Załącznik nr 1 do zaproszenia

Specyfikacja techniczna

w postępowaniu

na dostawę pakietu oprogramowania antywirusowego dla 200 stanowisk komputerowych oraz wsparcie techniczne w/w urządzeń na okres 24 miesięcy.

Przedmiot zamówienia:

1. Dostawa pakietu oprogramowania antywirusowego dla 200 stanowisk komputerowych oraz wsparcie techniczne w/w urządzeń na okres 24 miesięcy.
2. Wsparcie techniczne dla instalacji nowszej wersji oprogramowania, uruchomienia i konfiguracji centralnego serwera zarządzania oprogramowaniem stacji roboczych w sieci lokalnej Zamawiającego.
3. Wsparcie techniczne dla instalacji i konfiguracji oprogramowania na serwerach i stacjach roboczych.
4. Wsparcie techniczne w deinstalacji aktualnie używanego oprogramowania antywirusowego.
5. Aktualizacje oprogramowania oraz baz sygnatur przez okres 24 miesięcy.
6. Bezpłatna pomoc techniczna przez okres 24 miesięcy.

Wymagania ogólne:

1. Pakiet oprogramowania antywirusowego musi wspierać stacje robocze z systemem operacyjnym Windows XP/2003/2008R2/7/8.1/10/
2. MAC OS X oraz serwery z system operacyjnym: RedHat/Centos, Windows 2003/2008R2 a także musi być centralnie zarządzane dedykowanym systemem.
3. Okres ważności licencji - 24 miesiące, licząc od dnia odbioru przez Zamawiającego.
4. Wykonawca dostarczy licencje na zamówione oprogramowanie wraz z kluczami licencyjnymi.
5. Wykonawca zobowiązuje się do udzielania Zamawiającemu bezpłatnej pomocy technicznej na okres 24 miesięcy udzielanej w formie:
   a) telefonicznej, pocztą elektroniczną, zdalnie
   b) w przypadku braku usunięcia problemu w formie wymienionej w ppkt a. – wizyta technika.
6. Wsparcie techniczne musi obejmować aktualizacje 24h/24mc, samego pakietu oprogramowania oraz sygnatur baz danych antywirusowych w/w oprogramowania.
7. Program musi zabezpieczać procesory INTEL oraz AMD przed atakami SPECTRE i MELTOWN.

Oprogramowanie ochrony stacji roboczych z system operacyjnym Windows:

1. Oprogramowanie winno pracować na platformie sprzętowej z 1 GB RAM oraz jednordzeniowym procesorem 2 GHz – dot. 5% stacji roboczych, pozostała część stacji posiada znacznie wyższe parametry.
2. Polski interfejs użytkownika.
3. Program musi wspierać przynajmniej następujące systemy operacyjne: MS Windows 7/8.1/10 (32/64bit) oraz MS Windows XP w tym wersje współpracujące z usługą Active Directory.
4. Program ma zapewniać ochronę w czasie rzeczywistym oraz umożliwiać skanowanie na żądanie.
5. Program powinien zapewniać ochronę, przed wszystkimi rodzajami wirusów, przede wszystkim ransomware, trojan-ów, spyware, adware, a także przed złośliwym kodem (w tym Java i ActiveX), ochronę poczty elektronicznej.
6. Wykrywanie oprogramowania szpiegowskiego, pobierającego reklamy, programów podwyższonego ryzyka oraz narzędzi hakerskich.
7. System antywirusowy powinien posiadać możliwość skanowania archiwów i plików spakowanych niezależnie od poziomu ich zagnieżdżenia.
8. Leczenie i usuwanie plików z archiwów następujących formatów RAR, ARJ, ZIP, CAB, LHA, JAR, ICE.

9. Monitor antywirusowy musi być uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego.
10. Program musi posiadać możliwość określenia listy reguł wykluczeń dla wybranych obiektów, rodzajów zagrożeń oraz składników ochrony.
11. Oprogramowanie winno posiadać certyfikaty niezależnych laboratoriów.
12. Wbudowany ruch HTTP w czasie rzeczywistym niezależnie od przeglądarki oraz moduł skanujący protokoły POP3, SMTP, IMAP niezależnie od klienta pocztowego.
13. Skaner poczty powinien mieć możliwość usuwania określonych typów załączników.
14. Wbudowany moduł kontrolujący dostęp do rejestru systemowego, do ustawień Internet Explorera, chroniący przed phishingiem oraz moduł skanujący skrypty VB Script i Java Script wykonywane przez system operacyjny i przeglądarkę.
15. Skanowanie w czasie rzeczywistym:
    a) uruchamianych, otwieranych, kopiowanych, przenoszonych lub tworzonych plików;
    b) pobieranej poczty elektronicznej (wraz z załącznikami) poprzez POP3, SMTP, IMAP niezależnie od klienta pocztowego;
    c) pobieranych plików poprzez http:// i https:// treści i plików przesyłanych z wykorzystaniem komunikatorów internetowych.
16. Po wykryciu podejrzanych działań uruchamianych aplikacji (np. modyfikacje rejestru, wtargnięcie do innych procesów) musi istnieć możliwość zezwolenia lub zablokowania takiego działania.
17. Możliwość tworzenia list zaufanych procesów, dla których nie będzie monitorowana aktywność plikowa, aktywność aplikacji, nie będą dziedziczone ograniczenia nadrzędnego procesu, nie będzie monitorowana aktywność aplikacji potomnych, dostęp do rejestru oraz ruch sieciowy.
18. Skaner antywirusowy może być uruchamiany automatycznie zgodnie z terminarzem z możliwością skanowana wszystkich lokalnych dysków komputera.
19. W przypadku wykrycia szkodliwego kodu oprogramowanie może automatycznie:
    a) podejmować zalecane działanie, tj. próbować leczyć, utworzyć kopię zapasową przed podjęciem próby leczenia lub usunięcia zainfekowanego pliku w przypadku braku możliwości wyleczenia - usuwać obiekt;
    b) poddać kwarantannie podejrzany plik;
    c) rejestrować informację o wykryciu wirusa;
    d) powiadamiać administratora np.: przy użyciu e-mail.
20. Zapora ogniowa (moduł) z możliwością: tworzenia reguł monitorowania aktywności sieciowej dla wszystkich zainstalowanych aplikacji, w oparciu o charakterystyki pakietów sieciowych i podpis cyfrowy aplikacji; tworzenia nowych zestawów warunków i działań wykonywanych na pakietach sieciowych oraz strumieniach danych dla określonych protokołów, portów i adresów IP; zdefiniowania zaufanych podsieci, dla których nie będą stosowane żadne reguły zapory.
21. Ochrona przed niebezpiecznymi rodzajami aktywności sieciowej i atakami, możliwość tworzenia reguł wykluczających dla określonych adresów/zakresów IP.
22. Program powinien mieć możliwość zdefiniowania portów, które będą monitorowane lub wykluczone z monitorowania przez moduły skanujące ruch sieciowy.
23. Kontrola dostępu do zasobów sieciowych w zależności od ich zawartości i lokalizacji: możliwość definiowania reguł filtrujących zawartość na wybranej stronie lub wszystkich stronach w zależności od kategorii zawartości: np.: narkotyki, gry, portale społecznościowe itd.; możliwość definiowania reguł blokujących bądź zezwalających na wyświetlanie określonej treści na wybranej stronie lub wszystkich stronach w zależności od kategorii danych: pliki wideo, audio itd.
24. Nadzór nad systemem poprzez ochronę proaktywną przed nowymi zagrożeniami, które nie znajdują się w antywirusowych bazach danych, kontrola aktywności aplikacji, dostarczanie

szczegółowych informacji dla innych modułów aplikacji w celu zapewnienia jeszcze bardziej efektywnej ochrony, możliwość wycofywania zmian wprowadzanych w systemie przez szkodliwe oprogramowanie.

25. Wbudowany moduł wyszukiwania heurystycznego bazującego na analizie kodu potencjalnego wirusa, możliwość określenia poziomu czułości modułu heurystycznego.
26. Moduł blokujący określone kategorie urządzeń (np. pamięci masowe itp.), możliwość tworzenia reguł blokujących/zezwalających na korzystanie z danego urządzenia w zależności od konta, możliwość tylko zapisu bądź tylko odczytu, ewentualnie zapisu i odczytu na urządzeniu. Możliwość blokowania urządzeń według ich rodzaju: dyski, USB, drukarki itp. w zależności od konta użytkownika systemu Windows.
27. Monitor wykrywania luk w aplikacjach zainstalowanych na stacji roboczej oraz w samym systemie operacyjnym, wyświetlenie podsumowania o lukach w aplikacjach i systemie operacyjnym.
28. Oprogramowanie powinno mieć możliwość określenia źródła uaktualnień, określenia harmonogramu pobierania uaktualnień.
29. Terminarz pozwalający na planowanie zadań, w tym także terminów automatycznej aktualizacji baz sygnatur.
30. Program musi posiadać możliwość pobierania uaktualnień modułów dla zainstalowanej wersji aplikacji.
31. Program musi posiadać możliwość skanowania obiektów poddanych kwarantannie po zakończonej aktualizacji, możliwość cofnięcia ostatniej aktualizacji w przypadku uszkodzenia zestawu uaktualnień.
32. Zbieranie i przetwarzanie alarmów w czasie rzeczywistym.
33. Program powinien posiadać możliwość raportowania zdarzeń, określenia okresu przechowywania raportów.
34. Program powinien posiadać możliwość określenia okresu przechowywania obiektów znajdujących się w magazynie kopii zapasowych oraz kwarantannie.
35. Program musi posiadać możliwość wyłączenia zaplanowanych zadań skanowania podczas pracy na baterii w przypadku laptopa.
36. Program powinien posiadać możliwość wyeksportowania bieżącej konfiguracji programu w celu jej późniejszego zaimportowania na tym samym lub innym komputerze.
37. Program musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju.
38. Program musi posiadać funkcję chroniącą pliki, foldery i klucze rejestru wykorzystywane przez program przed zapisem i modyfikacją.
39. Możliwość wyłączenia zewnętrznej kontroli usługi antywirusowej oraz możliwość zresetowania wszystkich ustawień włącznie z regułami stworzonymi przez użytkownika.
40. Oprogramowanie musi posiadać możliwość zablokowania hasłem operacji zamykania programu, zatrzymywania zadań, wyłączania ochrony, wyłączania profilu administracyjnego, zmiany ustawień.
41. Możliwość zablokowania dostępu do ustawień programu dla użytkowników nie posiadających uprawnień administracyjnych.
42. Możliwość dynamicznej zmiany użycia zasobów systemowych w zależności od obciążenia systemu przez aplikacje użytkownika.
43. Centralne zbieranie i przetwarzanie alarmów w czasie rzeczywistym.
44. Możliwość wysłania podejrzanego obiektu do producenta oprogramowania antywirusowego w celu analizy.

Oprogramowanie ochrony stacji roboczych MAC:

1. Program musi wspierać przynajmniej system operacyjny OS X 10.9 (Mavericks).
2. Program powinien być certyfikowany.
3. Program powinien zapewniać ochronę przed wszystkimi rodzajami wirusów, przede wszystkim ransomware, trojanów, narzędzi hakerskich, oprogramowania typu spyware i adware oraz innymi potencjalnie niebezpiecznymi programami.

4. Program musi zapewniać ochronę w czasie rzeczywistym oraz umożliwiać skanowanie na żądanie.
5. Program musi posiadać możliwość określenia listy reguł wykluczeń dla wybranych obiektów, rodzajów zagrożeń oraz składników ochrony, a także powinien mieć możliwość określenia predefiniowanego poziomu ochrony.
6. Program powinien posiadać możliwość wyboru akcji podejmowanych wobec zainfekowanych obiektów.
7. Program musi posiadać możliwość określenia skanowania plików według ich formatu wewnętrznego lub rozszerzenia.
8. Program musi posiadać możliwość skanowania tylko nowych i zmienionych plików, pakietów instalacyjnych oraz archiwów w tym możliwość leczenia oraz usuwania zainfekowanych plików z archiwów.
9. Program musi posiadać wbudowany moduł wyszukiwania heurystycznego bazującego na analizie kodu potencjalnego wirusa z możliwością określenia poziomu analizy.
10. Program musi posiadać możliwość utworzenia kopii zapasowej zainfekowanego obiektu przed jego usunięciem i umieszczenie jej w magazynie kopii zapasowych.
11. Program musi posiadać możliwość przeniesienia podejrzanego obiektu do obszaru kwarantanny.
12. Program powinien posiadać możliwość określenia listy skanowanych obiektów.
13. Program musi posiadać możliwość tworzenia własnych zadań skanowania na żądanie.
14. Program musi posiadać możliwość określenia terminarza uruchamiania zadań skanowania na żądanie.
15. Program powinien posiadać możliwość określenia harmonogramu pobierania uaktualnień.
16. Program musi posiadać możliwość pobierania uaktualnień modułów dla zainstalowanej wersji aplikacji, program powinien posiadać możliwość określenia źródła uaktualnień w tym określenia katalogu.
17. Program musi posiadać możliwość skanowania obiektów poddanych kwarantannie po zakończonej aktualizacji.
18. Program powinien posiadać możliwość raportowania zdarzeń z określeniem okresu przechowywania raportów.
19. Program powinien posiadać możliwość określenia okresu przechowywania obiektów znajdujących się w magazynie kopii zapasowych oraz kwarantannie.
20. Program powinien posiadać możliwość wyeksportowania bieżącej konfiguracji programu w celu jej późniejszego zaimportowania na tym samym lub innym komputerze.
21. Program musi posiadać możliwość zdalnej administracji pozwalającej na: aktualizację baz danych sygnatur zagrożeń z repozytorium serwera zarządzającego; uruchamianie zadań skanowania antywirusowego; uzyskanie szczegółowych informacji na temat ochrony antywirusowej stacji roboczej.
22. Program musi posiadać możliwość przesłania informacji na temat obiektów przechowywanych w magazynie kopii zapasowych oraz kwarantannie bezpośrednio na serwer administracyjny w celu umożliwienia administratorom podjęcie wobec nich odpowiednich działań.

Oprogramowanie ochrony serwerów Linux:

1. Program musi wspierać przynajmniej następujące systemy operacyjne: Red Hat Enterprise Linux 6 Server oraz CentOS-6/7.
2. Program powinien posiadać przynajmniej certyfikat: RedHat Enterprise Linux Certified.
3. Program musi zapewniać ochronę w czasie rzeczywistym oraz umożliwiać skanowanie na żądanie.
4. Zarządzanie oprogramowaniem przynajmniej z poziomu wiersza poleceń.
5. Program powinien zapewniać ochronę przed wszystkimi rodzajami wirusów, przede wszystkim ransomware, trojanów, narzędzi hakerskich, oprogramowania typu spyware i adware oraz innymi potencjalnie niebezpiecznymi programami.

6. Program musi posiadać moduł analizy heurystycznej oraz możliwość skanowania archiwów przynajmniej formatów: ZIP, RAR.
7. Program musi posiadać moduł ochrony w czasie rzeczywistym skanujący pliki oraz udostępniane i zamontowane zasoby w trybie NFS.
8. Moduł skanowania na żądanie musi umożliwiać definiowanie zadań skanowania wybranych obszarów file systemu.
9. Program musi mieć możliwość uruchomienia działania ochrony w czasie rzeczywistym zgodnie z terminarzem oraz możliwość wstrzymania działania ochrony w czasie rzeczywistym po określonym czasie od jej uruchomienia lub w określonych przedziale czasowym.
10. Program musi mieć możliwość dostosowania zakresu ochrony w czasie rzeczywistym, tak aby monitorowane były tylko wybrane foldery oraz tak, aby monitorowane były jedynie pliki o określonych rozszerzeniach.
11. Program musi mieć możliwość zdefiniowania akcji jakie mają być wykonywane na obiektach zainfekowanych oraz podejrzanych oraz możliwość konfiguracji podejmowanych akcji w zależności od typu wykrytego zagrożenia.
12. Program musi posiadać funkcję wykluczania obiektów ze skanowania na podstawie ich nazwy oraz musi posiadać funkcję wykluczania obiektów ze skanowania na podstawie nazwy zagrożenia jakie jest w nich wykrywane.
13. Program musi mieć możliwość wykluczenia ze skanowania obiektów większych niż zadany rozmiar.
14. W przypadku wykrycia wirusa monitor antywirusowy powinien automatycznie: podejmować zalecane działanie czyli próbować leczyć, a jeżeli nie jest to możliwe usuwać obiekt; rejestrować w pliku raportu informację o wykryciu wirusa; utworzyć kopię zapasową przed podjęciem próby leczenia lub usunięcia zainfekowanego pliku; poddać kwarantannie podejrzany obiekt.
15. Program powinien mieć możliwość konfiguracji liczby aktywnych procesów skanujących.
16. Program powinien mieć możliwość eksportu i importu ustawień.
17. Program musi posiadać moduł kwarantanny przechowujący zainfekowane obiekty; system kwarantanny musi umożliwiać proste skanowanie, usuwanie i przywracanie do pierwotnej lokalizacji wybranych plików.
18. Program musi mieć możliwość zdefiniowania katalogu w którym przechowywane będą pliki poddane kwarantannie.
19. Program powinien umożliwiać aktualizację baz sygnatur z serwerów producenta oprogramowania, serwera administracyjnego lub wskazanego zasobu np.: HTTP, FTP lub określonej kartoteki plikowej.
20. Program musi umożliwiać uruchamianie zadania aktualizacji zgodnie z harmonogramem.
21. Program powinien posiadać możliwość eksportu baz sygnatur w celu aktualizacji programu na innym serwerze.
22. Program musi posiadać możliwość zapisywania zdarzeń z działania programu np.: w dzienniku zdarzeń wraz z informacją o każdym przeskanowanym pliku.
23. Program musi umożliwiać generowanie raportów w tym zapisanych do plików np.: html, pdf.
24. Program musi posiadać możliwość powiadamiania administratora na temat zaistniałych zdarzeń przynajmniej za pośrednictwem wiadomości mail.

<u>Oprogramowanie ochrony serwerów Windows:</u>

1. Program ma wspierać co najmniej serwerowe systemy operacyjne: MS Windows Server 2008 R2 Standard Edition, MS Windows Server 2003 Standard SP2.
2. Polskojęzyczny interfejs.
3. Program powinien posiadać certyfikaty niezależnych laboratoriów.
4. Program musi posiadać możliwość określenia listy reguł wykluczeń dla wybranych obiektów, rodzajów zagrożeń oraz składników ochrony.

5. Program ma możliwość klasyfikacji wszystkich aplikacji i możliwość ograniczenia ich działania na podstawie ich stanu.
6. Ochrona przed wszystkimi typami wirusów, przede wszystkim ransomware, robaków i koni trojańskich, a także złośliwym kodem, oprogramowaniem typu spyware i adware, możliwość wykrywania oprogramowania szpiegowskiego, pobierającego reklamy, programów podwyższonego ryzyka, narzędzi hakerskich oraz innymi potencjalnie niebezpiecznymi programami.
7. Program musi posiadać moduł wyszukiwania heurystycznego bazującego na analizie kodu potencjalnego wirusa, możliwość określenia poziomu czułości modułu heurystycznego.
8. Firewall z możliwością: tworzenia reguł monitorowania aktywności sieciowej dla wszystkich zainstalowanych aplikacji, w oparciu o charakterystyki pakietów sieciowych i podpis cyfrowy aplikacji; tworzenia nowych zestawów warunków i działań wykonywanych na pakietach sieciowych oraz strumieniach danych dla określonych protokołów, portów i adresów IP; zdefiniowania zaufanych podsieci, dla których nie będą stosowane żadne reguły zapory.
9. Ochrona przed niebezpiecznymi rodzajami aktywności sieciowej i atakami, możliwość tworzenia reguł wykluczających dla określonych adresów/zakresów IP.
10. Centralne zbieranie i przetwarzanie alarmów w czasie rzeczywistym.
11. Leczenie i usuwanie plików z archiwów następujących formatów RAR, ARJ, ZIP, CAB, LHA, JAR i ICE.
12. Terminarz pozwalający na planowanie zadań, w tym także terminów automatycznej aktualizacji baz sygnatur.
13. Możliwość wysłania podejrzanego obiektu do producenta oprogramowania antywirusowego w celu analizy.
14. Monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego.
15. Możliwość tworzenia list zaufanych procesów, dla których nie będzie monitorowana aktywność plikowa, aktywność aplikacji, nie będą dziedziczone ograniczenia nadrzędnego procesu, nie będzie monitorowana aktywność aplikacji potomnych.
16. Możliwość dynamicznej zmiany użycia zasobów systemowych w zależności od obciążenia systemu przez aplikacje użytkownika.
17. Możliwość wyłączenia zewnętrznej kontroli usługi antywirusowej.
18. Możliwość zresetowania wszystkich ustawień włącznie z regułami stworzonymi przez użytkownika.
19. Program musi posiadać możliwość zablokowania hasłem operacji zamykania programu, zatrzymywania zadań, wyłączania ochrony, wyłączania profilu administracyjnego, zmiany ustawień oraz odinstalowania programu.
20. W przypadku wykrycia wirusa monitor antywirusowy może automatycznie:
    a) podejmować zalecane działanie czyli próbować leczyć, a jeżeli nie jest to możliwe usuwać obiekt;
    b) utworzyć kopie zapasową przed podjęciem próby leczenia lub usunięcia zainfekowanego pliku;
    c) poddać kwarantannie podejrzany obiekt;
    d) rejestrować informację o wykryciu wirusa;
    e) powiadamiać administratora przy użyciu e-mail.

f) Skaner antywirusowy może być uruchamiany automatycznie zgodnie z terminarzem.
g) System antywirusowy powinien posiadać możliwość skanowania archiwów i plików spakowanych niezależnie od poziomu ich zagnieżdżenia.
h) Program powinien posiadać możliwość określenia harmonogramu pobierania uaktualnień.
i) Program musi posiadać możliwość pobierania uaktualnień modułów dla zainstalowanej wersji aplikacji.
j) Program powinien posiadać możliwość określenia źródła uaktualnień.
k) Program musi posiadać możliwość określenia katalogu, do którego będzie kopiowany zestaw uaktualnień po zakończeniu aktualizacji.

l) Program musi posiadać możliwość skanowania obiektów poddanych kwarantannie po zakończonej aktualizacji.
m) Program powinien posiadać możliwość cofnięcia ostatniej aktualizacji w przypadku uszkodzenia zestawu uaktualnień.
n) Program powinien posiadać możliwość raportowania zdarzeń.
o) Program powinien posiadać możliwość określenia okresu przechowywania raportów.
p) Program powinien posiadać możliwość określenia okresu przechowywania obiektów znajdujących się w magazynie kopii zapasowych oraz kwarantannie.
q) Program musi posiadać możliwość wyeksportowania bieżącej konfiguracji programu w celu jej późniejszego zaimportowania na tym samym lub innym serwerze.

Centralny system zarządzania oprogramowaniem antywirusowym stacji roboczych:

1. System scentralizowanego zarządzania powinien obsługiwać następujące systemy operacyjne: MS Windows XP Professional, MS Windows 7/8.1/10, MS Windows Server 2003, MS Windows Server 2008 R2.
2. System scentralizowanego zarządzania powinien przechowywać ustawienia/dane w relacyjnej bazie danych umożliwiający backup całej bazy.
3. System zdalnego zarządzania powinien posiadać polskojęzyczny lub angielski interfejs.
4. System zdalnego zarządzania powinien umożliwiać automatyczne umieszczenie komputerów w grupach administracyjnych odpowiadających strukturze sieci (struktura Active Directory i grupy robocze sieci Microsoft Windows).
5. System zdalnego zarządzania powinien umożliwiać automatyczne umieszczanie stacji roboczych w określonych grupach administracyjnych w oparciu o zdefiniowane reguły.
6. System zdalnego zarządzania powinien posiadać pakiet instalacyjny dla stacji roboczej jak również systemów serwerowych.
7. System zdalnego zarządzania powinien umożliwiać ograniczenie pasma sieciowego wykorzystywanego do komunikacji stacji z serwerem administracyjnych. Reguły powinny umożliwić ograniczenia w oparciu o zakresy adresów IP oraz przedziały czasowe.
8. System zdalnego zarządzania umożliwiający tworzenie hierarchicznej struktury serwerów administracyjnych.
9. System zdalnego zarządzania umożliwiający zarządzanie stacjami roboczymi i serwerami plików Windows, nawet wtedy, gdy znajdują się one za zaporą NAT/Firewall.
10. Komunikacja pomiędzy serwerem zarządzającym a stacjami roboczymi szyfrowana przy użyciu protokołu SSL.
11. Konsola administracyjna posiadająca możliwość zdalnego inicjowania skanowania antywirusowego na stacjach roboczych włączonych do sieci komputerowych.
12. Zarządzanie aplikacjami przy użyciu profili dla konkretnej aplikacji oraz zadań.
13. Konsola administracyjna posiadająca możliwość informowania administratorów o wykryciu epidemii wirusa.
14. Serwer zarządzający posiadający możliwość automatycznej reakcji na epidemie wirusa (automatyczne stosowanie wskazanego profilu ustawień stacji roboczych oraz uruchomienia odpowiednich zadań).
15. System centralnego zarządzania wyposażony w mechanizmy raportowania i dystrybucji oprogramowania oraz polityk antywirusowych.
16. System centralnej dystrybucji i instalacji aktualizacji sygnatur wirusów, który umożliwia automatyczne, niewidoczne dla użytkownika przesłanie i zainstalowanie nowej wersji.
17. System centralnej dystrybucji i instalacji aktualizacji oprogramowania, który umożliwia automatyczne, niewidoczne dla użytkownika przesłanie i zainstalowanie nowego oprogramowania.
18. System centralnego zbierania informacji i tworzenia sumarycznych raportów.

19. System zdalnego zarządzania powinien:

a) umożliwiać automatyczne wysyłanie raportów pocztą elektroniczną lub zapisywanie ich w postaci plików w zdefiniowanej lokalizacji (przynajmniej w formatach HTML i PDF).
b) umożliwiać podgląd w czasie rzeczywistym statystyk ochrony, stanu aktualizacji instalacji w sieci itp.,
c) umożliwiać tworzenie kategorii aplikacji i warunków ich uruchomienia,
d) umożliwiać przeglądanie informacji o aplikacjach i plikach wykonywalnych znajdujących się na stacjach roboczych,
e) wyświetlać szczegółowe informacje na temat luk w oprogramowaniu wykrytych na zarządzanych komputerach,
f) umożliwiać przeglądanie informacji o kopiach zapasowych obiektów wyleczonych/usuniętych na stacjach roboczych wraz z możliwością ich przywrócenia do początkowej lokalizacji i/lub zapisania na stacji administratora,
g) umożliwiać przeglądanie informacji o obiektach, które zostały wykryte ale program nie podjął względem nich żadnego działania wraz z możliwością wymuszenia przez administratora odpowiedniego działania,
h) umożliwiać automatyczne instalowanie licencji na stacjach roboczych,
i) umożliwiać ręczne/automatyczne i regularne tworzenie kopii zapasowej serwera zarządzającego, która umożliwi przywrócenie w pełni działającego systemu zarządzania,
j) umożliwiać wysłanie do stacji roboczych komunikatu o dowolnie zdefiniowanej treści,
k) umożliwiać zdalne włączanie, wyłączanie oraz restartowanie stacji roboczej wraz z możliwością interakcji z użytkownikiem,
l) posiadać możliwość sprawdzenia aktualnych wersji oprogramowania antywirusowego,
m) powinien tworzyć repozytorium sprzętu w tym min. nośników wymiennych.