MINIMALNE WYMAGANE PARAMETRY TECHNICZNE

I. Wymagania dla stacji roboczych

Wymagania sprzętowe i systemowe

Program musi wspierać następujące platformy:

- *Microsoft Windows 10 Pro x86 / x64*
- *Microsoft Windows 8.1 Pro x86 / x64*
- *Microsoft Windows 8 Pro x86 / x64*
- *Microsoft Windows 7 Professional x86 / x64*
- *Microsoft Windows Vista x86 / x64 SP2*
- *Microsoft Windows XP Professional x86 SP3*

Oprogramowanie musi mieć możliwość uruchomienia i być w pełni funkcjonalny na sprzęcie o minimalnych wymaganiach:

- *Intel Pentium 1 GHz (lub podobnej klasy)*
- *1 GB wolnej pamięci RAM*
- *2 GB wolnego miejsca na dysku*
- *Microsoft Internet Explorer 7.0 lub nowszy*
- *Microsoft Windows Installer 3.0 lub nowszy*

Informacje ogólne

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.*

Ochrona w czasie rzeczywistym

1. *Program ma możliwość skanowania i klasyfikowania plików oraz odsyłaczy do zasobów sieciowych na podstawie informacji gromadzonych w oparciu o technologię chmury.*
2. *Program ma możliwość wyświetlenia podsumowania o aktywności, reputacji i lukach w aplikacjach aktualnie uruchomionych w systemie.*
3. *Program ma możliwość monitorowania prób uruchamiania aplikacji przez użytkowników zgodnie z określonymi regułami.*
4. *Program ma możliwość klasyfikacji wszystkich aplikacji i możliwość ograniczenia ich działania na podstawie ich stanu. Program posiada dedykowany moduł blokujący określone kategorie urządzeń (np. pamięci masowe, urządzenia Bluetooth itp.).*
5. *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.*
6. *Możliwość utworzenia listy zaufanych urządzeń na podstawie modelu, bądź identyfikatora urządzenia dla określonego konta użytkownika systemu Windows.*
7. *Użytkownik, ma możliwość wysłania do administratora zgłoszenia z prośbą o umożliwienie dostępu do zablokowanego urządzenia; nośnik wymienny, napęd CD-ROM itd.*
8. *Użytkownik, ma możliwość wysłania do administratora zgłoszenia z prośbą o umożliwienie dostępu do zablokowanego zasobu sieciowego.*
9. *Użytkownik, ma możliwość wysłania do administratora zgłoszenia z prośbą o umożliwienie dostępu do zablokowanej aplikacji.*
10. *Kontrola sieci – kontrola dostępu do zasobów sieciowych w zależności od ich zawartości i lokalizacji:*
11. *Możliwość definiowania reguł filtrujących zawartość na wybranej stronie lub wszystkich stronach w zależności od kategorii zawartości: pornografia, narkotyki, broń, gry, sieci społecznościowe, banery, itd.*
12. *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.*
13. *Monitor wykrywania luk w aplikacjach zainstalowanych na stacji roboczej oraz w samym systemie operacyjnym.*
14. *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).*
15. *Możliwość wykrywania oprogramowania szpiegowskiego, pobierającego reklamy, programów podwyższonego ryzyka oraz narzędzi hakerskich.*
16. *Wbudowany moduł skanujący protokoły POP3, SMTP, IMAP i NNTP niezależnie od klienta pocztowego.*
17. *Skaner poczty powinien mieć możliwość zmiany nazwy lub usuwania określonych typów załączników.*

18. *Wbudowany moduł skanujący ruch HTTP w czasie rzeczywistym niezależnie od przeglądarki.*
19. *Wbudowany moduł wyszukiwania heurystycznego bazującego na analizie kodu potencjalnego wirusa.*
20. *Wbudowany moduł skanujący ruch komunikatorów ICQ, MSN, AIM, Mail.Ru Agent oraz IRC.*
21. *Możliwość określenia poziomu czułości modułu heurystycznego.*
22. *Wbudowany moduł skanujący skrypty napisane w językach VB Script i Java Script wykonywane przez system operacyjny Windows oraz program Internet Explorer.*
23. *Wbudowany moduł kontrolujący dostęp do rejestru systemowego.*
24. *Wbudowany moduł kontrolujący dostęp do ustawień Internet Explorer.*
25. *Wbudowany moduł chroniący przed phishingiem.*
26. *Moduł zapory ogniowej z możliwością:*
27. *Tworzenia reguł monitorowania aktywności sieciowej dla wszystkich zainstalowanych aplikacji, w oparciu o charakterystyki pakietów sieciowych i podpis cyfrowy aplikacji.*
28. *Tworzenia nowych zestawów warunków i działań wykonywanych na pakietach sieciowych oraz strumieniach danych dla określonych protokołów, portów i adresów IP.*
29. *Zdefiniowania zaufanych podsieci, dla których nie będą stosowane żadne reguły zapory.*
30. *Ochrona przed niebezpiecznymi rodzajami aktywności sieciowej i atakami, możliwość tworzenia reguł wykluczających dla określonych adresów/zakresów IP.*
31. *Kontrola systemu poprzez ochronę pro aktywną przed nowymi zagrożeniami, które nie znajdują się w antywirusowych bazach danych:*
32. *Kontrola aktywności aplikacji, dostarczanie szczegółowych informacji dla innych modułów aplikacji w celu zapewnienia jeszcze bardziej efektywnej ochrony.*
33. *Możliwość wycofywania zmian wprowadzanych w systemie przez szkodliwe oprogramowanie nawet w poprzednich sesjach logowania.*
34. *Centralne zbieranie i przetwarzanie alarmów w czasie rzeczywistym.*
35. *Leczenie i usuwanie plików z archiwów następujących formatów RAR, ARJ, ZIP, CAB, LHA, JAR i ICE.*
36. *Możliwość zablokowania dostępu do ustawień programu dla użytkowników nie posiadających uprawnień administracyjnych.*
37. *Terminarz pozwalający na planowanie zadań, w tym także terminów automatycznej aktualizacji baz sygnatur.*
38. *Możliwość wysłania podejrzanego obiektu do producenta oprogramowania antywirusowego w celu analizy.*
39. *Monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego.*
40. *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.*
41. *Możliwość dynamicznej zmiany użycia zasobów systemowych w zależności od obciążenia systemu przez aplikacje użytkownika.*
42. *Program posiada funkcję chroniącą pliki, foldery i klucze rejestru wykorzystywane przez program przed zapisem i modyfikacją.*
43. *Program posiada możliwość wyłączenia zewnętrznej kontroli usługi antywirusowej.*
44. *Program posiada możliwość zresetowania wszystkich ustawień włącznie z regułami stworzonymi przez użytkownika.*
45. *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.*
46. *Program ma możliwość zdefiniowania portów, które będą monitorowane lub wykluczone z monitorowania przez moduły skanujące ruch sieciowy (z wyłączeniem zapory ogniowej).*
47. *Program powinien zapewnić autoryzację urządzeń typu klawiatura podłączanych do portu USB.*
48. *Jeżeli podłączane urządzenie nie posiada fizycznych klawiszy np. czytnik kodów kreskowych, program powinien zapewnić możliwość autoryzacji urządzenia przy użyciu klawiatury ekranowej.*

Skanowanie na żądanie

1. *Skanowanie w czasie rzeczywistym:*
2. *Uruchamianych, otwieranych, kopiowanych, przenoszonych lub tworzonych plików.*
3. *Pobieranej z Internetu poczty elektronicznej (wraz z załącznikami) po protokołach POP3, SMTP, IMAP i NNTP niezależnie od klienta pocztowego.*
4. *Plików pobieranych z Internetu po protokole HTTP.*
5. *Poczty elektronicznej przetwarzanej przez program MS Outlook niezależnie od wykorzystywanego protokołu pocztowego.*
6. *Treści i plików przesyłanych z wykorzystaniem komunikatorów ICQ, MSN, AIM, Yahoo!, Jabber, Google Talk,*

Mail.Ru Agent oraz IRC.

7. *W przypadku wykrycia wirusa monitor antywirusowy może automatycznie:*
8. *Podejmować zalecane działanie czyli próbować leczyć, a jeżeli nie jest to możliwe usuwać obiekt*
9. *Rejestrować w pliku raportu informację o wykryciu wirusa*
10. *Powiadamiać administratora przy użyciu poczty elektronicznej lub poleceniem NET SEND*
11. *Utworzyć kopie zapasową przed podjęciem próby leczenia lub usunięcia zainfekowanego pliku*
12. *Poddać kwarantannie podejrzany obiekt*
13. *Skaner antywirusowy może być uruchamiany automatycznie zgodnie z terminarzem; skanowane są wszystkie lokalne dyski twarde komputera.*
14. *Informowanie o wykryciu podejrzanych działań uruchamianych aplikacji (np. modyfikacje rejestru, wtargnięcie do innych procesów) wraz z możliwością zezwolenia lub zablokowania takiego działania.*
15. *System antywirusowy posiada możliwość skanowania archiwów i plików spakowanych niezależnie od poziomu ich zagnieżdżenia.*

Aktualizacja baz danych sygnatur zagrożeń

1. *Program powinien posiadać możliwość określenia harmonogramu pobierania uaktualnień, w tym możliwość wyłączenia aktualizacji automatycznej.*
2. *Program musi posiadać możliwość pobierania uaktualnień modułów dla zainstalowanej wersji aplikacji.*
3. *Program powinien posiadać możliwość określenia źródła uaktualnień.*
4. *Program musi posiadać możliwość określenia katalogu, do którego będzie kopiowany zestaw uaktualnień po zakończeniu aktualizacji.*
5. *Program musi posiadać możliwość skanowania obiektów poddanych kwarantannie po zakończonej aktualizacji.*
6. *Program musi posiadać możliwość cofnięcia ostatniej aktualizacji w przypadku uszkodzenia zestawu uaktualnień.*
7. *Program musi posiadać możliwość określenia ustawień serwera Proxy w przypadku, gdy jest on wymagany do nawiązania połączenia z Internetem.*
8. *Antywirusowe bazy danych na serwerach producenta aktualizowane nie rzadziej niż raz na godzinę.*
9. *Pobieranie uaktualnień w trybie przyrostowym (np. po zerwaniu połączenia, bez konieczności retransmitowania już wczytanych fragmentów informacji).*

Szyfrowanie

1. *Program musi posiadać funkcjonalność szyfrowanie plików, folderów, dysków i nośników wymiennych.*
2. *Do szyfrowania musi być wykorzystywany algorytm AES.*
3. *Program powinien posiadać możliwość tworzenia zaszyfrowanych pakietów z poziomu menu kontekstowego.*
4. *Program powinien umożliwiać dostęp do zaszyfrowanych plików także na komputerach bez zainstalowanego oprogramowania szyfrującego.*
5. *Program musi posiadać funkcjonalność odzyskiwania danych z zaszyfrowanych nośników po utracie hasła lub w wyniku uszkodzenia nośnika.*
6. *Raportowanie*
7. *Program powinien posiadać możliwość raportowania zdarzeń informacyjnych.*
8. *Program powinien posiadać możliwość określenia okresu przechowywania raportów.*
9. *Program powinien posiadać możliwość określenia okresu przechowywania obiektów znajdujących się w magazynie kopii zapasowych oraz kwarantannie.*

Dodatkowa konfiguracja

1. *Program musi posiadać możliwość wyłączenia zaplanowanych zadań skanowania podczas pracy na bateriach.*
2. *Program musi posiadać możliwość wyeksportowania bieżącej konfiguracji programu w celu jej późniejszego zaimportowania na tym samym lub innym komputerze.*
3. *Program musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju.*
4. *Program musi mieć możliwość włączenia opcji współdzielenia zasobów z innymi aplikacjami.*

II. Wymagania dla stacji wyposażonych w system Microsoft Windows Server 2003

Wymagania sprzętowe i systemowe

1. *Program musi wspierać następujące systemy operacyjne:*
1. *Microsoft Windows Server 2003 Standard / Enterprise (SP2)*
2. *Program musi wspierać następujące serwery terminalowe:*
3. *Windows Server 2003 Terminal Server*

Informacje ogólne

1. *Program powinien posiadać certyfikaty:*
    - *West Coast Labs*
    - *VMware Ready*
    - *Citrix ready*
    - *Certified for Windows Server 2008 R2*

2. *Program powinien zapewniać ochronę przed wszystkimi rodzajami wirusów, trojanów, narzędzi hakerskich, oprogramowania typu spyware i adware, auto-dialerami i innymi potencjalnie niebezpiecznymi programami.*

Ochrona antywirusowa

1. *Program musi posiadać moduł ochrony w czasie rzeczywistym skanujący pliki, alternatywne strumienie danych NTFS, sektor MBR oraz sektory startowe dysków twardych i nośników wymiennych.*
2. *Program musi posiadać moduł analizatora skryptów w językach VBScript oraz JScript umożliwiający przerwanie działanie skryptu w momencie wykrycia podejrzanego zachowania.*
3. *Program powinien posiadać wbudowany moduł wyszukiwania heurystycznego bazującego na analizie kodu potencjalnego wirusa.*
4. *Program musi umożliwiać uruchomienie działania ochrony w czasie rzeczywistym i analizatora skryptów zgodnie z terminarzem.*
5. *Program musi posiadać możliwość wstrzymania działania ochrony w czasie rzeczywistym i analizatora skryptów po określonym czasie od jej uruchomienia lub w określonych godzinach.*
6. *Program musi mieć możliwość dostosowania zakresu ochrony w czasie rzeczywistym, tak aby monitorowane były tylko wybrane foldery.*
7. *Program musi mieć możliwość konfiguracji ochrony czasie rzeczywistym tak, aby monitorowane były jedynie pliki o określonych rozszerzeniach.*
8. *Program musi posiadać moduł skanowania na żądanie pozwalający na definiowanie zadań skanowania wybranych obszarów dysku.*
9. *Program musi mieć możliwość zdefiniowania akcji jakie mają być wykonywane na obiektach zainfekowanych oraz podejrzanych.*
10. *Program musi umożliwiać konfigurację podejmowanych akcji w zależności od typu wykrytego zagrożenia.*
11. *Program musi posiadać funkcję wykluczania obiektów ze skanowania na podstawie ich nazwy.*
12. *Program musi posiadać funkcję wykluczania obiektów ze skanowania na podstawie nazwy zagrożenia jakie jest w nich wykrywane.*
13. *Program podczas startu systemu musi skanować:*
    - *główny sektor rozruchowy (MBR)*
    - *sektory rozruchowe wszystkich nośników wymiennych*
    - *pamięć operacyjną komputera*
14. *W przypadku wykrycia wirusa program powinien automatycznie:*
    - *podejmować zalecane działanie czyli próbować leczyć, a jeżeli nie jest to możliwe to usuwać obiekt*
    - *rejestrować w pliku raportu informację o wykryciu wirusa*
    - *utworzyć kopie zapasową przed podjęciem próby leczenia lub usunięcia zainfekowanego pliku*
    - *poddać kwarantannie podejrzany obiekt*
15. *Program powinien posiadać możliwość skanowania tylko nowych i zmienionych plików.*
16. *Program powinien umożliwiać stworzenie list zaufanych procesów dla których nie będzie monitorowana aktywność plikowa.*
17. *Program powinien umożliwiać wykluczanie obiektów z procesu ochrony.*
18. *Program powinien mieć możliwość wykorzystania predefiniowanego zestawu wykluczeń rekomendowanych przez firmę Microsoft i producenta programu.*

Powiadomienia i raportowanie

1. *Program musi posiadać możliwość zapisywania zdarzeń z działania programu w lokalnym i systemowym dzienniku zdarzeń.*
2. *Program musi mieć możliwość eksportu zdarzeń z lokalnego dziennika zdarzeń do formatów CSV i TXT.*
3. *Program musi umożliwiać powiadamianie administratora na temat zaistniałych zdarzeń za pośrednictwem wiadomości mail, polecenia NET SEND lub pliku wykonywalnego.*
4. *Program powinien posiadać możliwość powiadamiania użytkowników terminalowych za pośrednictwem usług terminalowych.*
5. *Program powinien umożliwiać konfigurację tekstu dostarczanych powiadomień.*

Kopia zapasowa i kwarantanna

1. *Program musi posiadać system kwarantanny umożliwiający proste skanowanie, usuwanie i przywracanie do pierwotnej lub wybranej lokalizacji wybranych plików.*
2. *Program musi umożliwiać zdefiniowanie katalogu w którym przechowywana będzie baza kwarantanny i ustawienia maksymalnego jej rozmiaru.*
3. *Program musi posiadać moduł kopii zapasowej przechowujący pliki przetworzone przez program.*
4. *Program powinien posiadać możliwość wysłania podejrzanego obiektu do analizy w laboratorium zagrożeń z poziomu interfejsu programu.*

Aktualizacja baz danych sygnatur zagrożeń

1. *Program musi umożliwiać pobieranie aktualizacji baz zagrożeń oraz modułów programu pobierane z serwerów producenta, serwera administracyjnego lub wskazanego zasobu HTTP, FTP lub udostępnionego foldera.*
2. *Program musi posiadać odrębne i niezależne zadania aktualizacji baz zagrożeń oraz modułów programu.*
3. *Program powinien umożliwiać zdefiniowanie serwera Proxy wykorzystywanego do pobierania uaktualnień.*
4. *Program powinien umożliwiać zdefiniowanie konfiguracji konta systemowego z poświadczeniami którego zostanie uruchomione zadanie aktualizacji.*
5. *Program musi mieć możliwość uruchamiania zadania aktualizacji zgodnie z harmonogramem.*
6. *Program musi mieć możliwość konfiguracji automatycznej aktualizacji modułów programu lub jedynie powiadamianie o dostępności uaktualnień dla modułów.*
7. *Program musi mieć możliwość eksportu baz zagrożeń z programu w celu aktualizacji programu na innym komputerze.*
8. *Program musi mieć możliwość cofnięcia ostatniej aktualizacji baz zagrożeń.*

Zarządzanie i dodatkowa konfiguracja

1. *Program musi mieć możliwość konfiguracji uprawnień dostępu do poszczególnych funkcji programu.*
2. *Program musi posiadać możliwość konfiguracji liczby aktywnych procesów programu, procesów ochrony w czasie rzeczywistym i procesów skanowania na żądanie.*
3. *Program powinien posiadać możliwość przerwania działających i odroczenia zaplanowanych zadań skanowania jeśli komputer pracuje na zasilaniu awaryjnym.*
4. *Program powinien umożliwiać eksportowanie oraz importowanie ustawień.*
5. *Program powinien mieć możliwość zarządzania wieloma serwerami za pośrednictwem jednej konsoli.*
6. *Zarządzanie programem powinno być możliwe za pomocą dedykowanej konsoli zarządzającej oraz za pomocą konsoli administracyjnej służącej do centralnego zarządzania oprogramowaniem zabezpieczającym w sieci korporacyjnej.*
7. *Zarządzanie komputerem powinno być możliwe z poziomu wiersza poleceń.*

III. Wymagania dla stacji wyposażonych w system Microsoft Windows Server 2012 Standard

Wymagania sprzętowe i systemowe

1. *Program musi wspierać następujące systemy operacyjne:*
   - *Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter*
2. *Program musi wspierać następujące serwery terminalowe:*
   - *Windows 2012 Server Microsoft Remote Desktop Services*
   - *Microsoft Windows 2012 Server R2 Remote Desktop Services*

Informacje ogólne

1. *Program powinien posiadać certyfikaty:*
   - *VMware Ready*
   - *Citrix ready*
   - *Certified for Windows Server 2012 R2*
2. *Program powinien zapewniać ochronę przed wszystkimi rodzajami wirusów, trojanów, narzędzi hakerskich, oprogramowania typu spyware i adware, auto-dialerami i innymi potencjalnie niebezpiecznymi programami.*

Ochrona antywirusowa

1. *Program musi posiadać moduł ochrony w czasie rzeczywistym skanujący pliki, alternatywne strumienie danych NTFS, sektor MBR oraz sektory startowe dysków twardych i nośników wymiennych.*
2. *Program musi posiadać moduł analizatora skryptów w językach VBScript oraz JScript umożliwiający przerwanie działanie skryptu w momencie wykrycia podejrzanego zachowania.*
3. *Program powinien posiadać wbudowany moduł wyszukiwania heurystycznego bazującego na analizie kodu potencjalnego wirusa.*
4. *Program musi umożliwiać uruchomienie działania ochrony w czasie rzeczywistym i analizatora skryptów zgodnie z terminarzem.*
5. *Program musi posiadać możliwość wstrzymania działania ochrony w czasie rzeczywistym i analizatora skryptów po określonym czasie od jej uruchomienia lub w określonych godzinach.*
6. *Program musi mieć możliwość dostosowania zakresu ochrony w czasie rzeczywistym, tak aby monitorowane były tylko wybrane foldery.*
7. *Program musi mieć możliwość konfiguracji ochrony czasie rzeczywistym tak, aby monitorowane były jedynie pliki o określonych rozszerzeniach.*
8. *Program musi posiadać moduł skanowania na żądanie pozwalający na definiowanie zadań skanowania wybranych obszarów dysku.*

9. *Program musi mieć możliwość zdefiniowania akcji jakie mają być wykonywane na obiektach zainfekowanych oraz podejrzanych.*
10. *Program musi umożliwiać konfigurację podejmowanych akcji w zależności od typu wykrytego zagrożenia.*
11. *Program musi posiadać funkcję wykluczania obiektów ze skanowania na podstawie ich nazwy.*
12. *Program musi posiadać funkcję wykluczania obiektów ze skanowania na podstawie nazwy zagrożenia jakie jest w nich wykrywane.*
13. *Program podczas startu systemu musi skanować:*
    - *główny sektor rozruchowy (MBR)*
    - *sektory rozruchowe wszystkich nośników wymiennych*
    - *pamięć operacyjną komputera*
14. *W przypadku wykrycia wirusa program powinien automatycznie:*
    - *podejmować zalecane działanie czyli próbować leczyć, a jeżeli nie jest to możliwe to usuwać obiekt*
    - *rejestrować w pliku raportu informację o wykryciu wirusa*
    - *utworzyć kopie zapasową przed podjęciem próby leczenia lub usunięcia zainfekowanego pliku*
    - *poddać kwarantannie podejrzany obiekt*
15. *Program powinien posiadać możliwość skanowania tylko nowych i zmienionych plików.*
16. *Program powinien umożliwiać stworzenie list zaufanych procesów dla których nie będzie monitorowana aktywność plikowa.*
17. *Program powinien umożliwiać wykluczanie obiektów z procesu ochrony.*
18. *Program powinien mieć możliwość wykorzystania predefiniowanego zestawu wykluczeń rekomendowanych przez firmę Microsoft i producenta programu.*
19. *Program powinien zawierać moduł blokujący komputery, z których wykrył szkodliwą aktywność oraz czas ich blokowania.*
20. *Program powinien zawierać moduł wykrywający operacje szyfrowania plików na udostępnianych zasobach. W przypadku wykrycia takiego zachowania komputer, z którego nastąpiło takie zdarzenie powinien zostać zablokowany.*
21. *Program powinien zawierać moduł kontrolujący uruchamianie plików wykonywalnych oraz ładowanych bibliotek DLL.*
22. *Podczas tworzenia reguł dla modułu kontrolującego uruchamianie aplikacji program powinien wykorzystywać m.in.:*
    - *certyfikaty cyfrowe*
    - *skróty plików obliczone algorytmem SHA256*
    - *ścieżkę do pliku*
    - *konta użytkowników lub grupy systemu Windows*
    - *listy reguł w plikach XML*
    - *informacje o zablokowanych plikach z raportu narzędzia administracyjnego (konsoli administracyjnej)*
23. *Moduł kontrolujący uruchamianie aplikacji powinien pracować w jednym z dwóch trybów:*
    - *statystycznym – zbierane są tylko informacje o uruchamianych plikach*
    - *zgodnie ze zdefiniowanymi regułami*
24. *Moduł kontrolujący uruchamianie aplikacji powinien umożliwiać zastosowanie reguł do skryptów i pakietów MSI*

Powiadomienia i raportowanie

1. *Program musi posiadać możliwość zapisywania zdarzeń z działania programu w lokalnym i systemowym dzienniku zdarzeń.*
2. *Program musi mieć możliwość eksportu zdarzeń z lokalnego dziennika zdarzeń do formatów CSV i TXT.*
3. *Program musi umożliwiać powiadamianie administratora na temat zaistniałych zdarzeń za pośrednictwem wiadomości mail, polecenia NET SEND lub pliku wykonywalnego.*
4. *Program powinien posiadać możliwość powiadamiania użytkowników terminalowych za pośrednictwem usług terminalowych.*
5. *Program powinien umożliwiać konfigurację tekstu dostarczanych powiadomień.*

Kopia zapasowa i kwarantanna

1. *Program musi posiadać system kwarantanny umożliwiający proste skanowanie, usuwanie i przywracanie do pierwotnej lub wybranej lokalizacji wybranych plików.*
2. *Program musi umożliwiać zdefiniowanie katalogu w którym przechowywana będzie baza kwarantanny i ustawienia maksymalnego jej rozmiaru.*
3. *Program musi posiadać moduł kopii zapasowej przechowujący pliki przetworzone przez program.*
4. *Program powinien posiadać możliwość wysłania podejrzanego obiektu do analizy w laboratorium zagrożeń z poziomu interfejsu programu.*

Aktualizacja baz danych sygnatur zagrożeń

1. *Program musi umożliwiać pobieranie aktualizacji baz zagrożeń oraz modułów programu pobierane z serwerów producenta, serwera administracyjnego lub wskazanego zasobu HTTP, FTP lub udostępnionego foldera.*
2. *Program musi posiadać odrębne i niezależne zadania aktualizacji baz zagrożeń oraz modułów programu.*
3. *Program powinien umożliwiać zdefiniowanie serwera Proxy wykorzystywanego do pobierania uaktualnień.*
4. *Program powinien umożliwiać zdefiniowanie konfiguracji konta systemowego z poświadczeniami którego zostanie uruchomione zadanie aktualizacji.*
5. *Program musi mieć możliwość uruchamiania zadania aktualizacji zgodnie z harmonogramem.*
6. *Program musi mieć możliwość konfiguracji automatycznej aktualizacji modułów programu lub jedynie powiadamianie o dostępności uaktualnień dla modułów.*
7. *Program musi mieć możliwość eksportu baz zagrożeń z programu w celu aktualizacji programu na innym komputerze.*
8. *Program musi mieć możliwość cofnięcia ostatniej aktualizacji baz zagrożeń.*
9. *Aktualizacja baz powinna umożliwiać optymalizację ilości operacji I/O dysku.*

Zarządzanie i dodatkowa konfiguracja

1. *Program musi mieć możliwość konfiguracji uprawnień dostępu do poszczególnych funkcji programu.*
2. *Program musi posiadać możliwość konfiguracji liczby aktywnych procesów programu, procesów ochrony w czasie rzeczywistym i procesów skanowania na żądanie.*
3. *Program powinien posiadać możliwość przerwania działających i odroczenia zaplanowanych zadań skanowania jeśli komputer pracuje na zasilaniu awaryjnym.*
4. *Program powinien umożliwiać eksportowanie oraz importowanie ustawień.*
5. *Program powinien mieć możliwość zarządzania wieloma serwerami za pośrednictwem jednej konsoli.*
6. *Zarządzanie programem powinno być możliwe za pomocą dedykowanej konsoli zarządzającej oraz za pomocą konsoli administracyjnej służącej do centralnego zarządzania oprogramowaniem zabezpieczającym w sieci korporacyjnej.*
7. *Zarządzanie komputerem powinno być możliwe z poziomu wiersza poleceń.*

IV. Wymagania dla urządzeń mobilnych

Wymagania sprzętowe i systemowe

Android 4 – 7.1.1
iOS 7.0 – 10
Windows Phone 8, 8.1.
Windows 10 Mobile

Ogólne:

Możliwość zdalnego zarządzania.
Oprogramowanie musi posiadać możliwość integracji z Microsoft Exchange Active Sync. Możliwość tworzenia i zarządzania profilami poprzez Microsoft Exchange Active Sync.

Profile:

Oprogramowanie musi posiadać możliwość ustawienia w godzinach okresu synchronizacji z serwerem Exchange Active Sync.
Oprogramowanie musi posiadać możliwość konfiguracji hasła oraz jego ustawień.
musi posiadać możliwość konfiguracji synchronizacji zdarzeń kalendarza.
Oprogramowanie musi posiadać możliwość konfiguracji synchronizacji wiadomości e-mail.
Oprogramowanie musi posiadać możliwość ograniczenia wielkości wiadomości e-mail.
Oprogramowanie musi posiadać możliwość blokowania wiadomości e-mail w formacie HTML.
Oprogramowanie musi posiadać możliwość blokowania pobierania załączników z wiadomości e- mail na urządzenie oraz ograniczenie ich wielkości.

Zdalne zarządzanie:

Zdalne zarządzanie ustawieniami ochrony antywirusowej na urządzeniach mobilnych
Przeciwdziałanie wycieku lub kradzieży danych w przypadku zagubienia/kradzieży urządzenia
Kontrolowanie dostępnych zasobów internetowych.
Możliwość zdalnej instalacji oprogramowania firm trzecich
Powiadamianie administratora o zdarzeniach, które wystąpiły na urządzeniach mobilnych poprzez SMS lub wiadomość email.

Ochrona antywirusowa - Android

Skanowanie tylko nowych plików/aplikacji.
Możliwość włączenia ochrony systemu plików.
Skanowanie wszystkich otwieranych, modyfikowanych, przenoszonych, kopiowanych, uruchamianych oraz zapisywanych plików na urządzeniu przez użytkownika.
Skanowanie nowych aplikacji przed ich uruchomieniem, bazujące na usłudze w chmurze.
Oprogramowanie musi posiadać możliwość dodatkowego włączenia skanowania obiektów typu adware oraz riskware itp.
Oprogramowanie musi posiadać możliwość skanowania tylko plików wykonywalnych takich jak, EXE, DLL, MDL, APP, APK, RDL, PRT, PXT, LDD, PDD, CLASS, SO, ELF
Oprogramowanie musi posiadać możliwość wzbrania akcji która zostanie podjęta w przypadku niepowodzenia leczenia.

Możliwość zdalnego zresetowania PIN'u na urządzeniu mobilnym.

Możliwość definiowania ustawień aplikacji w oparciu o profile Android for Work.

Skanowanie – Android

Oprogramowanie musi posiadać możliwość skanowania tylko plików wykonywalnych takich jak, EXE, DLL, MDL, APP, APK, RDL, PRT, PXT, LDD, PDD, CLASS, SO, ELF.

Oprogramowanie musi posiadać możliwość skanowania archiwów takich jak: ZIP, JAR, JAD, SIS, SISX, CAB, APK

Oprogramowanie musi posiadać możliwość włączenia lub wyłączenia leczenia plików w przypadku gdy jest to możliwe.

Oprogramowanie musi posiadać możliwość wybrania akcji jaka będzie podjęta wobec wykrytego obiektu w sytuacji gdy leczenie nie jest możliwe.

Oprogramowanie musi posiadać możliwość zdefiniowania terminarza skanowania.

Oprogramowanie musi posiadać możliwość uruchomienia skanowania po pobraniu uaktualnień.

Aktualizacja – Android

Oprogramowanie musi posiadać możliwość włączenia lub wyłączenia pobierania aktualizacji w roamingu.

Oprogramowanie musi posiadać możliwość ręcznego zdefiniowania źródła aktualizacji.

Oprogramowanie musi posiadać możliwość ustawienia zadania aktualizacji zgodnie z terminarzem.

Moduł ochrony przed kradzieżą - Android

Oprogramowanie musi posiadać możliwość zdalnego zablokowania urządzenia.

Oprogramowanie musi posiadać możliwość zdalnego namierzenia oraz przesłania lokalizacji zagubionego urządzenia.

Oprogramowanie musi posiadać możliwość przesłania nowego numeru telefonu po zmianie karty SIM na podany wcześniej adres e-mail.

Oprogramowanie musi posiadać możliwość zablokowania urządzenia po zmianie karty SIM.

Oprogramowanie musi posiadać możliwość wprowadzenia własnego komunikatu który pojawi się po zablokowaniu urządzenia.

Oprogramowanie musi posiadać możliwość zdalnego usunięcia danych firmowych lub wszystkich danych z urządzenia.

Połączenie zdalne/Sieć - Android

Oprogramowanie musi posiadać możliwość ustawienia okresu synchronizacji z serwerem zdalnego zarządzania z możliwością wyłączenia synchronizacji w momencie gdy urządzenie pracuje w trybie roamingu.

Możliwość zablokowania wybranych stron internetowych zgodnie z utworzonymi kategoriami stron.

Kontenery – Android

Oprogramowanie musi posiadać możliwość zdefiniowania kontenerów w celu zabezpieczenia wrażliwych danych.

Oprogramowanie musi posiadać możliwość wybrania metody autoryzacji do danego kontenera np. hasło lub uprawnienia użytkownika domenowego.

Oprogramowanie musi posiadać możliwość zaszyfrowania zawartości kontenera.

Zarządzanie urządzeniem – Android

Oprogramowanie musi posiadać możliwość weryfikacji oraz informowania odnośnie hasła dla systemu operacyjnego gdy nie jest ustawione.

Oprogramowanie musi posiadać możliwość zdefiniowania minimalnej ilości znaków jaka jest wymagana podczas ustawiania hasła.

Oprogramowanie musi posiadać możliwość zablokowania Wifi.

Oprogramowanie musi posiadać możliwość zablokowania kamery.

Oprogramowanie musi posiadać możliwość zablokowania modułu Bluetooth.

Oprogramowanie musi posiadać możliwość zdefiniowania nazwy oraz poświadczeń dla sieci Wifi.

Kontrola aplikacji – Android

Oprogramowanie musi posiadać możliwość blokowania wybranych aplikacji lub kategorii aplikacji.

Oprogramowanie musi posiadać możliwość utworzenia listy zaufanych aplikacji.

Dodatkowe – Android

Kompatybilność z systemem Samsung Knox.

Możliwość konfiguracji zdarzeń oraz przesyłanie ich do administratora systemu.

IOS

Oprogramowanie musi posiadać możliwość zablokowania wybranych stron internetowych zgodnie z utworzonymi kategoriami stron.

Oprogramowanie musi posiadać możliwość wymuszenia profilu na urządzeniu z predefiniowanymi ustawieniami bezpieczeństwa.

Oprogramowanie musi posiadać możliwość zdalnego zablokowania/odblokowania urządzenia.

Oprogramowanie musi posiadać możliwość zdalnego usunięcia danych z urządzenia.

Oprogramowanie musi posiadać możliwość zdefiniowania hasła oraz jego parametrów na urządzeniu.

Oprogramowanie musi posiadać możliwość blokowania kamery.

Oprogramowanie musi posiadać możliwość blokowania FaceTime.

Oprogramowanie musi posiadać możliwość blokowania tworzenia zrzutów ekranu.

Oprogramowanie musi posiadać możliwość blokowania usługi Airdrop.

Oprogramowanie musi posiadać możliwość blokowania usługi iMessage.

Oprogramowanie musi posiadać możliwość blokowania połączeń głosowych.

Oprogramowanie musi posiadać możliwość blokowania asystenta Siri.

Oprogramowanie musi posiadać możliwość blokowania sklepu IBook.

Oprogramowanie musi posiadać możliwość blokowania instalacji aplikacji.

Oprogramowanie musi posiadać możliwość blokowania usuwania aplikacji.

Oprogramowanie musi posiadać możliwość blokowania opłat wewnętrznych w aplikacjach.

Oprogramowanie musi posiadać możliwość wymuszenia hasła podczas każdej próby zakupu w sklepie Itunes Store.
Oprogramowanie musi posiadać możliwość blokowania tworzenia kopii zapasowej w usłudze iCloud.
Oprogramowanie musi posiadać możliwość blokowania haseł usługi Icloud keychain.
Oprogramowanie musi posiadać możliwość blokowania udostępniania zdjęć w usłudze iCloud.
Oprogramowanie musi posiadać możliwość blokowania strumienia zdjęć My Photo Stream.
Oprogramowanie musi posiadać możliwość blokowania synchronizacji podczas roamingu,
Oprogramowanie musi posiadać możliwość włączenia szyfrowania kopii zapasowych.
Oprogramowanie musi posiadać możliwość zezwolenia na używanie niezaufanych certyfikatów TLS.
Oprogramowanie musi posiadać możliwość zezwolenia na automatyczną aktualizację zaufanych certyfikatów.
Oprogramowanie musi posiadać możliwość blokowania instalacji profilów konfiguracyjnych.
Oprogramowanie musi posiadać możliwość blokowania edycji ustawień konta.
Oprogramowanie musi posiadać możliwość blokowania ustawień usługi Find My Friend.
Oprogramowanie musi posiadać możliwość blokowania możliwości parowania z nieskonfigurowanymi hostami.
Oprogramowanie musi posiadać możliwość blokowania wysyłania materiałów diagnostycznych do firmy Apple.
Oprogramowanie musi posiadać możliwość blokowania Touch ID.
Oprogramowanie musi posiadać możliwość wymuszenia prośby o hasło podczas pierwszego połączenia AirPlay.
Oprogramowanie musi posiadać możliwość blokowania powiadomień ekranowych Passbook gdy ekran jest zablokowany.
Oprogramowanie musi posiadać możliwość blokowania Control Center gdy ekran jest zablokowany.
Oprogramowanie musi posiadać możliwość blokowania Notification Center gdy ekran jest zablokowany.
Oprogramowanie musi posiadać możliwość blokowania usługi Dzisiaj gdy ekran jest zablokowany.
Oprogramowanie musi posiadać możliwość blokowania Itunes Store.
Oprogramowanie musi posiadać możliwość blokowania Game Center.
Oprogramowanie musi posiadać możliwość blokowania Safari.
Oprogramowanie musi posiadać możliwość blokowania ciasteczek.
Oprogramowanie musi posiadać możliwość blokowania wybranych treści dla danego regionu świata.
Oprogramowanie musi posiadać możliwość zdefiniowania globalnych ustawień proxy.
Oprogramowanie musi posiadać możliwość tworzenia czarnej oraz białej listy stron internetowych.
Oprogramowanie musi posiadać możliwość zdefiniowania listy sieci Wifi wraz z konfiguracją.
Oprogramowanie musi posiadać możliwość dodania połączeń VPN wraz z konfiguracją.
Oprogramowanie musi posiadać możliwość dodania poświadczeń oraz zaufanych urządzeń dla usługi AirPlay.
Oprogramowanie musi posiadać możliwość zdefiniowania drukarek dla usługi AirPrint.
Oprogramowanie musi posiadać możliwość dodania kont e-mail.
Oprogramowanie musi posiadać możliwość dodania kont Exchange ActiveSync.
Oprogramowanie musi posiadać możliwość dodawania kont LDAP.
Oprogramowanie musi posiadać możliwość dodawania kont CalDAV.
Oprogramowanie musi posiadać możliwość dodawania kontaktów CardDAV.
Oprogramowanie musi posiadać możliwość dodawania subskrypcji kalendarza.
Oprogramowanie musi posiadać możliwość dodawania ikony typu WebClip.
*Oprogramowanie musi posiadać możliwość dodawania czcionek *.ttf, *.otf.*
Oprogramowanie musi posiadać możliwość dodawania certyfikatów.
Oprogramowanie musi posiadać możliwość dodawania profili SCEP.
Oprogramowanie musi posiadać możliwość dodawania konfiguracji Access Point.

Windows Phone 8, 8.1/10 Mobile

Oprogramowanie musi posiadać możliwość zlokalizowania urządzenia oraz przesłania geolokalizacji na podany adres e-mail.
Oprogramowanie musi posiadać możliwość ustawienia okresu synchronizacji z serwerem zdalnego zarządzania z możliwością wyłączenia synchronizacji w momencie gdy urządzenie pracuje w trybie roamingu.
Możliwość zablokowania wybranych stron internetowych zgodnie z utworzonymi kategoriami stron.

V. Wymagania dla systemów Linux

1. *Program musi wspierać co najmniej następujące platformy:*

32 bitowe:

- *Red Hat Enterprise Linux Server 6.x (6.0 – 6.6)*
- *Red Hat Enterprise Linux Server 5.x*
- *Fedora 14*
- *Canaima 3*
- *Asianux Server 3 SP4*
- *Asianux Server 4 SP1*
- *CentOS 6.x (6.0 - 6.6)*
- *CentOS 5.x*
- *SUSE Linux Enterprise Server 11 SP3 oraz SP1*
- *Novell Open Enterprise Server 2 SP3*
- *Ubuntu Server 12.04 LTS*
- *Ubuntu Server 14.04 LTS*
- *Ubuntu Server 14.10*

- *Ubuntu Server 10.04 LTS*
- *Oracle Linux 6.5*
- *Debian GNU/Linux 7.1, 7.5, 7.6, 7.7*
- *Debian GNU/Linux 6.0.5*
- *openSUSE® Linux 11.3*
- *Mandriva Enterprise Server 5.2*
- *FreeBSD 8.3*
- *FreeBSD 9.0*

64 bitowe:

- *Red Hat Enterprise Linux Server 6.x (6.0 - 6.6)*
- *Red Hat Enterprise Linux Server 7*
- *Canaima 3*
- *Asianux Server 3 SP4*
- *Asianux Server 4 SP1*
- *Fedora 14*
- *CentOS-6.x (6.0 - 6.6)*
- *CentOS-7.0*
- *CentOS-5.x*
- *SUSE Linux Enterprise Server 11 SP3 oraz SP1*
- *SUSE Linux Enterprise Server 12*
- *Novell Open Enterprise Server 11 SP1*
- *Novell Open Enterprise Server 11 SP2*
- *Novell Open Enterprise Server 2 SP3*
- *Ubuntu Server 12.04 LTS*
- *Ubuntu Server 14.04 LTS*
- *Ubuntu Server 14.10*
- *Ubuntu Server 10.04 LTS*
- *Oracle Linux 6.5*
- *Oracle Linux 7.0*
- *Debian GNU/Linux 7.1, 7.5, 7.6*
- *Debian GNU/Linux 6.0.5*
- *openSUSE 13.1*
- *openSUSE 11.3*
- *Red Hat Enterprise Linux Server 5.x*
- *FreeBSD 7.4*
- *FreeBSD 8.2*

Informacje ogólne

1. *Program powinien posiadać certyfikaty:*
   - *VMware Ready*
   - *RedHat Enterprise Linux Certified*
   - *Ready for SUSE Linux Enterprise Server*
   - *Ready for Novell Open Enterprise Server*
2. *Program powinien zapewniać ochronę przed wszystkimi rodzajami wirusów, trojanów, narzędzi hakerskich, oprogramowania typu spyware i adware, auto-dialerami i innymi potencjalnie niebezpiecznymi programami.*

Ochrona

1. *Program musi posiadać metody analizy heurystycznej.*
2. *Program musi umożliwiać skanowanie archiwów następujących formatów: ZIP, RAR, CAB i ARJ.*
3. *Program musi posiadać moduł ochrony w czasie rzeczywistym skanujący pliki oraz udostępniane i zamontowane zasoby Samba i NFS.*
4. *Integracja z systemem musi odbywać się poprzez moduł kernela lub moduł VFS serwera Samba.*
5. *Moduł skanowania na żądanie musi umożliwiać definiowanie zadań skanowania wybranych obszarów dysku.*
6. *Program musi mieć możliwość uruchomienia działania ochrony w czasie rzeczywistym zgodnie z terminarzem.*
7. *Program musi mieć możliwość wstrzymania działania ochrony w czasie rzeczywistym po określonym czasie od jej uruchomienia lub w określonych godzinach.*
8. *Program musi mieć możliwość dostosowania zakresu ochrony w czasie rzeczywistym, tak aby monitorowane były tylko wybrane foldery.*
9. *Program musi mieć możliwość konfiguracji ochrony czasie rzeczywistym tak, aby monitorowane były jedynie pliki o*

określonych rozszerzeniach.

10. *Program musi mieć możliwość zdefiniowania akcji jakie mają być wykonywane na obiektach zainfekowanych oraz podejrzanych.*
11. *Program musi mieć możliwość konfiguracji podejmowanych akcji w zależności od typu wykrytego zagrożenia.*
12. *Program musi posiadać funkcję wykluczania obiektów ze skanowania na podstawie ich nazwy.*
13. *Program musi posiadać funkcję wykluczania obiektów ze skanowania na podstawie nazwy zagrożenia jakie jest w nich wykrywane.*
14. *Program musi mieć możliwość wykluczenia ze skanowania obiektów większych niż zadany rozmiar.*
15. *W przypadku wykrycia wirusa monitor antywirusowy powinien automatycznie:*
    - *podejmować zalecane działanie czyli próbować leczyć, a jeżeli nie jest to możliwe to usuwać obiekt*
    - *rejestrować w pliku raportu informację o wykryciu wirusa*
    - *utworzyć kopie zapasową przed podjęciem próby leczenia lub usunięcia zainfekowanego pliku*
    - *poddać kwarantannie podejrzany obiekt*
16. *Program powinien mieć możliwość konfiguracji liczby aktywnych procesów skanujących.*
17. *Program powinien mieć możliwość eksportu i importu ustawień.*

Kopia zapasowa i kwarantanna

1. *Program musi posiadać moduł kwarantanny przechowujący zainfekowane obiekty.*
2. *System kwarantanny musi umożliwiać proste skanowanie, usuwanie i przywracanie do pierwotnej lokalizacji wybranych plików.*
3. *Program musi mieć możliwość zdefiniowania katalogu w którym przechowywane będą pliki poddane kwarantannie i ustawienia maksymalnego jej rozmiaru.*
4. *Program musi posiadać moduł kopii zapasowej przechowujący pliki przetwarzane przez program.*

Aktualizacja baz danych sygnatur zagrożeń

1. *Program powinien umożliwiać aktualizację baz zagrożeń z serwerów producenta, serwera administracyjnego lub wskazanego zasobu HTTP, FTP lub foldera.*
2. *Program powinien posiadać możliwość konfiguracji serwera proxy wykorzystywanego do pobierania uaktualnień.*
3. *Program musi umożliwiać uruchamianie zadania aktualizacji zgodnie z harmonogramem.*
4. *Program powinien posiadać możliwość eksportu baz zagrożeń z programu w celu aktualizacji programu na innym komputerze.*
5. *Program musi umożliwiać cofnięcie ostatniej aktualizacji baz zagrożeń.*

Raportowanie i powiadomienia

1. *Program musi posiadać możliwość zapisywania zdarzeń z działania programu w dzienniku zdarzeń.*
2. *Program musi posiadać możliwość zapisywania w dzienniku zdarzeń informacji o każdym przeskanowanym pliku.*
3. *Program musi umożliwiać generowanie raportów w formatach HTML, PDF i XLS.*
4. *Program powinien posiadać możliwość konfiguracji rotacji plików dziennika zdarzeń.*
5. *Program musi posiadać możliwość powiadamiania poprzez wysyłanie pułapek SNMP.*
6. *Program musi posiadać możliwość powiadamiania administratora na temat zaistniałych zdarzeń za pośrednictwem wiadomości mail lub pliku wykonywalnego.*
7. *Program powinien umożliwiać konfigurację tekstu dostarczanych powiadomień.*

Administracja

1. *Program powinien umożliwiać zarządzania z poziomu wiersza poleceń.*
2. *Program musi posiadać interfejs zarządzający w postaci strony WWW udostępnianej przy użyciu wbudowanego serwera.*

VI. Wymagania dla systemu scentralizowanego zarządzania

1. *System scentralizowanego zarządzania powinien obsługiwać następujące systemy operacyjne:*
    - *Microsoft Windows 10 Pro 32-bitowy / 64-bitowy*
    - *Microsoft Windows 8.1 Pro 32-bitowy / 64-bitowy*
    - *Microsoft Windows 8 Pro 32-bitowy / 64-bitowy*
    - *Microsoft Windows 7 Professional SP1 32-bitowy / 64-bitowy*
    - *Microsoft Windows 7 Professional 32-bitowy / 64-bitowy*
    - *Microsoft Windows Server 2008 Standard SP1 32-bitowy / 64-bitowy*
    - *Microsoft Windows Server 2008 Standard 32-bitowy / 64-bitowy*
    - *Microsoft Windows Server 2008 Enterprise 32-bitowy / 64-bitowy*
    - *Microsoft Windows Server 2008 R2 Enterprise 64-bitowy*
    - *Microsoft Windows Server 2008 R2 Enterprise SP1 64-bitowy*
    - *Microsoft Windows Server 2008 R2 Standard 64-bitowy*
    - *Microsoft Windows Server 2008 R2 Standard SP1 64-bitowy*

- *Microsoft Windows Server 2012 Standard 64-bitowy*

2. *System scentralizowanego zarządzania powinien przechowywać ustawienia w relacyjnej bazie danych:*
    - *Microsoft SQL Server 2005 Express Edition 32-bitowy*
    - *Microsoft SQL Server 2008 Express 32-bitowy*
    - *Microsoft SQL 2008 R2 Express 64-bitowy*
    - *Microsoft SQL 2012 Express 64-bitowy*
    - *Microsoft SQL 2014 Express 64-bitowy*
    - *Microsoft SQL Server 2005 (wszystkie edycje) 32-bitowy / 64-bitowy*
    - *Microsoft SQL Server 2008 (wszystkie edycje) 32-bitowy / 64-bitowy*
    - *Microsoft SQL Server 2008 R2 (wszystkie edycje) 64-bitowy*
    - *Microsoft SQL Server 2008 R2 Service Pack 2 (wszystkie edycje) 64-bitowy*
    - *Microsoft SQL Server 2012 (wszystkie edycje) 64-bitowy*
    - *Microsoft SQL Server 2014 (wszystkie edycje) 64-bitowy*
    - *Microsoft Azure SQL Database*
    - *MySQL 5.0.67, 5.0.77, 5.0.85, 5.0.87 (SP1), 5.0.91*
    - *MySQL Enterprise 5.0.60 (SP1), 5.0.70, 5.0.82 (SP1), 5.0.90*
3. *System zdalnego zarządzania powinien posiadać polskojęzyczny interfejs konsoli programu.*
4. *System zdalnego zarządzania powinien umożliwiać automatyczne umieszczenie komputerów w grupach administracyjnych odpowiadających strukturze sieci (grupy robocze sieci Microsoft Windows i/lub struktura Active Directory).*
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 jeden 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 umożliwia tworzenie hierarchicznej struktury serwerów administracyjnych jak również tworzenie wirtualnych serwerów administracyjnych.*
9. *System zdalnego zarządzania umożliwia zarządzanie stacjami roboczymi i serwerami plików Windows, nawet wtedy, gdy znajdują się one za zaporą NAT/Firewall.*
10. *Komunikacja pomiędzy serwerem zarządzającym a agentami sieciowymi na stacjach roboczych jest szyfrowana przy użyciu protokołu SSL.*
11. *Konsola administracyjna posiada możliwość zdalnego inicjowania skanowania antywirusowego na stacjach roboczych włączonych do sieci komputerowych w całej firmie.*
12. *Zarządzanie aplikacjami odbywa się przy użyciu profili aplikacji oraz zadań.*
13. *Konsola administracyjna ma możliwość informowania administratorów o wykryciu epidemii wirusa.*
14. *Serwer zarządzający ma 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 w sieciach korporacyjnych.*
16. *System centralnej dystrybucji i instalacji aktualizacji bibliotek sygnatur wirusów, który umożliwia automatyczne, niewidoczne dla użytkownika przesłanie i zainstalowanie nowej wersji biblioteki.*
17. *System centralnej dystrybucji i instalacji aktualizacji oprogramowania, który umożliwia automatyczne, niewidoczne dla użytkownika przesłanie i zainstalowanie nowego oprogramowania.*
18. *Po instalacji oprogramowania antywirusowego nie jest wymagane ponowne uruchomienie komputera do prawidłowego działania programu.*
19. *System centralnego zarządzania powinien zapewniać obsługę trybu dynamicznego dla Virtual Desktop Infrastructure (VDI).*
20. *System centralnego zbierania informacji i tworzenia sumarycznych raportów.*
21. *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).*
22. *System zdalnego zarządzania powinien umożliwiać podgląd w czasie rzeczywistym statystyk ochrony, stanu aktualizacji instalacji w sieci itp.*
23. *System zdalnego zarządzania powinien umożliwiać tworzenie kategorii aplikacji i warunków ich uruchomienia.*
24. *System zdalnego zarządzania powinien umożliwiać przeglądanie informacji o aplikacjach i plikach wykonywalnych znajdujących się na stacjach roboczych.*

25. *Program powinien mieć możliwość deinstalacji aplikacji niekompatybilnych jak również dowolnej aplikacji znajdującej się w rejestrze aplikacji użytkownika.*
26. *System zdalnego zarządzania powinien wyświetlać szczegółowe informacje na temat luk w oprogramowaniu wykrytych na zarządzanych komputerach oraz ich naprawę.*
27. *Program powinien dać możliwość kontrolowania na stacjach roboczych aktualizacji systemowych oraz ich instalację.*
28. *System zdalnego zarządzania powinien mieć możliwość zbierania informacji o sprzęcie zainstalowanym na komputerach klienckich.*
29. *System zdalnego zarządzania powinien umożliwiać przeglądanie informacji o obiektach poddanych kwarantannie oraz podejmowanie odpowiednich działań (np. przywracanie, skanowanie itp.).*
30. *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.*
31. *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.*
32. *System zdalnego zarządzania powinien umożliwiać automatyczne instalowanie licencji na stacjach roboczych.*
33. *System zdalnego zarządzania powinien umożliwiać automatyczne i regularne tworzenie kopii zapasowej serwera zarządzającego, która umożliwi przywrócenie w pełni działającego systemu zarządzania.*
34. *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.*
35. *System zdalnego zarządzania powinien umożliwiać wysłanie do stacji roboczych komunikatu o dowolnie zdefiniowanej treści.*
36. *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).*
37. *Program powinien umożliwiać ukrycie przed użytkownikiem interfejsu aplikacji, ikony w pasku systemowym, wpisów w Menu Start oraz na liście zainstalowanych programów.*
38. *Program powinien umożliwić administratorowi wyłączenie niektórych lub wszystkich powiadomień wyświetlanych na stacjach roboczych.*
39. *System zdalnego zarządzania powinien umożliwiać administrację poprzez przeglądarkę internetową.*
40. *System zdalnego zarządzania powinien dać możliwość wykorzystania bramy połączenia dla komputerów, które nie mają bezpośredniego połączenia z Serwerem administracyjnym.*
41. *System zdalnego zarządzania powinien mieć możliwość sprawdzenia aktualnych wersji oprogramowania antywirusowego.*
42. *System zdalnego zarządzania powinien umożliwiać przechwytywanie i instalację obrazów systemu operacyjnego.*
43. *Do przechwytywania obrazów systemów operacyjnych Windows system zdalnego zarządzania powinien wykorzystywać bezpłatne narzędzia producenta OS.*
44. *System zdalnego zarządzania powinien umożliwić zdefiniowanie własnej listy serwerów PXE oraz dodawanie lub importowanie adresów MAC komputerów docelowych.*
45. *System zdalnego zarządzania powinien umożliwić dodawanie własnych sterowników do obrazu preinstalacyjnego OS.*
46. *System zdalnego zarządzania powinien zawierać predefiniowaną listę aplikacji firm trzecich umożliwiającą automatyczne pobranie i utworzenie pakietu instalacyjnego.*
47. *System zdalnego zarządzania powinien zapewnić pobieranie i instalację poprawek lub uaktualnień aplikacji firm trzecich.*
48. *System zdalnego zarządzania powinien umożliwić wykorzystanie go jako serwer aktualizacji systemu Windows (WSUS).*
49. *System zdalnego zarządzania w trybie WSUS powinien umożliwiać konfigurację typu aktualizacji, wersji językowych oraz aplikacji i systemów, dla których będą pobierane poprawki.*
50. *System zdalnego zarządzania w trybie WSUS powinien umożliwiać zatwierdzanie lub odrzucanie wybranych poprawek.*
51. *System zdalnego zarządzania w trybie WSUS powinien umożliwiać instalację wszystkich, wybranych lub tylko zatwierdzonych poprawek.*
52. *System zdalnego zarządzania powinien umożliwić dodawanie i kontrolę licencji aplikacji firm trzecich. Kontrolowana powinna być zarówno ilość jak i okres ważności licencji.*

53. *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.*
54. *System zdalnego zarządzania powinien umożliwić wysyłanie powiadomień do wybranych użytkowników przy użyciu poczty elektronicznej lub wiadomości SMS.*
55. *System zdalnego zarządzania powinien umożliwić instalowanie certyfikatów na urządzeniach mobilnych wybranych użytkowników.*
56. *System zdalnego zarządzania powinien umożliwić instalowanie certyfikatów iOS MDM na urządzeniach mobilnych wybranych użytkowników.*
57. *System zdalnego zarządzania powinien tworzyć repozytorium sprzętu w tym min. komputerów i nośników wymiennych.*
58. *Administrator powinien mieć możliwość dopisywania informacji do sprzętu w repozytorium w tym min. numeru ewidencyjnego, numeru seryjnego, producenta, daty zakupu, aktualnego użytkownika.*
59. *Administrator powinien mieć możliwość zaznaczenia czy urządzenie jest lub nie jest aktualnie wykorzystywane.*
60. *Administrator powinien mieć możliwość oznaczania urządzeń jako firmowe.*
61. *System zdalnego zarządzania powinien umożliwić zarządzanie urządzeniami mobilnymi z wykorzystaniem serwerów Exchange ActiveSync i iOS MDM.*
62. *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.*
63. *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.*
64. *System zdalnego zarządzania powinien umożliwiać definiowanie reguł szyfrowania na stacjach roboczych (długość i złożoność hasła, blokada hasła, szyfrowanie dysków, plików, folderów, nośników wymiennych itd.).*
65. *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.*
66. *Dla zaszyfrowanych dysków system powinien umożliwiać odzyskiwanie haseł dostępu do dysków.*
67. *Dla nośników wymiennych system musi umożliwiać wymuszenie szyfrowania całego nośnika, wszystkich plików oraz tylko nowych plików.*
68. *Dla nośników wymiennych powinien być dostępny tryb przenośny umożliwiający odczyt zaszyfrowanych plików na dowolnym komputerze (również bez modułu szyfrującego).*
69. *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.*
70. *W całym okresie trwania subskrypcji użytkownik ma prawo do korzystania z bezpłatnej pomocy technicznej świadczonej za pośrednictwem telefonu i poczty elektronicznej.*
71. *W całym okresie trwania subskrypcji użytkownik ma możliwość pobierania i instalacji nowszych wersji oprogramowania i konsoli zarządzającej.*

VII. Wsparcie techniczne

pomoc techniczną - kontakt telefoniczny/poprzez e-mail w godzinach pracy oraz przez 24 h/7 z ograniczeniami; możliwy jest również bezpośredni kontakt ze specjalistą ds. pomocy techn.

- *szkolenie/ prezentacja on-line*
- *wdrożenie zdalne darmowe*

1. Wymagania dotyczące sposobu realizacji zamówienia:
   1) Wykonawca zobowiązuje się na czas trwania gwarancji do nieodpłatnego wparcia technicznego na zasadach określonych we wzorze umowy
   2) Wykonawca zapewni dostęp do pomocy technicznej, umożliwiającej zgłaszanie wad lub usterek za pomocą Internetu lub telefonicznie.