguły można umieścić na początku lub końcu istniejącej listy.
89. Administrator musi otrzymywać powiadomienia o dostępnych aktualizacjach z poziomu interfejsu Konsoli administracyjnej

Wszystkie w/w wymagania muszą być spełnione przez najnowszą wersję oprogramowania.

III. Wymagania dotyczące oprogramowania równoważnego

1. Zamawiający dopuszcza możliwość zastosowania przez wykonawców w ofertach rozwiązań kompleksowej ochrony systemów komputerowych opierających się na innym – równoważnym oprogramowaniu, po spełnieniu warunków opisanych poniżej, określających równoważność oprogramowania w stosunku do wskazanego w specyfikacji istotnych warunków zamówienia.
2. Równoważność oprogramowania antywirusowego w stosunku do określonego w specyfikacji istotnych warunków zamówienia – przez równoważność oprogramowania należy rozumieć spełnienie następujących wymagań:
   - oferowane oprogramowanie spełnia specyfikację wymagań funkcjonalnych,
   - wykonawca wdroży oprogramowanie równoważne w nieprzekraczalnym terminie 10 dni roboczych od zawarcia umowy, czynności wykonywane będą w godzinach pracy zamawiającego,
   - wykonawca przeszkoli personel techniczny (4 osoby) w zakresie używania, zarządzania oraz administrowania programem,
   - wykonawca przygotuje i przekaże zamawiającemu wersję elektroniczną instrukcji obsługi interfejsu użytkownika oprogramowania zainstalowanego na komputerze (adekwatnie do liczby licencji),
   - wykonawca dokona pełnej deinstalacji istniejącego oprogramowania w liczbie 1100 licencji (w lokalizacjach: Września – wszystkie jednostki organizacyjne Zamawiającego), łącznie z usunięciem wpisów w rejestrach systemowych (nie wszystkie stacje zarządzane są za pomocą konsoli),
   - wykonawca dokona zainstalowania oprogramowania na komputerach w liczbie zgodnej z liczbą wymaganych licencji,
   - wykonawca dołączy do oferty sporządzoną przez siebie specyfikację funkcjonalną potwierdzającą spełnianie przez oferowane oprogramowanie wymagań określonych w punkcie I i II.

- wykonawca w ramach wdrożenia oprogramowania równoważnego przetestuje dostarczane oprogramowanie w kwestii zgodności z oprogramowaniem używanym w Gminie Września, w celu wykluczenia problemów w funkcjonowaniu dostarczonego oprogramowania i programów użytkowanych w Gminie Września. Zakończenie testów zostanie potwierdzone protokołem zawierającym spis przetestowanego oprogramowania użytkowanego przez Gminę Września.
- dostarczone równoważne oprogramowanie nawet w minimalny sposób nie może powodować spadku wydajności każdej stacji roboczej w konfiguracji tożsamej do używanej obecnie (uruchomione te same moduły skanowania)