Załącznik nr. 1

# Przedmiot zamówienia

Przedmiotem zmówienia jest zakup kontynuacji obecnie posiadanego oprogramowania antywirusowego Kaspersky Endpoint Security for Windows w wersji Select z rozbudową do wersji Advanced dla 150 licencji, w tym 2 licencji na serwer na okres 36 miesięcy lub równoważnego nowego oprogramowania innego producenta. Oprogramowanie innego producenta musi być równoważne i posiadać następujące funkcje:

# I. Oprogramowanie **Antywirusowe na stacje robocze**

1. Program musi wspierać następujące platformy:
   * Windows 10 Home / Pro / Education / Enterprise
   * Windows 8.1 Professional / Enterprise
   * Windows 8 Professional / Enterprise
   * Windows 7 Home / Professional / Enterprise Service Pack 1 lub nowszy
2. Program musi spełniać następujące minimalne wymagania sprzętowe:
   * Procesor 1 GHz lub szybszy (wymagana jest obsługa SSE2).
   * Pamięć RAM:

1 GB dla 32-bitowych systemów operacyjnych.

2 GB dla 64-bitowych systemów operacyjnych.

* + 2 GB wolnej przestrzeni na dysku twardym.

1. Polskojęzyczny interfejs konsoli programu i jego monitora na stacjach roboczych.
2. Program powinien posiadać certyfikaty niezależnych laboratoriów.
3. Program powinien zapewniać ochronę przed wszystkimi rodzajami wirusów, trojanów, narzędzi hakerskich, oprogramowania typu spyware i adware, auto-dialerami i innymi potencjalnie niebezpiecznymi programami.
4. Program musi posiadać możliwość określenia listy reguł wykluczeń dla wybranych obiektów, rodzajów zagrożeń oraz składników ochrony.
5. Program powinien posiadać możliwość skanowania i klasyfikowania plików oraz odsyłaczy do zasobów sieciowych na podstawie informacji gromadzonych w oparciu o technologię chmury.
6. Program ma mieć możliwość wyświetlenia podsumowania o aktywności, reputacji i lukach w aplikacjach aktualnie uruchomionych w systemie.
7. Program ma mieć możliwość monitorowania prób uruchamiania aplikacji przez użytkowników zgodnie z określonymi regułami.
8. Program ma mieć możliwość klasyfikacji wszystkich aplikacji i możliwość ograniczenia ich działania na podstawie ich stanu.
9. Program ma posiadać dedykowany moduł blokujący określone kategorie urządzeń (np. pamięci masowe, urządzenia Bluetooth itp.).

* Możliwość tworzenia reguł blokujących/zezwalających na korzystanie z danego urządzenia w zależności od konta, na którym pracuje użytkownik, określenia przedziału czasu, w którym użytkownik będzie miał możliwość tylko zapisu bądź tylko odczytu, ewentualnie zapisu i odczytu.
* Możliwość utworzenia listy zaufanych urządzeń na podstawie modelu, bądź identyfikatora urządzenia dla określonego konta użytkownika systemu Windows.

1. Użytkownik, ma możliwość wysłania do administratora zgłoszenia z prośbą o umożliwienie dostępu do zablokowanego urządzenia; nośnik wymienny, napęd CD-ROM itd.
2. Użytkownik, ma możliwość wysłania do administratora zgłoszenia z prośbą o umożliwienie dostępu do zablokowanego zasobu sieciowego.
3. Użytkownik, ma możliwość wysłania do administratora zgłoszenia z prośbą o umożliwienie dostępu do zablokowanej aplikacji.
4. Kontrola sieci – 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: pornografia, narkotyki, broń, gry, sieci społecznościowe, banery, 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, archiwa itd.

1. Program powinien zawierać moduł wykorzystujący zestaw reguł do śledzenia nietypowych zachować na chronionych komputerach.

* Reguły powinny być aktualizowane automatycznie ale zatwierdzane ręcznie przez administratora.
* Moduł powinien posiadać możliwość tworzenia wykluczeń dla poszczególnych reguł.

1. Ochrona przed wszystkimi typami wirusów, robaków i koni trojańskich, przed zagrożeniami z Internetu i poczty elektronicznej, a także złośliwym kodem (w tym Java i ActiveX).
2. Wbudowany moduł chroniący pamięć procesów systemowych
3. Możliwość wykrywania oprogramowania szpiegowskiego, pobierającego reklamy, programów podwyższonego ryzyka oraz narzędzi hakerskich.
4. Wbudowany moduł skanujący protokoły POP3, SMTP, IMAP i NNTP niezależnie od klienta pocztowego.
5. Skaner poczty powinien mieć możliwość zmiany nazwy lub usuwania określonych typów załączników.
6. Wbudowany moduł skanujący ruch HTTP w czasie rzeczywistym niezależnie od przeglądarki.
7. Wbudowany moduł wyszukiwania heurystycznego bazującego na analizie kodu potencjalnego wirusa.
8. Możliwość określenia poziomu czułości modułu heurystycznego.
9. Wbudowany moduł kontrolujący dostęp do rejestru systemowego.
10. Wbudowany moduł kontrolujący dostęp do ustawień Internet Explorera.
11. Wbudowany moduł chroniący przed phishingiem.
12. Moduł zapory ogniowej 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.

1. Ochrona przed niebezpiecznymi rodzajami aktywności sieciowej i atakami, możliwość tworzenia reguł wykluczających dla określonych adresów/zakresów IP.
2. Kontrola systemu 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.
* Kontrola udostępnionych folderów przed zewnętrznymi operacjami szyfrowania plików.
* Moduł gromadzący dane o podejrzanej aktywności w bieżącej oraz wcześniejszych sesjach użytkownika, który umożliwi wycofanie zmian wprowadzanych w systemie przez szkodliwe oprogramowanie.

1. Centralne zbieranie i przetwarzanie alarmów w czasie rzeczywistym.
2. Leczenie i usuwanie plików z archiwów następujących formatów RAR, ARJ, ZIP, CAB, LHA, JAR i ICE.
3. Możliwość zablokowania dostępu do ustawień programu dla użytkowników nie posiadających uprawnień administracyjnych.
4. Terminarz pozwalający na planowanie zadań, w tym także terminów automatycznej aktualizacji baz sygnatur.
5. Monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego.
6. 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.
7. Możliwość dynamicznej zmiany użycia zasobów systemowych w zależności od obciążenia systemu przez aplikacje użytkownika.
8. Program ma posiadać funkcję chroniącą pliki, foldery i klucze rejestru wykorzystywane przez program przed zapisem i modyfikacją.
9. Program ma posiadać możliwość wyłączenia zewnętrznej kontroli usługi antywirusowej.
10. Program ma posiadać możliwość zresetowania wszystkich ustawień włącznie z regułami stworzonymi przez użytkownika.
11. Program musi posiadać możliwość zablokowania operacji zamykania programu, zatrzymywania zadań, wyłączania ochrony, wyłączania profilu administracyjnego, zmiany ustawień, usunięcia licencji oraz odinstalowania programu przy użyciu zdefiniowanej nazwy użytkownika i hasła.
12. Program ma możliwość zdefiniowania portów, które będą monitorowane lub wykluczone z monitorowania przez moduły skanujące ruch sieciowy (z wyłączeniem zapory ogniowej).
13. Program powinien zapewnić autoryzację urządzeń typu klawiatura podłączanych do portu USB.
14. Jeżeli podłączane urządzenie nie posiada fizycznych klawiszy np. czytnik kodów kreskowych, program powinien zapewnić możliwość autoryzacji urządzenia przy użyciu klawiatury ekranowej.
15. Program powinien posiadać wbudowany moduł do obsługi technologii AMSI firmy Microsoft.
16. Skanowanie w czasie rzeczywistym:

* Uruchamianych, otwieranych, kopiowanych, przenoszonych lub tworzonych plików.
* Pobieranej z Internetu poczty elektronicznej (wraz z załącznikami) po protokołach POP3, SMTP, IMAP i NNTP niezależnie od klienta pocztowego.
* Plików pobieranych z Internetu po protokole HTTP.
* Poczty elektronicznej przetwarzanej przez program MS Outlook niezależnie od wykorzystywanego protokołu pocztowego.

1. W przypadku wykrycia wirusa monitor antywirusowy może automatycznie:

* Podejmować zalecane działanie czyli próbować leczyć, a jeżeli nie jest to możliwe usuwać obiekt
* Rejestrować w pliku raportu informację o wykryciu wirusa
* Powiadamiać administratora przy użyciu poczty elektronicznej lub poleceniem NET SEND
* Utworzyć kopie zapasową przed podjęciem próby leczenia lub usunięcia zainfekowanego pliku

1. Skaner antywirusowy może być uruchamiany automatycznie zgodnie z terminarzem; skanowane są wszystkie lokalne dyski twarde komputera.
2. Informowanie o wykryciu podejrzanych działań uruchamianych aplikacji (np. modyfikacje rejestru, wtargnięcie do innych procesów) wraz z możliwością zezwolenia lub zablokowania takiego działania.
3. System antywirusowy ma posiadać możliwość skanowania archiwów i plików spakowanych niezależnie od poziomu ich zagnieżdżenia.
4. Program powinien posiadać możliwość określenia harmonogramu pobierania uaktualnień, w tym możliwość wyłączenia aktualizacji automatycznej.
5. Program musi posiadać możliwość pobierania uaktualnień modułów dla zainstalowanej wersji aplikacji.
6. Program powinien posiadać możliwość określenia źródła uaktualnień.
7. Program musi posiadać możliwość określenia katalogu, do którego będzie kopiowany zestaw uaktualnień po zakończeniu aktualizacji.
8. Program musi posiadać możliwość cofnięcia ostatniej aktualizacji w przypadku uszkodzenia zestawu uaktualnień.
9. Program musi posiadać możliwość określenia ustawień serwera proxy w przypadku, gdy jest on wymagany do nawiązania połączenia z Internetem.
10. Pobieranie uaktualnień w trybie przyrostowym (np. po zerwaniu połączenia, bez konieczności retransmitowania już wczytanych fragmentów informacji).
11. Program musi posiadać funkcjonalność szyfrowanie plików, folderów, dysków i nośników wymiennych.
12. Do szyfrowania musi być wykorzystywany algorytm AES.
13. Program powinien posiadać możliwość zarządzania funkcją BitLocker systemów Windows
14. Program powinien posiadać możliwość tworzenia zaszyfrowanych pakietów z poziomu menu kontekstowego.
15. Program powinien umożliwiać dostęp do zaszyfrowanych plików także na komputerach bez zainstalowanego oprogramowania szyfrującego.
16. Program musi posiadać funkcjonalność odzyskiwania danych z zaszyfrowanych nośników po utracie hasła lub w wyniku uszkodzenia nośnika.
17. Program powinien posiadać możliwość określenia okresu przechowywania raportów.
18. Program powinien posiadać możliwość określenia okresu przechowywania obiektów znajdujących się w magazynie kopii zapasowych.
19. Program musi posiadać możliwość wyłączenia zaplanowanych zadań skanowania podczas pracy na bateriach.
20. Program musi posiadać możliwość wyeksportowania bieżącej konfiguracji programu w celu jej późniejszego zaimportowania na tym samym lub innym komputerze.
21. Program musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju.
22. Program musi mieć możliwość włączenia opcji współdzielenia zasobów z innymi aplikacjami.
23. Program powinien posiadać możliwość skanowania połączeń szyfrowanych.

* Moduł powinien umożliwiać blokowanie połączeń SSL 2.0
* Umożliwiać włączenia deszyfracji bezpiecznego połączenia z certyfikatem EV.
* Umożliwiać zdefiniowanie działania w przypadku wystąpienia błędu skanowania.
* Umożliwiać zdefiniowanie działania w przypadku odwiedzania domeny z niezaufanych certyfikatem.
* Umożliwić dodanie zaufanych domen.

# II. Oprogramowanie Antywirusowe na serwer

1. Program musi wspierać następujące platformy:
   * Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
   * Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
   * Windows Server 2016 Essentials / Standard / Datacenter;
   * Windows Server 2019 Essentials / Standard / Datacenter.
2. Program musi spełniać następujące minimalne wymagania sprzętowe:

Procesor 1 GHz lub szybszy (wymagana jest obsługa SSE2).

* + Pamięć RAM:

1 GB dla 32-bitowych systemów operacyjnych.

2 GB dla 64-bitowych systemów operacyjnych.

* + 2 GB wolnej przestrzeni na dysku twardym.

1. Polskojęzyczny interfejs konsoli programu i jego monitora na stacjach roboczych.
2. Program powinien posiadać certyfikaty niezależnych laboratoriów.
3. Program powinien zapewniać ochronę przed wszystkimi rodzajami wirusów, trojanów, narzędzi hakerskich, oprogramowania typu spyware i adware, auto-dialerami i innymi potencjalnie niebezpiecznymi programami.
4. Program musi posiadać możliwość określenia listy reguł wykluczeń dla wybranych obiektów, rodzajów zagrożeń oraz składników ochrony.
5. Program ma możliwość skanowania i klasyfikowania plików na podstawie informacji gromadzonych w oparciu o technologię chmury.
6. Program ma możliwość wyświetlenia podsumowania o aktywności, reputacji i lukach w aplikacjach aktualnie uruchomionych w systemie.
7. Program ma możliwość monitorowania prób uruchamiania aplikacji przez użytkowników zgodnie z określonymi regułami.
8. Program ma możliwość klasyfikacji wszystkich aplikacji i możliwość ograniczenia ich działania na podstawie ich stanu.
9. Użytkownik, ma możliwość wysłania do administratora zgłoszenia z prośbą o umożliwienie dostępu do zablokowanej aplikacji.
10. Wbudowany moduł zapobiegający wykorzystaniu luk w aplikacjach zainstalowanych na stacji roboczej oraz w samym systemie operacyjnym.
11. Wbudowany moduł chroniący pamięć procesów systemowych
12. Ochrona przed wszystkimi typami wirusów, robaków i koni trojańskich a także złośliwym kodem.
13. Możliwość wykrywania oprogramowania szpiegowskiego, pobierającego reklamy, programów podwyższonego ryzyka oraz narzędzi hakerskich.
14. Wbudowany moduł wyszukiwania heurystycznego bazującego na analizie kodu potencjalnego wirusa.
15. Możliwość określenia poziomu czułości modułu heurystycznego.
16. Moduł zapory ogniowej 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.

1. Ochrona przed niebezpiecznymi rodzajami aktywności sieciowej i atakami, możliwość tworzenia reguł wykluczających dla określonych adresów/zakresów IP.
2. Centralne zbieranie i przetwarzanie alarmów w czasie rzeczywistym.
3. Leczenie i usuwanie plików z archiwów następujących formatów RAR, ARJ, ZIP, CAB, LHA, JAR i ICE.
4. Możliwość zablokowania dostępu do ustawień programu dla użytkowników nie posiadających uprawnień administracyjnych.
5. Terminarz pozwalający na planowanie zadań, w tym także terminów automatycznej aktualizacji baz sygnatur.
6. Monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego.
7. 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.
8. Możliwość dynamicznej zmiany użycia zasobów systemowych w zależności od obciążenia systemu przez aplikacje użytkownika.
9. Program posiada funkcję chroniącą pliki, foldery i klucze rejestru wykorzystywane przez program przed zapisem i modyfikacją.
10. Program ma posiadać możliwość wyłączenia zewnętrznej kontroli usługi antywirusowej.
11. Program ma posiadać możliwość zresetowania wszystkich ustawień włącznie z regułami stworzonymi przez użytkownika.
12. Program musi posiadać możliwość zablokowania operacji zamykania programu, zatrzymywania zadań, wyłączania ochrony, wyłączania profilu administracyjnego, zmiany ustawień, usunięcia licencji oraz odinstalowania programu przy użyciu zdefiniowanej nazwy użytkownika i hasła.
13. Program powinien zapewnić autoryzację urządzeń typu klawiatura podłączanych do portu USB.
14. Jeżeli podłączane urządzenie nie posiada fizycznych klawiszy np. czytnik kodów kreskowych, program powinien zapewnić możliwość autoryzacji urządzenia przy użyciu klawiatury ekranowej.
15. Program powinien posiadać wbudowany moduł do obsługi technologii AMSI firmy Microsoft.
16. W przypadku wykrycia wirusa monitor antywirusowy może automatycznie:

* Podejmować zalecane działanie czyli próbować leczyć, a jeżeli nie jest to możliwe usuwać obiekt
* Rejestrować w pliku raportu informację o wykryciu wirusa
* Powiadamiać administratora przy użyciu poczty elektronicznej lub poleceniem NET SEND
* Utworzyć kopie zapasową przed podjęciem próby leczenia lub usunięcia zainfekowanego pliku

1. Skaner antywirusowy może być uruchamiany automatycznie zgodnie z terminarzem; skanowane są wszystkie lokalne dyski twarde komputera.
2. System antywirusowy ma posiadać możliwość skanowania archiwów i plików spakowanych niezależnie od poziomu ich zagnieżdżenia.
3. Program powinien posiadać możliwość określenia harmonogramu pobierania uaktualnień, w tym możliwość wyłączenia aktualizacji automatycznej.
4. Program musi posiadać możliwość pobierania uaktualnień modułów dla zainstalowanej wersji aplikacji.
5. Program powinien posiadać możliwość określenia źródła uaktualnień.
6. Program musi posiadać możliwość określenia katalogu, do którego będzie kopiowany zestaw uaktualnień po zakończeniu aktualizacji.
7. Program musi posiadać możliwość cofnięcia ostatniej aktualizacji w przypadku uszkodzenia zestawu uaktualnień.
8. Program musi posiadać możliwość określenia ustawień serwera proxy w przypadku, gdy jest on wymagany do nawiązania połączenia z Internetem.
9. Pobieranie uaktualnień w trybie przyrostowym (np. po zerwaniu połączenia, bez konieczności retransmitowania już wczytanych fragmentów informacji).
10. Program powinien posiadać możliwość zarządzania funkcją BitLocker systemów Windows
11. Program powinien posiadać możliwość określenia okresu przechowywania raportów.
12. Program powinien posiadać możliwość określenia okresu przechowywania obiektów znajdujących się w magazynie kopii zapasowych.
13. Program musi posiadać możliwość wyłączenia zaplanowanych zadań skanowania podczas pracy na bateriach.
14. Program musi posiadać możliwość wyeksportowania bieżącej konfiguracji programu w celu jej późniejszego zaimportowania na tym samym lub innym komputerze.
15. Program musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju.
16. Program musi mieć możliwość włączenia opcji współdzielenia zasobów z innymi aplikacjami.

# III. Konsola

1. System scentralizowanego zarządzania powinien obsługiwać następujące systemy operacyjne:

Microsoft Windows 10 pro / home 32-bitowy/64-bitowy

Microsoft Windows 7 Professional z pakietem Service Pack 1 i nowszym 32 / 64-bitowy

Windows Server 2019 Standard / Core / Datacenter 64-bitowy

Windows Server 2016 Server Standard / Datacenter / Core 64-bitowy

Windows Server 2012 R2 Standard / Server Core / Essentials / Datacenter 64-bitowy

Windows Server 2012 Standard / Server Core / Essentials / Datacenter 64-bitowy

1. System scentralizowanego zarządzania powinien przechowywać ustawienia w relacyjnej bazie danych:

Microsoft SQL Server 2012 Express 64-bitowy

Microsoft SQL Server 2014 Express 64-bitowy

Microsoft SQL Server 2016 Express 64-bitowy

Microsoft SQL Server 2017 Express 64-bitowy

Microsoft SQL Server 2019 Express 64-bitowy

Microsoft SQL Server 2014 (wszystkie wersje) 64-bitowy

Microsoft SQL Server 2016 (wszystkie wersje) 64-bitowy

Microsoft SQL Server 2017 (wszystkie wersje) na 64-bitowy system Windows

Microsoft SQL Server 2017 (wszystkie wersje) na 64-bitowy system Linux

Microsoft SQL Server 2019 (wszystkie edycje) na 64-bitowy system Windows (wymaga dodatkowych działań)

Microsoft SQL Server 2019 (wszystkie edycje) na 64-bitowy system Linux (wymaga dodatkowych działań)

MySQL Standard Edition 5.7 32-bitowy/64-bitowy

MySQL Enterprise Edition 5.7 32-bitowy/64-bitowy

Wszystkie obsługiwane wersje serwera SQL w platformach chmury Amazon RDS i Microsoft Azure

MariaDB Server 10.3 32-bitowy/64-bitowy z silnikiem magazynowania InnoDB

1. System zdalnego zarządzania powinien posiadać polskojęzyczny interfejs konsoli programu.
2. System zdalnego zarządzania powinien umożliwiać automatyczne umieszczenie komputerów w grupach administracyjnych odpowiadających strukturze sieci (grupy robocze sieci Microsoft Windows i/lub struktura Active Directory).
3. System zdalnego zarządzania powinien umożliwiać automatyczne umieszczanie stacji roboczych w określonych grupach administracyjnych w oparciu o zdefiniowane reguły.
4. System zdalnego zarządzania powinien posiadać jeden pakiet instalacyjny dla stacji roboczej jak również systemów serwerowych.
5. 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.
6. System zdalnego zarządzania umożliwia tworzenie hierarchicznej struktury serwerów administracyjnych jak również tworzenie wirtualnych serwerów administracyjnych.
7. System zdalnego zarządzania umożliwia zarządzanie stacjami roboczymi i serwerami plików Windows, nawet wtedy, gdy znajdują się one za zaporą NAT/Firewall.
8. Komunikacja pomiędzy serwerem zarządzającym a agentami sieciowymi na stacjach roboczych jest szyfrowana przy użyciu protokołu SSL.
9. Konsola administracyjna ma posiadać możliwość zdalnego inicjowania skanowania antywirusowego na stacjach roboczych włączonych do sieci komputerowych w całej firmie.
10. Zarządzanie aplikacjami odbywa się przy użyciu profili aplikacji oraz zadań.
11. Konsola administracyjna ma możliwość informowania administratorów o wykryciu epidemii wirusa.
12. Serwer zarządzający ma możliwość automatycznej reakcji na epidemie wirusa (automatyczne stosowanie wskazanego profilu ustawień stacji roboczych oraz uruchomienia odpowiednich zadań).
13. System centralnego zarządzania wyposażony w mechanizmy raportowania i dystrybucji oprogramowania oraz polityk antywirusowych w sieciach korporacyjnych.
14. System centralnej dystrybucji i instalacji aktualizacji bibliotek sygnatur wirusów, który umożliwia automatyczne, niewidoczne dla użytkownika przesłanie i zainstalowanie nowej wersji biblioteki.
15. System centralnej dystrybucji i instalacji aktualizacji oprogramowania, który umożliwia automatyczne, niewidoczne dla użytkownika przesłanie i zainstalowanie nowego oprogramowania.
16. Po instalacji oprogramowania antywirusowego nie jest wymagane ponowne uruchomienie komputera do prawidłowego działania programu.
17. System centralnego zarządzania powinien zapewniać obsługę trybu dynamicznego dla Virtual Desktop Infrastructure (VDI).
18. System centralnego zbierania informacji i tworzenia sumarycznych raportów.
19. System zdalnego zarządzania powinien umożliwiać automatyczne wysyłanie raportów pocztą elektroniczną lub zapisywanie ich w postaci plików w zdefiniowanej lokalizacji (przynajmniej w formatach HTML, XML i PDF).
20. System zdalnego zarządzania powinien umożliwiać podgląd w czasie rzeczywistym statystyk ochrony, stanu aktualizacji instalacji w sieci itp.
21. System zdalnego zarządzania powinien umożliwiać tworzenie kategorii aplikacji i warunków ich uruchomienia.
22. System zdalnego zarządzania powinien umożliwiać przeglądanie informacji o aplikacjach i plikach wykonywalnych znajdujących się na stacjach roboczych.
23. Program powinien mieć możliwość dezinstalacji aplikacji niekompatybilnych jak również dowolnej aplikacji znajdującej się w rejestrze aplikacji użytkownika.
24. System zdalnego zarządzania powinien wyświetlać szczegółowe informacje na temat luk w oprogramowaniu wykrytych na zarządzanych komputerach oraz ich naprawę.
25. Program powinien dać możliwość kontrolowania na stacjach roboczych aktualizacji systemowych oraz ich instalację.
26. System zdalnego zarządzania powinien mieć możliwość zbierania informacji o sprzęcie zainstalowanym na komputerach klienckich.
27. System zdalnego zarządzania powinien umożliwiać przeglądanie informacji o obiektach poddanych kwarantannie oraz podejmowanie odpowiednich działań (np. przywracanie, skanowanie itp.).
28. System zdalnego zarządzania powinien 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.
29. System zdalnego zarządzania powinien umożliwiać przeglądanie informacji o obiektach, które zostały wykryte ale program nie podjął względem nich żadnego działania wraz z możliwością wymuszenia przez administratora odpowiedniego działania.
30. System zdalnego zarządzania powinien umożliwiać automatyczne instalowanie licencji na stacjach roboczych.
31. System zdalnego zarządzania powinien umożliwiać automatyczne i regularne tworzenie kopii zapasowej serwera zarządzającego, która umożliwi przywrócenie w pełni działającego systemu zarządzania.
32. System zdalnego zarządzania powinien umożliwiać automatyczne uruchomienie wyłączonych komputerów przed wykonaniem odpowiednich zadań administracyjnych (z wykorzystaniem funkcji Wake-On-LAN) a po zakończeniu wykonywania zadań ich wyłączenie. Funkcjonalność ta nie może być ograniczona tylko do podsieci, w której znajduje się serwer administracyjny.
33. System zdalnego zarządzania powinien umożliwiać wysłanie do stacji roboczych komunikatu o dowolnie zdefiniowanej treści.
34. System zdalnego zarządzania powinien umożliwiać zdalne włączanie, wyłączanie oraz restartowanie komputerów wraz z możliwością interakcji z użytkownikiem (np. natychmiastowe wykonanie działania lub jego odłożenie na zdefiniowany okres czasu).
35. Program powinien umożliwiać ukrycie przed użytkownikiem interfejsu aplikacji, ikony w pasku systemowym, wpisów w Menu Start oraz na liście zainstalowanych programów.
36. Program powinien umożliwić administratorowi wyłączenie niektórych lub wszystkich powiadomień wyświetlanych na stacjach roboczych.
37. System zdalnego zarządzania powinien umożliwiać administrację poprzez przeglądarkę internetową.
38. System zdalnego zarządzania powinien dać możliwość wykorzystania bramy połączenia dla komputerów, które nie mają bezpośredniego połączenia z Serwerem administracyjnym.
39. System zdalnego zarządzania powinien mieć możliwość sprawdzenia aktualnych wersji oprogramowania antywirusowego.
40. System zdalnego zarządzania powinien umożliwiać przechwytywanie i instalację obrazów systemu operacyjnego.
41. Do przechwytywania obrazów systemów operacyjnych Windows system zdalnego zarządzania powinien wykorzystywać bezpłatne narzędzia producenta OS.
42. System zdalnego zarządzania powinien umożliwić zdefiniowanie własnej listy serwerów PXE oraz dodawanie lub importowanie adresów MAC komputerów docelowych.
43. System zdalnego zarządzania powinien umożliwić dodawanie własnych sterowników do obrazu preinstalacyjnego OS.
44. System zdalnego zarządzania powinien zawierać predefiniowaną listę aplikacji firm trzecich umożliwiającą automatyczne pobranie i utworzenie pakietu instalacyjnego.
45. System zdalnego zarządzania powinien zapewnić pobieranie i instalację poprawek lub uaktualnień aplikacji firm trzecich.
46. System zdalnego zarządzania powinien umożliwić wykorzystanie go jako serwer aktualizacji systemu Windows (WSUS).
47. System zdalnego zarządzania w trybie WSUS powinien umożliwiać konfigurację typu aktualizacji, wersji językowych oraz aplikacji i systemów, dla których będą pobierane poprawki.
48. System zdalnego zarządzania w trybie WSUS powinien umożliwiać zatwierdzanie lub odrzucanie wybranych poprawek.
49. System zdalnego zarządzania w trybie WSUS powinien umożliwiać instalację wszystkich, wybranych lub tylko zatwierdzonych poprawek.
50. System zdalnego zarządzania powinien umożliwić dodawanie i kontrolę licencji aplikacji firm trzecich. Kontrolowana powinna być zarówno ilość jak i okres ważności licencji.
51. System zdalnego zarządzania powinien tworzyć listę kont użytkowników sieci. Do tworzenia powinny być wykorzystywane różne źródła w tym min. AD, kontrolery domen oraz lokalne konta na komputerach.
52. System zdalnego zarządzania powinien umożliwić wysyłanie powiadomień do wybranych użytkowników przy użyciu poczty elektronicznej lub wiadomości SMS.
53. System zdalnego zarządzania powinien umożliwić instalowanie certyfikatów na urządzeniach mobilnych wybranych użytkowników.
54. System zdalnego zarządzania powinien umożliwić instalowanie certyfikatów iOS MDM na urządzeniach mobilnych wybranych użytkowników.
55. System zdalnego zarządzania powinien tworzyć repozytorium sprzętu w tym min. komputerów i nośników wymiennych.
56. Administrator powinien mieć możliwość dopisywania informacji do sprzętu w repozytorium w tym min. numeru ewidencyjnego, numeru seryjnego, producenta, daty zakupu, aktualnego użytkownika.
57. Administrator powinien mieć możliwość zaznaczenia czy urządzenie jest lub nie jest aktualnie wykorzystywane.
58. Administrator powinien mieć możliwość oznaczania urządzeń jako firmowe.
59. System zdalnego zarządzania powinien umożliwić zarządzanie urządzeniami mobilnymi z wykorzystaniem serwerów Exchange ActiveSync i iOS MDM.
60. Zarządzanie urządzeniami przenośnymi Exchange ActiveSync powinno umożliwiać przypisywanie ustawień do wybranych kont pocztowych. Ustawienia powinny obejmować w zależności od systemu operacyjnego przynajmniej synchronizacje poczty, korzystanie z określonych aplikacji, ustawienie hasła użytkownika, szyfrowanie danych.
61. Zarządzanie urządzeniami przenośnymi iOS MDM powinno umożliwiać przynajmniej dodawanie i zmienianie profili konfiguracji, instalować profile zabezpieczeń, instalować aplikacje na urządzeniu przenośnym, zablokować urządzenie przenośne, zresetować hasło urządzenia lub usunąć z niego wszystkie dane.
62. System zdalnego zarządzania powinien umożliwiać definiowanie reguł szyfrowania na stacjach roboczych (długość i złożoność hasła, blokada hasła, szyfrowanie dysków, plików, folderów, nośników wymiennych itd.).
63. System zdalnego zarządzania powinien pozwalać na zaszyfrowanie dysku za pomocą narzędzia BitLocker.
64. Dla zaszyfrowanych dysków system powinien umożliwiać automatyczne tworzenie kont autoryzacji dla wszystkich aktywnych kont na komputerach, kont domenowych i lokalnych, lokalnego administratora i aktywnego konta.
65. Dla zaszyfrowanych dysków system powinien umożliwiać odzyskiwanie haseł dostępu do dysków.
66. Dla nośników wymiennych system musi umożliwiać wymuszenie szyfrowania całego nośnika, wszystkich plików oraz tylko nowych plików.
67. Dla nośników wymiennych powinien być dostępny tryb przenośny umożliwiający odczyt zaszyfrowanych plików na dowolnym komputerze (również bez modułu szyfrującego).
68. System zdalnego zarządzania powinien umożliwiać definiowanie niestandardowych reguł szyfrowania dla wybranych nośników. Wybór nośników powinien być możliwy spośród wszystkich nośników zarejestrowanych na serwerze administracyjnym lub tylko z nośników dozwolonych w module kontroli urządzeń.
69. W całym okresie trwania subskrypcji użytkownik ma prawo do korzystania z bezpłatnej pomocy technicznej świadczonej za pośrednictwem telefonu i poczty elektronicznej.

W całym okresie trwania subskrypcji użytkownik musi mieć możliwość pobierania i instalacji nowszych wersji oprogramowania i konsoli zarządzającej.