Załącznik nr 1 do SIWZ

WYKAZ ZAMAWIANEGO OPROGRAMOWANIA – ZESTAWIENIE CEN JEDNOSTKOWYCH

Lp.	Rodzaj artykułu	Nazwa oprogramowania proponowanego przez Wykonawcę	Ilość / jedn. m.	Cena jednostkowa netto	Wartość Netto	Stawka podatku VAT	Kwota podatku VAT	Wartość brutto
1	2	3	4	5	6	7	8	9
1	**Microsoft Windows Server 2016 Standard Core 2 licencje** - język Single Language - typ licencji Standard - licencja komercyjna		**40 szt**					
2	**Microsoft Windows Server Standard Core 2016 Sngl 16Licenses NoLevel CoreLic** - język Single Language - typ licencji Standard - licencja komercyjna		**1 szt**					
3	**Microsoft Windows Server 2016 Standard User CAL** - język Single Language - typ licencji Standard - licencja komercyjna		**140 szt**					
4	**Microsoft Exchange Server 2016 Standard** - język Single Language - typ licencji Standard - licencja komercyjna		**2 szt**					
5	**Microsoft Exchange Server 2016 Standard User CAL** - język Single Language - typ licencji Standard - licencja komercyjna		**140 szt**					
6	**Microsoft SQL Server Standard Edition 2017 Single Open No Level** - język Single Language - typ licencji Standard - licencja komercyjna		**1 szt**					
7	**Microsoft SQL 2017 Single OPEN 1 license No Level User CAL** - język Single Language - typ licencji Standard - licencja komercyjna		**20 szt**					
8	**VMware vCenter Server 6 Standard for vSphere 6 (Per Instance) wraz z rocznym wsparciem Basic Support/Subscription VMware vCenter Server 6 Standard for vSphere 6 (Per Instance) for 1 year** Licencja komercyjna		**1 szt**					
9	**VMware vSphere 6 Standard for 1 processor wraz z rocznym wsparciem Basic Support/Subscription VMware vSphere 6 Standard for 1 processor for 1 year** Licencja komercyjna		**4 szt**					
10	**Odnowienie wsparcia oraz licencji Cisco Iron Port na okres 36 miesięcy** Nr seryjne posiadanych urządzeń: 1. FCZ1849N00G 2. FCZ1849N00L Posiadana obecnie licencja to Inbound Essentials Bundle(AS+AV+OF) dla 200 użytkowników		**1 szt**					

11	**<u>Oprogramowanie antywirusowe takie jak ESET Endpoint Antivirus Suite lub równoważne o parametrach nie gorszych niż wyspecyfikowano</u>** 1. Pełne wsparcie dla systemu Windows XP SP3/Vista/Windows 7/Windows8/Windows 8.1/Windows 8.1 Update/10 2. Wsparcie dla 32- i 64-bitowej wersji systemu Windows. 3.Wersja programu dla stacji roboczych Windows dostępna zarówno w języku polskim jak i angielskim. 4. Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim. 5. Skuteczność programu potwierdzona nagrodami VB100 i AV-comparatives Ochrona antywirusowa i antyspyware 6. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 7. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. 8. Wbudowana technologia do ochrony przed rootkitami. 9. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 10. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 11. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 12. System ma oferować administratorowi możliwość definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym i jeśli tak – nie wykonywało danego zadania. 13. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania). 14. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 15. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu. 16. Możliwość skanowania dysków sieciowych i dysków przenośnych. 17. Skanowanie plików spakowanych i skompresowanych. 18. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. 19. Wykluczenie ze skanowania musi odbywać się nie tylko po nazwie pliku ale również ma być możliwe użycie symbolu wieloznacznego „*” zastępującego dowolne znaki w ścieżce. 20. Administrator ma możliwość dodania wykluczenia po tzw. HASH’u zagrożenia, wskazującego bezpośrednio na określoną infekcję a nie konkretny plik. 21. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu. 22. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu. 23.Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera. 24. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji. 25. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera. 26. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej. 27. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego).		**160 szt**					

	28. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail. 29. Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 30. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. 31. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail. 32. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie. 33. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Program musi umożliwić blokowanie danej strony internetowej po podaniu na liście całej nazwy strony lub tylko wybranego słowa występującego w nazwie strony. 34. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora. 35. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. 36. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 37. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe. 38. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta. 39. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego. 40. Program musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. 41. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym. 42. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego. 43. W przypadku gdy stacja robocza nie będzie posiadała dostępu do sieci Internet ma odbywać się skanowanie wszystkich procesów również tych, które wcześniej zostały uznane za bezpieczne. 44. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie. 45. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń mają być wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika. 46. Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika. 47. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia. 48. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe. 49. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium							

	producenta. 50. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła. 51. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło. 52. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo. 53. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i administratora wraz z listą niezainstalowanych aktualizacji. 54. Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu. 55. Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów. 56. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku. 57. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym. 58. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM , urządzeń przenośnych oraz urządzeń dowolnego typu. 59. Funkcja blokowania nośników wymiennych bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model. 60. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia, dana funkcjonalność musi pozwalać na automatyczne wypełnienie właściwości urządzenia dla tworzonej reguły. 61. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie brak dostępu do podłączanego urządzenia. 62. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. 63. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika. 64. Użytkownik ma posiadać możliwość takiej konfiguracji programu aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika 65. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS). 66. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: • tryb automatyczny z regułami gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, • tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, • tryb oparty na regułach gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, • tryb uczenia się, w którym program uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi							

	samoczynnie przełączyć się w tryb pracy oparty na regułach. • Tryb inteligentny – w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach. 67. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego. 68. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól. 69. Oprogramowanie musi posiadać zaawansowany skaner pamięci. 70. Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp. 71. Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach. 72. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa. 73. Program ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie. 74. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu. 75. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami. 76. Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji program zgłosi posiadanie nieaktualnej bazy sygnatur. 77. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji. 78. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http 79. Program musi być wyposażona w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback). 80. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 81. Program ma być w pełni zgodny z technologią CISCO Network Access Control. 82. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełno ekranowym. 83. W momencie wykrycia trybu pełno ekranowego aplikacja ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań aplikacji. 84. Użytkownik ma mieć możliwość skonfigurowania programu tak aby automatycznie program włączał powiadomienia oraz zadania pomimo pracy w trybie pełnoekranowym po określonym przez użytkownika czasie. 85. Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, kontroli stron Internetowych i kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania. 86. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. 87. Program musi posiadać możliwość utworzenia z poziomu interfejsu aplikacji dziennika diagnostycznego na potrzeby pomocy technicznej. 88. Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline. 89. Możliwość podejrzenia licencji za pomocą, której program został aktywowany.							

	90. W programie musi istnieć możliwość tymczasowego wstrzymania polityk wysłanych z poziomu serwera zdalnej administracji. 91. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej. 92. Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas po którym automatycznie zostają przywrócone dotychczasowe ustawienia. 93. Administrator ma możliwość wstrzymania polityk na 10 min, 30 min, 1 godzinę i 4 godziny 94. Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika. 95. Program musi posiadać opcję automatycznego skanowania komputera po dokonaniu zmian z użyciem opcji wstrzymania polityki. 96. Aplikacja musi posiadać funkcję ręcznej aktualizacji komponentów programu. 97. Możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych. 98. Program musi posiadać możliwość definiowana stanów aplikacji, jakie będą wyświetlane użytkownikowi np. powiadomień o wyłączonych mechanizmach ochrony czy stanie licencji. 99. Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie. Ochrona serwera plików Windows 1. Wsparcie dla systemów: Microsoft Windows Server 2003, 2008, 2008 R2, 2012, 2012 R2, 2016 SBS 2003, SBS 2003 R2, SBS 2008, SBS 2011, Microsoft MultiPoint Server 2010, Microsoft MultiPoint Server 2011, Windows MultiPoint Server 2012. 2. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 3. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. 4. Wbudowana technologia do ochrony przed rootkitami i exploitami. 5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 6. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 7. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu. Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania). 8. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 9. System antywirusowy ma mieć możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu. 10. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych. 11. Użytkownik ma mieć możliwość zmiany ilości wątków skanowania w ustawieniach systemu antywirusowego. 12. Możliwość skanowania dysków sieciowych i dysków przenośnych. 13. Skanowanie plików spakowanych i skompresowanych. 14. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. 15. Program musi posiadać funkcjonalność pozwalającą na ograniczenie wielokrotnego skanowania plików w środowisku wirtualnym za pomocą mechanizmu przechowującego informacje o przeskanowanym już obiekcie i współdzieleniu tych informacji z innymi maszynami wirtualnymi. 16. Aplikacja powinna wspierać mechanizm klastrowania. 17.Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).							

	18. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS. 19. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. 20. Program ma umożliwiać użytkownikowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: pamięci masowych, płyt CD/DVD i pamięci masowych FireWire. 21. Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model. 22. Aplikacja musi posiadać funkcjonalność, która automatycznie uzupełni elementy wymagane dla tworzenia reguł w oparciu o informacje dostępne z aktualnie podłączonego nośnika. 23. Aplikacja ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, brak dostępu do podłączanego urządzenia. 24. Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. 25. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika. 26. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 27. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony. 28. Dodanie automatycznych wyłączeń nie wymaga restartu serwera. 29. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych. 30. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji. 31. W przypadku restartu serwera – usunięte z listy wyłączeń elementy mają być automatycznie uzupełnione. 32. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego. 33. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line). 34. Możliwość przeniesienia zainfekowanych plików w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej. 35. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie. 36. Możliwość skanowania wyłącznie z zastosowaniem algorytmów heurystycznych tj. wyłączenie skanowania przy pomocy sygnatur baz wirusów. 37. Aktualizacje modułów analizy heurystycznej. 38. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika. 39. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia. 40. Wysyłanie zagrożeń do laboratorium ma być możliwe z serwera zdalnego zarządzania i lokalnie z każdej stacji roboczej w przypadku komputerów mobilnych.							

	41. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe. 42. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. 43. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e mail. 44. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy serwerze przy próbie dostępu do konfiguracji systemu antywirusowego był proszony o podanie hasła. 45. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program ma pytać o hasło. 46. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji ma być takie samo. 47. System antywirusowy ma być w pełni zgodny z technologią CISCO NAC. 48. System antywirusowy ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji. 49. System antywirusowy ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie. Program ma także posiadać opcję dezaktywacji tego mechanizmu. 50. Po instalacji systemu antywirusowego, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów. 51. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku. 52. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym. 53. Program powinien umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: nośników CD/DVD oraz urządzeń USB. 54. System antywirusowy ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach. 55. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa. 56. System antywirusowy ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie. 57. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń. 58. Aktualizacja dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP). 59. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy. 60. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja). 61. Do każdego zadania aktualizacji można przypisać dwa różne profile z innym ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja). Przykładowo, domyślny profil aktualizuje z sieci lokalnej a							

	w przypadku jego niedostępności wybierany jest profil rezerwowy pobierający aktualizację z Internetu. 62. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 63. Aplikacja musi wspierać skanowanie magazynu Hyper-V 64. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów 65. Wykluczenie ze skanowania musi odbywać się nie tylko po nazwie procesu ale również ma być możliwe użycie symbolu wieloznacznego „*” zastępującego dowolne znaki. 66. Administrator ma możliwość dodania wykluczenia po tzw. HASH'u zagrożenia, wskazującego bezpośrednio na określoną infekcję a nie konkretny plik. 67. Praca programu musi być niezauważalna dla użytkownika. 68.Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania. 69. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. Administracja zdalna 1. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2003, 2008, 2012 oraz systemach Linux. 2. Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance). 3. Serwer administracyjny musi wspierać instalację w oparciu o co najmniej bazy danych MS SQL i MySQL. 4. Serwer administracyjny musi oferować możliwość wykorzystania już istniejącej bazy danych MS SQL lub MySQL użytkownika. 5. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji i konsoli w postaci jednego pakietu instalacyjnego lub każdego z modułów oddzielnie bezpośrednio ze strony producenta. 6. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej. 7. Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy występujące w sieci. 8. Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6. 9. Podczas logowania administrator musi mieć możliwość wyboru języka w jakim zostanie wyświetlony panel zarządzający. 10. Zmiana języka panelu administracyjnego nie może wymagać zatrzymania lub reinstalacji oprogramowania zarządzającego. 11. Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL. 12. Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci. 13. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych. 14. Jeden centralny serwer centralnego zarządzania bez względu na wielkość sieci. 15. Instalacja serwera administracyjnego powinna oferować wybór trybu pracy serwera w sieci w przypadku rozproszonych sieci –serwer pośredniczący (proxy) lub serwer centralny. 16. Serwer proxy musi pełnić funkcję pośrednika pomiędzy lokalizacjami zdalnymi a serwerem centralnym. 17. Serwer proxy musi być wyposażony we własną bazę danych, w której będą przechowywane dane z agentów na wypadek braku połączenia z serwerem centralnym. 18. Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM. 19. Serwer administracyjny musi oferować możliwość instalacji serwera http proxy pozwalającego na pobieranie aktualizacji baz sygnatur oraz pakietów instalacyjnych na stacjach roboczych bez dostępu do							

	Internetu. 20. Serwer http proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) najczęściej pobieranych elementów. 21. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów. 22. Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy. 23. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na stacjach roboczych z systemami Windows, Mac OS X oraz Linux oraz serwerach Windows. 24. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na urządzeniach mobilnych z systemem Android. 25. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci. 26. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta. 27. Administrator musi posiadać możliwość zarządzania za pomocą dedykowanego agenta stacjami nie posiadającymi zainstalowanego programu zabezpieczającego. 28. Agent musi przekazywać informacje na temat stanu systemu operacyjnego do serwera administracji zdalnej 29. Agent musi posiadać możliwość pobrania listy zainstalowanego oprogramowania firm trzecich na stacji roboczej z możliwością jego odinstalowania. 30. Serwer administracyjny musi oferować możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie. 31. Instalacja agenta musi odbywać się przy wykorzystaniu repozytorium producenta. Repozytorium powinno zawierać aktualne wersje agentów bez względu na rodzaj systemu operacyjnego. 32. Instalacja agenta nie może wymagać określenia typu systemu (32 lub 64 – bitowy) oraz jego rodzaju (Windows, Mac, itp) a dobór odpowiedniego pakietu musi być w pełni automatyczny. 33. Instalacja klienta na urządzeniach mobilnych musi być dostępna za pośrednictwem portalu WWW udostępnionego przez moduł MDM z poziomu urządzenia użytkownika. 34. W przypadku braku zainstalowanego klienta na urządzeniu mobilnym musi istnieć możliwość jego pobrania ze sklepu Google Play. 35. Administrator musi posiadać możliwość utworzenia listy zautoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji. 36. Serwer administracyjny musi oferować możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, nie komunikację za pośrednictwem wiadomości SMS. 37. Serwer administracyjny musi oferować możliwość utworzenia polityk konfiguracji dla aplikacji zabezpieczającej na urządzeniu mobilnym. 38. Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi. 39. Administrator musi posiadać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli zarządzającej 40. Dwu fazowa autoryzacja musi się odbywać za pomocą wiadomości SMS lub haseł jednorazowych generowanych na urządzeniu mobilnym za pomocą dedykowanej aplikacji. 41. Administrator musi posiadać możliwość utworzenia użytkownika wbudowanego lub zintegrowanego z grupą z usługi Active Directory. 42. Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących							

	zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp. 43. Administrator musi posiadać możliwość nadania dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko do odczytu, odczyt/zapis. 44. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika. 45. Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta bez konieczności logowania się do panelu administracyjnego. 46. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności po jakim użytkownik zostanie automatycznie wylogowany. 47. Dostępne zadania muszą być podzielone na dwie grupy: zadania klienta oraz zadania serwera. 48. Zadania serwera obejmujące zadanie instalacji agenta, generowania raportów oraz synchronizacji grup. 49. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej. 50. Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji. 51. Serwer administracyjny musi w przejrzysty sposób informować administratora o elementach zadań jakie są wymagane do jego uruchomienia a w przypadku jego braku wskazywać brakujące elementy konfiguracji. 52. Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym. 53. Serwer administracyjny musi oferować możliwość wyboru parametrów pakietu instalacyjnego zależnych od systemu operacyjnego oraz licencji na program zabezpieczający. 54. Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu. 55. Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką. 56. Serwer administracyjny musi oferować możliwość utworzenia jednego zadania dla kilku klientów lub grupy. 57. Serwer administracyjny musi oferować możliwość uruchomienia zadania automatycznie zgodnie z harmonogramem, po wystąpieniu nowego dziennika zdarzeń lub umieszczeniu nowego klienta w grupie dynamicznej. 58. Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów. 59. Grupy dynamiczne tworzone na podstawie szablonu określającego warunki jakie musi spełnić klient aby zostać umieszczony w danej grupie. Przykładowe warunki: Adresy sieciowe IP, Aktywne zagrożenia, Stan funkcjonowania/ochrony, Wersja systemu operacyjnego, itp. 60. Serwer administracyjny musi oferować możliwość utworzenia polityk dla programów zabezpieczających i modułów serwera centralnego zarządzania. 61. Serwer administracyjny musi oferować możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów. Serwer administracyjny musi oferować możliwość przypisania kilku polityk z innymi priorytetami dla jednego klienta. 62. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej. 63. Serwer administracyjny musi oferować możliwość nadania priorytetu „Wymuś” dla konkretnej opcji w konfiguracji klienta. Opcja ta nie będzie mogła być zmieniona na stacji klienckiej bez względu na zabezpieczenie całej konfiguracji hasłem lub w przypadku jego braku. 64. Serwer administracyjny musi oferować możliwość ukrycia graficznego interfejsu użytkownika na stacji klienckiej i jego uruchomienia tylko przez administratora.							

	65. Serwer administracyjny musi umożliwiać wyświetlenie polityk do których przynależy dana stacja robocza oraz ich edycję z poziomu właściwości samego klienta 66. Serwer administracyjny musi oferować możliwość utworzenia własnych raportów lub skorzystanie z predefiniowanych wzorów. 67. Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania. 68. Serwer administracyjny musi oferować możliwość wyboru formy przedstawienia danych w raporcie w postaci tabeli, wykresu lub obu elementów jednocześnie. 69. Serwer administracyjny musi oferować możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy, itp. 70. Serwer administracyjny musi oferować możliwość określenia danych jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na elementach wykresu oraz ich odfiltrowania i posortowania. 71. Serwer administracyjny musi być wyposażona w mechanizm importu oraz eksportu szablonów raportów. 72. Serwer administracyjny powinien posiadać Panel kontrolny z raportami administratora, pozwalający na szybki dostępu do najbardziej interesujących go danych. Panel ten musi oferować możliwość modyfikacji jego elementów. 73. Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym dostępnym z poziomu interfejsu konsoli WWW. 74. Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub PS. 75. Serwer administracyjny musi oferować możliwość skonfigurowania czasu automatycznego odświeżania raportu na panelu kontrolnym oraz umożliwiać jego odświeżenie na żądanie. 76. Serwer administracyjny musi oferować możliwość tworzenia wielu zakładek panelu, w których będą widoczne wybrane przez administratora elementy monitorujące. 77. Serwer administracyjny musi oferować możliwość maksymalizacji wybranego elementu monitorującego. 78. Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy. 79. Serwer administracyjny musi oferować możliwość utworzenia własnych powiadomień lub skorzystanie z predefiniowanych wzorów. 80. Powiadomienia muszą dotyczyć zmiany ilości klientów danej grupy dynamicznej, wzrostu liczby grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń lub skanowania lub stanu obiektu serwer centralnego zarządzania. 81. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP. 82. Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu. 83. Serwer administracyjny musi oferować możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu. 84. Serwer administracyjny musi oferować możliwość podłączenia serwera administracji zdalnej do portalu zarządzania licencjami dostępnego na serwerze producenta. 85. Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji. 86. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty. 87. Serwer administracyjny musi oferować możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej							

	właściciela. 88. Narzędzie administracyjne musi być wyposażone w mechanizm wyszukiwania zarządzanych komputerów na podstawie co najmniej nazwy komputera, adresu IPv4 i IPv6 lub wyszukania konkretnej nazwy zagrożenia. 89. Serwer administracyjny musi być wyposażona w machizm autodopasowania kolumn w zależności od rozdzielczości urządzenia na jakim jest wyświetlana. 90. Serwer administracji musi umożliwić granulację uprawnień dla Administratorów w taki sposób, aby każdemu z nich możliwe było przyznanie oddzielnych uprawnień do poszczególnych grup komputerów, polityk lub zadań. 91. Konfiguracja zestawów uprawnień musi umożliwiać przypisanie praw tylko do odczytu, odczytu i użycia, oraz prawo do zapisania zmian w ramach danego zadania lub polityki w konsoli ERA. 92. Konsola webowa musi umożliwiać stronicowanie w widoku komputerów w celu ograniczenia liczby wyświetlanych maszyn na jednej stronie. 93. Administrator musi mieć możliwość podłączenia do stacji roboczej z użyciem protokołu RDP bezpośrednio z poziomu konsoli ERA. 94. Serwer musi wspierać wysyłanie logów do systemu SIEM IBM qRadar 95. Musi istnieć mechanizm, umożliwiający dodawanie reguł do istniejących już w module firewalla lub harmonogramie. Takie reguły można umieścić na początku lub końcu istniejącej listy. 96. Konsola administracyjna musi umożliwiać dodanie własnego logotypu do interfejsu webowego. **Licencja na 24 miesiące**							
12	**Oprogramowanie do szyfrowania danych takie jak Deslock Pro lub równoważne o parametrach nie gorszych niż wyspecyfikowano** 1.Konsola centralnego zarządzania musi wspierać systemy operacyjne Microsoft Windows Server 2003 32-bit i 64-bit, 2008 32-bit i 64-bit, 2012 64-bit oraz Microsoft Windows XP SP3/Vista/7/8/10 32-bit i 64-bit 2. Konsola centralnego zarządzania musi umożliwiać centralne administrowanie klientami systemu szyfrowania danych dla systemów Microsoft Windows. 3. Konsola centralnego zarządzania dzięki wykorzystaniu bazy danych SQL ma stanowić centralną bazę informacji o klientach systemu szyfrowania danych, kluczach szyfrujących oraz użytkownikach. 4. Konsola centralnego zarządzania musi współpracować z bazą danych Microsoft SQL Server 2005, Microsoft SQL Server 2008, Microsoft SQL Server 2008 R2, Microsoft SQL Server 2012 zarówno w wersji 32-bit i 64-bit oraz z Microsoft SQL Server 2005 Express Edition, Microsoft SQL 2008 Express Edition, Microsoft SQL Server 2012 Express Edition zarówno w wersji 32-bit i 64-bit. 5. Środowisko wymaga instalacji następujących składników: a) MS SQL w wersjach pełnych i Express b) Apache od wersji 2 lub IIS od wersji 6 c) PHP od wersji 5.3 6. Pakiet instalacyjny konsoli administracyjnej musi być wyposażony we wbudowane instalatory składników SQL Express, Apache oraz PHP 7. Konsola centralnego zarządzania musi pozwalać na generowanie paczek instalacyjnych dla stacji końcowych na dwa różne sposoby: a) Instalacja ręczna na kliencie b) Instalacja wypychana 8. Komunikacja pomiędzy konsolą centralną zarządzania, a serwerem proxy musi być na bezpiecznym porcie 443 9. Administrator może w konsoli do zarządzania tworzyć wiele kluczy szyfrujących opartych o kilka algorytmów szyfrujących, co najmniej AES, DES, Blowfish. 10. Administrator powinien mieć możliwość tworzenia różnych użytkowników mających dostęp do konsoli centralnego zarządzania wraz z możliwością przypisywania im różnych ról.		**10 szt**					

	11. Administrator powinien mieć możliwość tworzenia dodatkowych ról na podstawie opcji dostępnych w konsoli centralnego zarządzania. 12. Logowanie do konsoli centralnego zarządzania powinno być objęte warunkami złożoności hasła. 13. Powinna istnieć możliwość konfiguracji złożoności hasła do konsoli centralnego zarządzania, w tym a) ilości znaków b) czy hasło ma zawierać wielkie litery c) czy hasło ma zawierać małe litery d) czy hasło ma zawierać cyfry e) czy hasło ma zawierać znaki specjalne f) okres ważności g) ilość nieudanych logowań 14. Administrator powinien mieć możliwość konfiguracji złożoności haseł dla użytkowników na stacjach roboczych. 15. Powinna istnieć możliwość konfiguracji złożoności hasła dla użytkowników na stacjach roboczych, w tym: a) ilości znaków b) czy hasło ma zawierać wielkie litery c) czy hasło ma zawierać małe litery d) czy hasło ma zawierać cyfry e) czy hasło ma zawierać znaki specjalne f) okres ważności g) ilość nieudanych logowań h) możliwość zmiany hasła 16. Konsola centralnego zarządzania powinna gromadzić informacje o: a) nazwach stacji roboczych, na których jest zainstalowany klient systemu szyfrowania danych b) dacie ostatniej modyfikacji ustawień klienta systemu szyfrowania danych c) dacie instalacji klienta systemu szyfrowania danych d) statusu szyfrowania zastosowanego na stacji roboczej e) typie urządzenia na którym jest zainstalowany klient systemu szyfrowania danych f) informacjach czy profil ustawień został zaktualizowany na stacjach roboczych g) wersji klienta systemu szyfrowania danych h) wersji systemu operacyjnego stacji roboczej i) liczby użytkowników uprawnionych do logowania do klienta systemu szyfrowania danych na stacji roboczej 17. Konsola centralnego zarządzania powinna pozwalać na generowanie dla każdej ze stacji płyty ratunkowej. 18. Konsola musi być dostępna z poziomu przeglądarki internetowej. 19. Administrator powinien mieć możliwość zarządzania stacjami klienckimi, które mają dostep do sieci Internet, niezależnie od tego, gdzie komputery w danym momencie się znajdują. 20. Administrator musi mieć możliwość wykonania poniższych czynności w sposób zdalny: a) instalacji klienta na stacji b) zaszyfrowania/odszyfrowania stacji c) wygenerowania klucza aktywacyjnego dla użytkownika d) zablokowania stacji, e) zablokowania użytkownika, f) administrowania kluczami szyfrującymi, g) administrowania użytkownikami, którzy mają dostęp do stacji, h) administrowania profilem ustawień dla użytkowników, i) administrowania profilem ustawień dla stacji roboczych							

	j) wymuszenia zmiany hasła k) zarządzania wieloma organizacjami z poziomu jednej konsoli 21. System szyfrowania danych powinien dawać możliwość szyfrowania powierzchni dysku sektor po sektorze. 22. System szyfrowania danych powinien umożliwiać wstrzymanie procesu szyfrowania powierzchni dysku i jego wznowienie. Proces szyfrowania danych powinien rozpocząć się od momentu w którym został przerwany. 23. System szyfrowania danych powinien umożliwiać wstrzymanie procesu szyfrowania w sytuacji gdy laptop nie jest podłączony do zasilania. Proces szyfrowania powinien zostać wznowiony automatycznie po podłączeniu zasilacza. 24. System szyfrowania danych, oprócz szyfrowania całej powierzchni dysku, powinien posiadać możliwość szyfrowania pojedynczych plików, zawartości katalogów, pamięci przenośnych, wiadomości e-mail wraz z załącznikami, tekstu oraz schowka systemowego. 25. Wymagane jest wykorzystanie do szyfrowania poniższych algorytmów szyfrowania: a. AES (Rijndael) b. Blowfish c. Triple DES (3DES) 26. System szyfrowania danych powinien umożliwiać współpracę z dyskami SSD. 27. System szyfrowania danych powinien umożliwiać szyfrowanie danych na komputerach z UEFI 28. Administrator ma mieć możliwość sprawdzenia przed zaszyfrowaniem całej powierzchni dysku, czy nie pojawią się problemy po ponownym uruchomieniu komputera. 29. Administrator ma mieć możliwość wybrania szyfrowania dodatkowych partycji dysku (niesystemowych). 30. W przypadku utraty hasła, system szyfrowania danych powinien umożliwiać Administratorowi odzyskanie dostępu do zaszyfrowanego dysku poprzez użycie zdefiniowanego wcześniej hasła administratora. 31. System szyfrowania danych powinien umożliwiać wygenerowanie płyty ratunkowej (dostępnej na nośniku wymiennym USB lub CD/DVD) z poziomu konsoli centralnego zarządzania. 32. W przypadku utraty hasła, system szyfrowania danych powinien umożliwiać użytkownikowi odzyskanie dostępu do zaszyfrowanego dysku poprzez użycie otrzymanego od administratora unikalnego hasła, wygenerowanego z poziomu konsoli centralnego zarządzania. 33. System szyfrowania danych powinien być dostępny przynajmniej w języku polskim i angielskim. 34. System szyfrowania danych powinien umożliwiać zarządzanie z poziomu konsoli centralnego zarządzania (zależnie od rodzaju licencji). 35. Hasło dla użytkowników na stacjach roboczych powinno zawierać co najmniej poniższe założenia (w przypadku wersji centralnie zarządzanej): a) ilości znaków b) czy hasło ma zawierać wielkie litery c) czy hasło ma zawierać małe litery d) czy hasło ma zawierać cyfry e) czy hasło ma zawierać znaki specjalne f) okres ważności g) ilość nieudanych logowań h) możliwość zmiany hasła 36. Defragmentacja dysku nie może mieć negatywnego wpływu na system szyfrowania. 37. System szyfrowania danych musi umożliwiać szyfrowanie nośników wymiennych w następujący sposób: a. Sektor po sektorze, b.Kontener.							

	38. Zaszyfrowany nośnik wymienny oraz nośnik CD/DVD może być odczytany także na dowolnej stacji na której nie ma zainstalowanego klienta systemu szyfrowania. Dostęp do takiego nośnika musi być udzielony po podaniu hasła. 39. Dostęp do zaszyfrowanych nośników wymiennych lub zaszyfrowanych nośników CD/DVD może być zabezpieczony hasłem. 40. System szyfrowania danych musi pozwalać na szyfrowanie wiadomości e-mail wraz z załącznikami. 41. System szyfrowania danych musi umożliwiać automatyczną deszyfrację otrzymywanych wiadomości e-mail. 42. System szyfrowania danych musi pozwalać na szyfrowanie całego tekstu aktywnego dokumentu, jego części a także zawartości schowka systemowego. 43. Zaszyfrowany tekst oraz zawartość schowka systemowego może być odczytana w wbudowanej przeglądarce. 44. Zaszyfrowany tekst może być odczytany za pomocą darmowego narzędzia dostarczanego przez producenta na stacji bez zainstalowanego klienta systemu szyfrowania. 45. System szyfrowania danych powinien umożliwiać wybór klucza szyfrującego (w przypadku posiadania wielu kluczy w pęku), który ma być używany w procesie szyfrowania. 46. System szyfrowania danych powinien umożliwiać wybór domyślnego klucza szyfrowania. 47. System szyfrowania danych powinien umożliwiać zaszyfrowanie obiektu z poziomu menu kontekstowego. 48. System szyfrowania danych powinien umożliwiać zaszyfrowanie obiektu z poziomu menu kontekstowego a następnie wysłanie go przy pomocy dedykowanego klienta pocztowego jako załącznik. 49. Możliwe jest utworzenie skrótów klawiszowych umożliwiających zaszyfrowanie/odszyfrowanie całego tekstu aktywnego dokumentu, jego części a także zawartości schowka systemowego. 50. System szyfrowania danych powinien umożliwiać tworzenie wirtualnych partycji. Dostęp do takich partycji ma być możliwy przy użyciu klucza szyfrującego lub hasła. 51. System szyfrowania danych powinien umożliwiać zdefiniowanie wielkości wirtualnej partycji, z dokładnością do 1MB. 52.System szyfrowania danych musi umożliwiać tworzenie zaszyfrowanego archiwum. Dostęp do takiego archiwum ma być możliwy przy użyciu klucza szyfrującego lub hasła. 53. System szyfrowania danych powinien umożliwiać trwałe usuwanie danych za pomocą poniższych algorytmów: a. Guttman b. US Department of Defence 5220.22-M (8-306. /E) c. US Department of Defence 5220.22-M (8-306. /E, CiE) d. Cryptographic Random Number Data 54. Dedykowana wtyczka powinna wspierać co najmniej klientów pocztowych MS Outlook 2003 lub nowszych, również dostępnych z poziomu Office 365. 55. System szyfrowania danych powinien umożliwiać automatyczne zalogowanie użytkownika do konsoli klienta systemu szyfrowania danych po uruchomieniu systemu operacyjnego. 56. System szyfrowania danych powinien umożliwiać automatyczne wylogowanie z aplikacji w przypadku bezczynności użytkownika w systemie. 57. System szyfrowania danych powinien posiadać opcję automatycznego odpytywania serwerów producenta o dostępność nowszych wersji. 58. Użytkownik powinien posiadać możliwość ręcznego sprawdzania czy dostępna jest nowsza wersja programu, z poziomu GUI. 59. Konieczna jest autentykacja typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. 60. System powinien umożliwiać określenie co najmniej 127 unikalnych użytkowników, którzy będą mieć dostęp do chronionej stacji roboczej na poziomie Pre-Boot.							

	61. System powinien umożliwiać przetrzymywanie co najmniej 64 kluczy szyfrujących w jednym pęku kluczy (key file) 62. Dostęp do klucza powinien być chroniony przy pomocy hasła. 63. System szyfrowania danych musi wspierać instalacje aplikacji klienckiej w środowisku Microsoft Windows XP SP3/Vista/7/8/10 32-bit i 64-bit oraz w środowiskach Microsoft Windows Server 2003 32-bit i 64-bit, 2008 32-bit i 64-bit, 2012 64-bit. 64. Administrator ma możliwość zainstalowania systemu szyfrowania danych w środowisku wirtualnym (VMWARE). 65. System musi posiadać certyfikat FIPS 140-2 Level 1 **Licencja na 12 miesięcy**							
13	**Oprogramowanie do szyfrowania danych takie jak Deslock Standard lub równoważne o parametrach nie gorszych niż wyspecyfikowano** 1. Konsola centralnego zarządzania musi wspierać systemy operacyjne Microsoft Windows Server 2003 32-bit i 64-bit, 2008 32-bit i 64-bit, 2012 64-bit oraz Microsoft Windows XP SP3/Vista/7/8/10 32-bit i 64-bit 2. Konsola centralnego zarządzania musi umożliwiać centralne administrowanie klientami systemu szyfrowania danych dla systemów Microsoft Windows. 3. Konsola centralnego zarządzania dzięki wykorzystaniu bazy danych SQL ma stanowić centralną bazę informacji o klientach systemu szyfrowania danych, kluczach szyfrujących oraz użytkownikach. 4. Konsola centralnego zarządzania musi współpracować z bazą danych Microsoft SQL Server 2005, Microsoft SQL Server 2008, Microsoft SQL Server 2008 R2, Microsoft SQL Server 2012 zarówno w wersji 32-bit i 64-bit oraz z Microsoft SQL Server 2005 Express Edition, Microsoft SQL 2008 Express Edition, Microsoft SQL Server 2012 Express Edition zarówno w wersji 32-bit i 64-bit. 5. Środowisko wymaga instalacji następujących składników: a) MS SQL w wersjach pełnych i Express b) Apache od wersji 2 lub IIS od wersji 6 c) PHP od wersji 5.3 6. Pakiet instalacyjny konsoli administracyjnej musi być wyposażony we wbudowane instalatory składników SQL Express, Apache oraz PHP 7. Konsola centralnego zarządzania musi pozwalać na generowanie paczek instalacyjnych dla stacji końcowych na dwa różne sposoby: a) Instalacja ręczna na kliencie b) Instalacja wypychana 8. Komunikacja pomiędzy konsolą centralną zarządzania, a serwerem proxy musi być na bezpiecznym porcie 443 9. Administrator może w konsoli do zarządzania tworzyć wiele kluczy szyfrujących opartych o kilka algorytmów szyfrujących, co najmniej AES, DES, Blowfish. 10. Administrator powinien mieć możliwość tworzenia różnych użytkowników mających dostęp do konsoli centralnego zarządzania wraz z możliwością przypisywania im różnych ról. 11. Administrator powinien mieć możliwość tworzenia dodatkowych ról na podstawie opcji dostępnych w konsoli centralnego zarządzania. 12. Logowanie do konsoli centralnego zarządzania powinno być objęte warunkami złożoności hasła. 13. Powinna istnieć możliwość konfiguracji złożoności hasła do konsoli centralnego zarządzania, w tym a) ilości znaków b) czy hasło ma zawierać wielkie litery c) czy hasło ma zawierać małe litery d) czy hasło ma zawierać cyfry e) czy hasło ma zawierać znaki specjalne f) okres ważności		**70 szt**					

	g) ilość nieudanych logowań 14. Administrator powinien mieć możliwość konfiguracji złożoności haseł dla użytkowników na stacjach roboczych. 15. Hasło dla użytkowników na stacjach roboczych powinno zawierać co najmniej poniższe założenia: a) ilości znaków b) czy hasło ma zawierać wielkie litery c) czy hasło ma zawierać małe litery d) czy hasło ma zawierać cyfry e) czy hasło ma zawierać znaki specjalne f) okres ważności g) ilość nieudanych logowań h) możliwość zmiany hasła 16. Konsola centralnego zarządzania powinna gromadzić informacje o: a) nazwach stacji roboczych, na których jest zainstalowany klient systemu szyfrowania danych b) dacie ostatniej modyfikacji ustawień klienta systemu szyfrowania danych c) dacie instalacji klienta systemu szyfrowania danych d) statusu szyfrowania zastosowanego na stacji roboczej e) typie urządzenia na którym jest zainstalowany klient systemu szyfrowania danych f) informacjach czy profil ustawień został zaktualizowany na stacjach roboczych g) wersji klienta systemu szyfrowania danych h) wersji systemu operacyjnego stacji roboczej i) liczby użytkowników uprawnionych do logowania do klienta systemu szyfrowania danych na stacji roboczej 17. Konsola centralnego zarządzania powinna pozwalać na generowanie dla każdej ze stacji płyty ratunkowej. 18. Konsola musi być dostępna z poziomu przeglądarki internetowej. 19. Administrator powinien mieć możliwość zarządzania stacjami klienckimi, które mają dostep do sieci Internet, niezależnie od tego, gdzie komputery w danym momencie się znajdują. 20. Administrator musi mieć możliwość wykonania poniższych czynności w sposób zdalny: a) instalacji klienta na stacji b) zaszyfrowania/odszyfrowania stacji c) wygenerowania klucza aktywacyjnego dla użytkownika d) zablokowania stacji, e) zablokowania użytkownika, f) administrowania kluczami szyfrującymi, g) administrowania użytkownikami, którzy mają dostęp do stacji, h) administrowania profilem ustawień dla użytkowników, i) administrowania profilem ustawień dla stacji roboczych j) wymuszenia zmiany hasła k) zarządzania wieloma organizacjami z poziomu jednej konsoli 21. System szyfrowania danych musi wspierać instalacje aplikacji klienckiej w środowisku Microsoft Windows XP SP3/Vista/7/8/10 32-bit i 64-bit oraz w środowiskach Microsoft Windows Server 2003 32-bit i 64-bit, 2008 32-bit i 64-bit, 2012 64-bit. 22. Administrator ma możliwość zainstalowania systemu szyfrowania danych w środowisku wirtualnym (VMWARE). 23. System musi posiadać certyfikat FIPS 140-2 Level 1 24. System szyfrowania danych powinien być dostępny przynajmniej w języku polskim i angielskim. 25. System szyfrowania danych powinien umożliwiać zarządzanie z poziomu konsoli centralnego zarządzania (zależnie od rodzaju licencji).							

	26. Hasło dla użytkowników na stacjach roboczych powinno zawierać co najmniej poniższe założenia (w przypadku wersji centralnie zarządzanej): a) Ilość nieudanych logowań b) Możliwość zmiany hasła c) Ważność hasła d) Ilość znaków e) Ilość wielkich liter f) Ilość małych liter g) Ilość znaków numerycznych h) Ilość znaków specjalnych 27. Defragmentacja dysku nie może mieć negatywnego wpływu na system szyfrowania. 28. System szyfrowania danych musi umożliwiać szyfrowanie nośników wymiennych w następujący sposób: a) Sektor po sektorze, b) Kontener. 29. Zaszyfrowany nośnik wymienny oraz nośnik CD/DVD może być odczytany także na dowolnej stacji na której nie ma zainstalowanego klienta systemu szyfrowania. Dostęp do takiego nośnika musi być udzielony po podaniu hasła. 30. Dostęp do zaszyfrowanych nośników wymiennych lub zaszyfrowanych nośników CD/DVD może być zabezpieczony hasłem. 31. System szyfrowania danych musi pozwalać na szyfrowanie wiadomości e-mail wraz z załącznikami. 32. System szyfrowania danych musi umożliwiać automatyczną deszyfrację otrzymywanych wiadomości e-mail. 33. System szyfrowania danych musi pozwalać na szyfrowanie całego tekstu aktywnego dokumentu, jego części a także zawartości schowka systemowego. 34. Zaszyfrowany tekst oraz zawartość schowka systemowego może być odczytana w wbudowanej przeglądarce. 35. Zaszyfrowany tekst może być odczytany za pomocą darmowego narzędzia dostarczanego przez producenta na stacji bez zainstalowanego klienta systemu szyfrowania. 36. System szyfrowania danych powinien umożliwiać wybór klucza szyfrującego (w przypadku posiadania wielu kluczy w pęku), który ma być używany w procesie szyfrowania. 37. System szyfrowania danych powinien umożliwiać wybór domyślnego klucza szyfrowania. 38. System szyfrowania danych powinien umożliwiać zaszyfrowanie obiektu z poziomu menu kontekstowego. 39. System szyfrowania danych powinien umożliwiać zaszyfrowanie obiektu z poziomu menu kontekstowego a następnie wysłanie go przy pomocy dedykowanego klienta pocztowego jako załącznik. 40. Możliwe jest utworzenie skrótów klawiszowych umożliwiających zaszyfrowanie/odszyfrowanie całego tekstu aktywnego dokumentu, jego części a także zawartości schowka systemowego. 41. System szyfrowania danych powinien umożliwiać tworzenie wirtualnych partycji. Dostęp do takich partycji ma być możliwy przy użyciu klucza szyfrującego lub hasła. 42. System szyfrowania danych powinien umożliwiać zdefiniowanie wielkości wirtualnej partycji, z dokładnością do 1MB. 43. System szyfrowania danych musi umożliwiać tworzenie zaszyfrowanego archiwum. Dostęp do takiego archiwum ma być możliwy przy użyciu klucza szyfrującego lub hasła. 44. System szyfrowania danych powinien umożliwiać trwałe usuwanie danych za pomocą poniższych algorytmów: a) Guttman b) US Department of Defence 5220.22-M (8-306. /E) c) US Department of Defence 5220.22-M (8-306. /E, CiE)							

	d) Cryptographic Random Number Data 45. Dedykowana wtyczka powinna wspierać co najmniej klientów pocztowych MS Outlook 2003 lub nowszych, również dostępnych z poziomu Office 365. 46. System szyfrowania danych powinien umożliwiać automatyczne zalogowanie użytkownika do konsoli klienta systemu szyfrowania danych po uruchomieniu systemu operacyjnego. 47. System szyfrowania danych powinien umożliwiać automatyczne wylogowanie z aplikacji w przypadku bezczynności użytkownika w systemie. 48. System szyfrowania danych powinien posiadać opcję automatycznego odpytywania serwerów producenta o dostępność nowszych wersji. 49. Użytkownik powinien posiadać możliwość ręcznego sprawdzania czy dostępna jest nowsza wersja programu, z poziomu GUI. 50. System szyfrowania danych powinien posiadać możliwość szyfrowania pojedynczych plików, zawartości katalogów, pamięci przenośnych, wiadomości e-mail wraz z załącznikami, tekstu oraz schowka systemowego. 51.Wymagane jest wykorzystanie do szyfrowania poniższych algorytmów szyfrowania: a) AES (Rijndael) b) Blowfish c) Triple DES (3DES) 52. System szyfrowania danych powinien umożliwiać współpracę z dyskami SSD. **Licencja na 12 miesięcy**							
14	**Oprogramowanie Autodesk AutoCAD LT 2018 Commercial New Single-user ELD 3-Year Subscription** Licencja komercyjna na 36 miesięcy		**1 szt**					
15	**Microsoft Windows 10 Pro 64 bity** Polska wersja językowa Licencja komercyjna wieczysta Wersja BOX Typ nośnika USB		**1 szt**					
16	**Acronis True Image 2018 5 komputerów pakiet Standard zakup jednorazowy**		**1 szt**					
17	**RAZEM:**	**X**	**X**	**X**	……	**X**	……	……

1. **W niniejszym załączniku do SIWZ prosimy wypełnić kolumny: 3, 5, 6, 7, 8 i 9 w poz. 1 do 16, natomiast w poz. 17 prosimy wypełnić kolumny 6,8 i 9.**
2. **W przypadku potrzeby wstępnej rejestracji zamawianych urządzeń, licencji, Zamawiający udzieli Wykonawcy wszelkich niezbędnych informacji, potrzebnych do przeprowadzenia procesu rejestracji.**
3. **Wykonawca, który powołuje się na rozwiązania równoważne opisywane przez Zamawiającego w Załączniku do SIWZ „WYKAZ ZAMAWIANEGO OPROGRAMOWANIA – ZESTAWIENIE CEN JEDNOSTKOWYCH " jest zobowiązany wykazać, że oferowane przez niego urządzenia, spełniają wymagania określone przez Zamawiającego.**
4. **Wymaganie konkretnego asortymentu urządzeń lub oprogramowania wynika z dotychczas zastosowanych rozwiązań.**