Załącznik nr 1B do SIWZ

Szczegółowy opis przedmiotu zamówienia- wymagania sprzętowe dla infrastruktury klienckiej

1. Wymagania szczegółowe dla Infrastruktury sprzętowej

1.1. Zestawy- stanowiska komputerowe- 150 sztuk

1.1.1. Jednostka centralna

Lp.	Parametr	Charakterystyka (wymagania minimalne)
1.	Komputer	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu.
2.	Obudowa	Typu Small Form Factor z obsługą kart PCI Express wyłącznie o niskim profilu. Wyposażona w min. 2 kieszenie: 1 szt. 5,25” zewnętrzna (dopuszcza się w wersji tzw. slim zajętej przez napęd optyczny), 1 szt. 3,5”, możliwość rozbudowy komputera do konfiguracji dwudyskowej w oparciu o dyski w rozmiarach 2.5” + 3,5”. Obudowa musi być wyposażona w czujnik otwarcia obudowy. Obudowa musi mieć możliwość zainstalowania oryginalnego filtra przeciwpyłowego zapobiegającego nadmiernemu gromadzeniu się kurzu w środku obudowy. Filtr musi umożliwiać łatwe czyszczenie bez otwierania obudowy. Wymagana możliwość czyszczenia filtra za pomocą wody. Filtr musi być także opcją producenta komputera możliwą do zamówienia jako część eksploatacyjna. W ofercie należy podać numer katalogowy (PN) części pod jaką można zamówić filtr u producenta komputera. Bez narzędziowe otwieranie obudowy oraz wymiana HDD, ODD i kart rozszerzających. Obudowa trwale oznaczona nazwą producenta, nazwą komputera, numerem katalogowym PN, numerem seryjnym. Obudowa gotowa do pracy w trybie Pion lub Poziom.
3.	Chipset	Dostosowany do zaoferowanego procesora.
4.	Płyta główna	Zaprojektowana i wyprodukowana przez producenta komputera, trwale oznaczona nazwą producenta komputera (na etapie produkcji). Wyposażona złącza dla kart PCIe oraz umożliwiająca ich montaż obudowa:1 x PCI Express 3.0 x16,2 x PCI Express 2.0 x1,
5.	Procesor	Procesor osiągający w teście PassMark CPU Mark wynik min. 5900 punktów (wynik zaproponowanego procesora musi znajdować się na stronie: www.cpubenchmark.net).

6.	Pamięć operacyjna	Min. 4 GB RAM, 2400MHz DDR4, 4 sloty na pamięć, z czego 3wolny. Możliwość rozbudowy do 64 GB.
7.	Dysk twardy	Min. 500GB 7200 obr./min., zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii.
8.	Napęd optyczny	Nagrywarka DVD +/-RW wyposażona w tackę z zaczepami umożliwiającymi pracę w poziomie i pionie.
9.	Karta graficzna	Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki. Karta graficzną osiągająca min. 1220 pkt w teście Videocard Benchmark (http://www.videocardbenchmark.net/)
10.	Audio	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition.
11.	Karta sieciowa	10/100/1000 – złącze RJ45
12.	Porty/złącza	Wbudowane porty: 1 x VGA, 2 x DP, 8 x USB w tym: - z przodu obudowy min.:4x USB3.1 Gen 1 - z tyłu obudowy min.: 2x USB3.1 Gen 1, 2x USB2.0, - 1 x port sieciowy RJ-45, - 2 x port szeregowy RS-232, - 1 x port równoległy, - porty słuchawek i mikrofonu na przednim lub tylnym panelu obudowy Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.
13.	Klawiatura/mysz	Klawiatura przewodowa USB w układzie US, wyposażona w czytnik kart mikroprocesorowych; mysz przewodowa USB z rolką (scroll)
14.	Zasilacz	Energooszczędny zasilacz o mocy nie większej niż 210W oraz sprawności na poziomie: • 20% obciążenia 83% sprawności, • na poziomie 50% obciążenia 85% sprawności • na poziomie 100% obciążenia 83% sprawności. Zasilacz musi posiadać certyfikat 80 PLUS klasy min BRONZE. Należy dołączyć certyfikat ze strony https://plugloadsolutions.com/80pluspowersupplies.aspx potwierdzający spełnianie w/w wymogu.
15.	System operacyjny	System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet

		lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.

		19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)." 24. Wbudowany mechanizm wirtualizacji typu hypervisor." 25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 34. Możliwość tworzenia wirtualnych kart inteligentnych. 35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.

		37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38. Mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty inteligentne i certyfikaty (smartcard), c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN e. Certyfikat/Klucz i uwierzytelnienie biometryczne 39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń
16.	Oprogramowanie antywirusowe	1. Pełne wsparcie dla systemu zaproponowanego przez Wykonawcę w ofercie– LICENCJA NA OKRES MINIMUM 36 MIESIĘCY 2. Wersja programu dla stacji roboczych dostępna zarówno w języku polskim jak i angielskim. **Ochrona antywirusowa i antyspyware** 3. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 4. Wbudowana technologia do ochrony przed rootkitami. 5. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 6. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 7. System ma oferować administratorowi możliwość definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym i jeśli tak – nie wykonywało danego zadania. 8. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami 9. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu. 10. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu. 11. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.

		12. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera. 13. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera. 14. 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. 15. 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). 16. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. 17. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail. 18. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie. 19. 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. 20. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. 21. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 22. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe. 23. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta. 24. Program musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. 25. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym. 26. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego. 27. 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. 28. 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. 29. Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika. 30. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła. 31. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo. 32. 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. 33. Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów. 34. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku. 35. 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. 36. 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. 37. 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. 38. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. 39. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika. 40. Użytkownik ma posiadać możliwość takiej konfiguracji programu aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika 41. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS). 42. Oprogramowanie musi posiadać zaawansowany skaner pamięci. 43. Program musi być wyposażona w mechanizm ochrony przed exploitami w

		popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp. 44. 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. 45. 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. 46. 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. 47. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu. 48. Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji program zgłosi posiadanie nieaktualnej bazy sygnatur. 49. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji. 50. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http 51. Program musi być wyposażona w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (roll back). 52. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa). 53. 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. 54. Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli stron Internetowych i kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania. 55. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. 56. Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline. 57. W programie musi istnieć możliwość tymczasowego wstrzymania polityk wysłanych z poziomu serwera zdalnej administracji. 58. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej. 59. 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.

		Ochrona przed spamem 60. Program ma umożliwiać uaktywnienie funkcji wyłączenia skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej. 61. Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego. 62. Możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną wiadomość i odwrotnie oraz ręcznego dodania wiadomości do białej i czarnej listy z wykorzystaniem funkcji programu zintegrowanych z programem pocztowym. 63. Możliwość definiowania swoich własnych folderów, gdzie program pocztowy będzie umieszczać spam. 64. Możliwość zdefiniowania dowolnego Tag-u dodawanego do tematu wiadomości zakwalifikowanej jako spam. 65. Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną zmieni jej właściwość jako „nieprzeczytana" oraz w momencie zaklasyfikowania wiadomości jako spam na automatyczne ustawienie jej właściwości jako „przeczytana". 66. Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera. **Zapora osobista (personal firewall)** 67. Zapora osobista ma pracować jednym z 4 trybów: • tryb automatyczny – program blokuje cały ruch przychodzący i zezwala tylko na znane, bezpieczne połączenia wychodzące, jednocześnie umożliwia utworzenie dodatkowych reguł przez administratora • tryb interaktywny – program pyta się o każde nowe nawiązywane połączenie i automatycznie tworzy dla niego regułę (na stałe lub tymczasowo), • tryb oparty na regułach – użytkownik/administrator musi ręcznie zdefiniować reguły określające jaki ruch jest blokowany a jaki przepuszczany, • tryb uczenia się – umożliwia zdefiniowanie przez administratora określonego okresu czasu w którym oprogramowanie samo tworzy odpowiednie reguły zapory analizując aktywność sieciową danej stacji. 68. Program musi akceptować istniejące reguły w zaporze systemu zaproponowanej przez Wykonawcę w ofercie, zezwalające na ruch przychodzący 69. Możliwość tworzenia list sieci zaufanych. 70. Możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie 71. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego. 72. Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer w tym minimum dla strefy zaufanej i sieci Internet. 73. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz

		wykrywaniem aktywności wirusów sieciowych. 74. Program musi umożliwiać ochronę przed przyłączeniem komputera do sieci botnet. 75. Wykrywanie zmian w aplikacjach korzystających z sieci i monitorowanie o tym zdarzeniu. 76. Program ma oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6. 77. Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci. 78. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci 79. Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowaniu sieci bezprzewodowej lub jego braku, aktywności połączenia bezprzewodowego lub jego braku, konkretny interfejs sieciowy w systemie. 80. Program musi możliwość ustalenia tymczasowej czarnej listy adresów IP, które będą blokowane podczas próby połączenia. 81. Program musi posiadać kreator, który umożliwia rozwiązać problemy z połączeniem. **Kontrola dostępu do stron internetowych** 82. Aplikacja musi być wyposażona w zintegrowany moduł kontroli odwiedzanych stron internetowych. 83. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane zdefiniowane reguły. 84. Profile mają być automatycznie aktywowane w zależności od zalogowanego użytkownika. 85. Podstawowe kategorie w jakie aplikacja musi być wyposażona to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii. 86. Moduł musi posiadać także możliwość grupowania kategorii już istniejących. 87. Aplikacja musi posiadać możliwość określenia uprawnień dla dostępu do kategorii url – zezwól, zezwól i ostrzeż, blokuj. 88. Program musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania określonej w regułach witryny. **Ochrona serwera plików** 1. Wsparcie dla systemów zaproponowanych przez Wykonawcę w ofercie. 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. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 8. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych. 9. Użytkownik ma mieć możliwość zmiany ilości wątków skanowania w ustawieniach systemu antywirusowego. 10. Możliwość skanowania dysków sieciowych i dysków przenośnych. 11. Skanowanie plików spakowanych i skompresowanych. 12. 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. 13. Aplikacja powinna wspierać mechanizm klastrowania. 14. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS). 15. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS. 16. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. 17. Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model i wersję modelu urządzenia. 18. 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. 19. Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. 20. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 21. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony. 22. Dodanie automatycznych wyłączeń nie wymaga restartu serwera. 23. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych. 24. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji. 25. W przypadku restartu serwera – usunięte z listy wyłączeń elementy mają być automatycznie uzupełnione. 26. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego. 27. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line). 28. 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. 29. 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. 30. 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. 31. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. 32. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail. 33. 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. 34. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji ma być takie samo. 35. 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. 36. 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. 37. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym. 38. 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. 39. 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. 40. 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. 41. 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). 42. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy. 43. Aplikacja musi wspierać skanowanie magazynu Hyper-V 44. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów

		45. 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). 46. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 47. 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 zaproponowanych przez Wykonawcę w ofercie. 2. Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance). 3. 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. 4. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej. 5. Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6. 6. Podczas logowania administrator musi mieć możliwość wyboru języka w jakim zostanie wyświetlony panel zarządzający. 7. Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL. 8. Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci. 9. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych. 10. Instalacja serwera administracyjnego powinna oferować wybór trybu pracy serwera w sieci w przypadku rozproszonych sieci –serwer pośredniczący (proxy) lub serwer centralny. 11. Serwer proxy musi pełnić funkcję pośrednika pomiędzy lokalizacjami zdalnymi a serwerem centralnym. 12. Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM. 13. 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. 14. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów. 15. Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy. 16. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci.

		17. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta. 18. Agent musi posiadać możliwość pobrania listy zainstalowanego oprogramowania firm trzecich na stacji roboczej z możliwością jego odinstalowania. 19. Serwer administracyjny musi oferować możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie. 20. Instalacja klienta na urządzeniach mobilnych musi być dostępna za pośrednictwem portalu WWW udostępnionego przez moduł MDM z poziomu urządzenia użytkownika. 21. Administrator musi posiadać możliwość utworzenia listy zautoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji. 22. 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. 23. Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi. 24. Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp. 25. Administrator musi posiadać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli zarządzającej. 26. Dwu fazowa autoryzacja musi się odbywać za pomocą wiadomości SMS lub haseł jednorazowych generowanych na urządzeniu mobilnym za pomocą dedykowanej aplikacji. 27. Administrator musi posiadać możliwość nadania dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko do odczytu, odczyt/zapis. 28. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika. 29. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności po jakim użytkownik zostanie automatycznie wylogowany. 30. 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. 31. Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym. 32. Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu. 33. Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką. 34. Serwer administracyjny musi oferować możliwość utworzenia grup

		statycznych i dynamicznych komputerów. 35. 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. 36. 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. 37. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej. 38. 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. 39. Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania. 40. Serwer administracyjny musi oferować możliwość wyboru formy przedstawienia danych w raporcie w postaci tabeli, wykresu lub obu elementów jednocześnie. 41. Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym dostępnym z poziomu interfejsu konsoli WWW. 42. Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub PS. 43. Serwer administracyjny musi oferować możliwość maksymalizacji wybranego elementu monitorującego. 44. Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy. 45. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP. 46. Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu. 47. Serwer administracyjny musi oferować możliwość podłączenia serwera administracji zdalnej do portalu zarządzania licencjami dostępnego na serwerze producenta. 48. Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji. 49. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty. 50. Serwer administracyjny musi być wyposażona w machizm auto dopasowania kolumn w zależności od rozdzielczości urządzenia na jakim jest wyświetlana. 51. Administrator musi mieć możliwość określenia zakresu czasu w jakim dane zadanie będzie wykonywane (sekundy, minuty, godziny, dni, tygodnie). 52. 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.

17.	BIOS	BIOS zgodny ze specyfikacją UEFI - Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych informacji o: modelu komputera, PN, numerze seryjnym, Asset Tag, MAC Adres karty sieciowej, wersja Biosu wraz z datą produkcji, zainstalowanym procesorze, jego taktowaniu i ilości rdzeni, ilości pamięci RAM wraz z taktowaniem, stanie pracy wentylatora na procesorze, stanie pracy wentylatorów w obudowie komputera, napędach lub dyskach podłączonych do portów M.2 oraz SATA (model dysku twardego i napędu optycznego) Możliwość z poziomu Bios: wyłączenia/włączenia selektywnego (pojedynczo) portów USB zarówno z przodu jak i z tyłu obudowy; wyłączenia kontrolera selektywnego (pojedynczego) portów SATA; konfiguracji kontrolera SATA; wyłączenia karty sieciowej, karty audio, portu szeregowego, wbudowanego głośnika, PXE; możliwość ustawienia portów USB w jednym z dwóch trybów: 1. użytkownik może kopiować dane z urządzenia pamięci masowej podłączonego do pamięci USB na komputer ale nie może kopiować danych z komputera na urządzenia pamięci masowej podłączone do portu USB 2. użytkownik nie może kopiować danych z urządzenia pamięci masowej podłączonego do portu USB na komputer oraz nie może kopiować danych z komputera na urządzenia pamięci masowej ustawienia hasła: administratora, Power-On, HDD; blokady aktualizacji BIOS bez podania hasła administratora; wglądu w system zbierania logów (min. Informacja o update Bios, błędzie wentylatora na procesorze, wyczyszczeniu logów) z możliwością czyszczenia logów; alertowania zmiany konfiguracji sprzętowej komputera; wyboru trybu uruchomienia komputera po utracie zasilania (włącz, wyłącz, poprzedni stan); ustawienia trybu wyłączenia komputera w stan niskiego poboru energii; zdefiniowania trzech sekwencji botujących (podstawowa, WOL, po awarii); załadowania optymalnych ustawień BIOS, obsługa BIOS za pomocą klawiatury i myszy bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.
18.	Zintegrowany System Diagnostyczny	Wizualny system diagnostyczny producenta działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera umożliwiający na wykonanie diagnostyki następujących podzespołów: • wykonanie testu pamięci RAM • test dysku twardego • test monitora • test magistrali PCI-e • test portów USB • test płyty głównej Wizualna lub dźwiękowa sygnalizacja w przypadku błędów któregokolwiek z powyższych podzespołów komputera. Ponadto system powinien umożliwiać identyfikacje testowanej jednostki i jej komponentów w następującym zakresie: • PC: Producent, model

		• BIOS: Wersja oraz data wydania Bios • Procesor : Nazwa, taktowanie • Pamięć RAM : Ilość zainstalowanej pamięci RAM, producent oraz numer seryjny poszczególnych kości pamięci • Dysk twardy: model, numer seryjny, wersja firmware, pojemność, temperatura pracy • Monitor: producent, model, rozdzielczość System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera.
19.	Certyfikaty i standardy	- Certyfikat ISO9001:2000 dla producenta sprzętu – ENERGY STAR 6.1 - Deklaracja zgodności CE - Głośność jednostki mierzona z pozycji operatora z umiejscowieniem komputera na biurku w trybie IDLE 23 dB - dołączyć certyfikat lub dokument potwierdzający głośność jednostki - Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki
20.	Waga/rozmiary urządzenia	Waga urządzenia max. 7kg Suma wymiarów nie może przekraczać: 735mm
21.	Bezpieczeństwo i zdalne zarządzanie	- Złącze typu Kensington Lock umożliwiające zastosowanie zabezpieczenia fizycznego w postaci linki metalowej uniemożliwiającej również otwarcie obudowy - Dedykowane oczko na kłódkę umożliwiającą zastosowanie zabezpieczenia fizycznego przed otwarciem obudowy - Moduł TPM 2.0
22.	Oprogramowanie	Dedykowane oprogramowanie producenta sprzętu umożliwiające automatyczna weryfikacje i instalację sterowników oraz oprogramowania użytkowego producenta w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralna bazą sterowników i oprogramowania użytkowego producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika. Oprogramowanie musi być wyposażone w moduł rejestru zdarzeń, w którym znajdują się informacje o tym kiedy i jakie sterowniki zostały zainstalowane na danej maszynie. Oprogramowanie musi zapewniać również ustawienie automatycznego uaktualnienia wszystkich sterowników we wskazanym dniu miesiąca.
23.	Gwarancja	minimum 3 lata świadczona w miejscu użytkowania sprzętu (on-site) z gwarantowanym czasem reakcji w następnym dniu roboczym. Oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. Sprzęt musi być wyprodukowany nie wcześniej niż w II połowie 2017 roku.
24.	Wsparcie techniczne	Dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej. Możliwość weryfikacji na stronie producenta konfiguracji fabrycznej zakupionego sprzętu. Naprawy gwarancyjne urządzeń muszą być realizowany przez

	producenta	Producenta lub Autoryzowanego Partnera Serwisowego Producenta.
25.	Dodatkowe	Przewód Patchcord UTP kategorii 6A, RJ 45, długość 3 metry

1.1.2. Monitor – 150 sztuk

L.p.	Parametr	Charakterystyka (wymagania minimalne)
1.	Przekątna ekranu i wymiary aktywnego obszaru wyświetlania	21,5“ 476 mm x 268 mm
2.	zalecana rozdzielczość	1920 x 1080 (Full HD)
3.	Typowy pobór mocy / w trybie Power management	19 W / 0,5 W
4.	złącza	VGA, HDMI
5.	kontrast typowy	600 : 1
6.	kontrast ACR	10 000 000 : 1
7.	Jasność typowa	200 cd/m2
8.	wielkość plamki	0,248 mm
9.	Czas reakcji	5 ms
10.	Kąt widzenia przy CR>10	poziomo/pionowo: min. 90°/65°
11.	Regulacja cyfrowa OSD	TAK
12.	Certyfikaty i standardy	- CE, - EnergyStar 6.0, - TCO, - EPEAT Silver
13.	Gwarancja	minimum 36 miesięcy

1.2. Zestawy- stanowiska komputerowe- 10 sztuk

1.2.1. Jednostka centralna

Lp.	Parametr	Charakterystyka (wymagania minimalne)
1.	Komputer	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu.
2.	Obudowa	Typu Small Form Factor z obsługą kart PCI Express wyłącznie o niskim profilu. Wyposażona w min. 2 kieszenie: 1 szt. 5,25” zewnętrzna (dopuszcza się w wersji

		tzw. slim zajętej przez napęd optyczny), 1 szt. 3,5", możliwość rozbudowy komputera do konfiguracji dwudyskowej w oparciu o dyski w rozmiarach 2.5" + 3,5". Obudowa musi być wyposażona w czujnik otwarcia obudowy. Obudowa musi mieć możliwość zainstalowania oryginalnego filtra przeciwpyłowego zapobiegającego nadmiernemu gromadzeniu się kurzu w środku obudowy. Filtr musi umożliwiać łatwe czyszczenie bez otwierania obudowy. Wymagana możliwość czyszczenia filtra za pomocą wody. Filtr musi być także opcją producenta komputera możliwą do zamówienia jako część eksploatacyjna. W ofercie należy podać numer katalogowy (PN) części pod jaką można zamówić filtr u producenta komputera. Bez narzędziowe otwieranie obudowy oraz wymiana HDD, ODD i kart rozszerzających. Obudowa trwale oznaczona nazwą producenta, nazwą komputera, numerem katalogowym PN, numerem seryjnym. Obudowa gotowa do pracy w trybie Pion lub Poziom.
3.	Chipset	Dostosowany do zaoferowanego procesora.
4.	Płyta główna	Zaprojektowana i wyprodukowana przez producenta komputera, trwale oznaczona nazwą producenta komputera (na etapie produkcji). Wyposażona złącza dla kart PCIe oraz umożliwiająca ich montaż obudowa:1 x PCI Express 3.0 x16,2 x PCI Express 2.0 x1,
5.	Procesor	Procesor osiągający w teście PassMark CPU Mark wynik min. 5900 punktów (wynik zaproponowanego procesora musi znajdować się na stronie: www.cpubenchmark.net).
6.	Pamięć operacyjna	Min. 4 GB RAM, 2400MHz DDR4, 4 sloty na pamięć, z czego 3wolny. Możliwość rozbudowy do 64 GB.
7.	Dysk twardy	Min. 500GB 7200 obr./min., zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii.
8.	Napęd optyczny	Nagrywarka DVD +/-RW wyposażona w tackę z zaczepami umożliwiającymi pracę w poziomie i pionie.
9.	Karta graficzna	Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki. Karta graficzną osiągająca min. 1220 pkt w teście Videocard Benchmark (http://www.videocardbenchmark.net/)
10.	Audio	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition.
11.	Karta sieciowa	10/100/1000 – złącze RJ45
12.	Porty/złącza	Wbudowane porty: 1 x VGA, 2 x DP, 8 x USB w tym: - z przodu obudowy min.:4x USB3.1 Gen 1,

		- z tyłu obudowy min.: 2x USB3.1 Gen 1, 2x USB2.0 - 1 x port sieciowy RJ-45, - 2 x port szeregowy RS-232 - 1 x port równoległy - porty słuchawek i mikrofonu na przednim lub tylnym panelu obudowy Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.
13.	Klawiatura/mysz	Klawiatura przewodowa USB w układzie US, wyposażona w czytnik kart mikroprocesorowych; Mysz przewodowa USB z rolką (scroll)
14.	Zasilacz	Energooszczędny zasilacz o mocy nie większej niż 210W oraz sprawności na poziomie: - 20% obciążenia 83% sprawności, - na poziomie 50% obciążenia 85% sprawności - na poziomie 100% obciążenia 83% sprawności. Zasilacz musi posiadać certyfikat 80 PLUS klasy min BRONZE. Należy dołączyć certyfikat ze strony https://plugloadsolutions.com/80pluspowersupplies.aspxpotwierdzający spełnianie w/w wymogu.
15.	System operacyjny	System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu,

		pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)." 24. Wbudowany mechanizm wirtualizacji typu hypervisor."

		25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 34. Możliwość tworzenia wirtualnych kart inteligentnych. 35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38. Mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty inteligentne i certyfikaty (smartcard), c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN e. Certyfikat/Klucz i uwierzytelnienie biometryczne 39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji

		roboczej. 41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń
16.	Oprogramowanie antywirusowe	1. Pełne wsparcie dla systemu zaproponowanego przez Wykonawcę w ofercie– LICENCJA NA OKRES MINIMUM 36 MIESIĘCY 2. Wersja programu dla stacji roboczych dostępna zarówno w języku polskim jak i angielskim. **Ochrona antywirusowa i antyspyware** 3. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 4. Wbudowana technologia do ochrony przed rootkitami. 5. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 6. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 7. System ma oferować administratorowi możliwość definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym i jeśli tak – nie wykonywało danego zadania. 8. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami 9. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu. 10. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu. 11. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu. 12. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera. 13. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera. 14. 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. 15. 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).

		16. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. 17. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail. 18. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie. 19. 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. 20. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. 21. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 22. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe. 23. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta. 24. Program musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. 25. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym. 26. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego. 27. 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. 28. 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. 29. Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika. 30. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do

		konfiguracji był proszony o podanie hasła. 31. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo. 32. 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. 33. Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów. 34. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku. 35. 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. 36. 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. 37. 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. 38. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. 39. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika. 40. Użytkownik ma posiadać możliwość takiej konfiguracji programu aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika 41. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS). 42. Oprogramowanie musi posiadać zaawansowany skaner pamięci. 43. Program musi być wyposażona w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp. 44. 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. 45. 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. 46. 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. 47. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu. 48. Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji program zgłosi posiadanie nieaktualnej bazy sygnatur. 49. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji. 50. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http 51. Program musi być wyposażona w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (roll back). 52. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa). 53. 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. 54. Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli stron Internetowych i kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania. 55. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. 56. Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline. 57. W programie musi istnieć możliwość tymczasowego wstrzymania polityk wysłanych z poziomu serwera zdalnej administracji. 58. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej. 59. 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. **Ochrona przed spamem** 60. Program ma umożliwiać uaktywnienie funkcji wyłączenia skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej. 61. Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego. 62. Możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną wiadomość i odwrotnie oraz ręcznego dodania wiadomości do białej i czarnej listy z wykorzystaniem funkcji programu zintegrowanych z

		programem pocztowym. 63. Możliwość definiowania swoich własnych folderów, gdzie program pocztowy będzie umieszczać spam. 64. Możliwość zdefiniowania dowolnego Tag-u dodawanego do tematu wiadomości zakwalifikowanej jako spam. 65. Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną zmieni jej właściwość jako „nieprzeczytana" oraz w momencie zaklasyfikowania wiadomości jako spam na automatyczne ustawienie jej właściwości jako „przeczytana". 66. Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera. **Zapora osobista (personal firewall)** 67. Zapora osobista ma pracować jednym z 4 trybów: • tryb automatyczny – program blokuje cały ruch przychodzący i zezwala tylko na znane, bezpieczne połączenia wychodzące, jednocześnie umożliwia utworzenie dodatkowych reguł przez administratora • tryb interaktywny – program pyta się o każde nowe nawiązywane połączenie i automatycznie tworzy dla niego regułę (na stałe lub tymczasowo), • tryb oparty na regułach – użytkownik/administrator musi ręcznie zdefiniować reguły określające jaki ruch jest blokowany a jaki przepuszczany, • tryb uczenia się – umożliwia zdefiniowanie przez administratora określonego okresu czasu w którym oprogramowanie samo tworzy odpowiednie reguły zapory analizując aktywność sieciową danej stacji. 68. Program musi akceptować istniejące reguły w zaporze systemu zaproponowanej przez Wykonawcę w ofercie, zezwalające na ruch przychodzący 69. Możliwość tworzenia list sieci zaufanych. 70. Możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie 71. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego. 72. Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer w tym minimum dla strefy zaufanej i sieci Internet. 73. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 74. Program musi umożliwiać ochronę przed przyłączeniem komputera do sieci botnet. 75. Wykrywanie zmian w aplikacjach korzystających z sieci i monitorowanie o tym zdarzeniu. 76. Program ma oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6. 77. Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.

78. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci
79. Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowaniu sieci bezprzewodowej lub jego braku, aktywności połączenia bezprzewodowego lub jego braku, konkretny interfejs sieciowy w systemie.
80. Program musi możliwość ustalenia tymczasowej czarnej listy adresów IP, które będą blokowane podczas próby połączenia.
81. Program musi posiadać kreator, który umożliwia rozwiązać problemy z połączeniem.

Kontrola dostępu do stron internetowych

82. Aplikacja musi być wyposażona w zintegrowany moduł kontroli odwiedzanych stron internetowych.
83. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane zdefiniowane reguły.
84. Profile mają być automatycznie aktywowane w zależności od zalogowanego użytkownika.
85. Podstawowe kategorie w jakie aplikacja musi być wyposażona to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii.
86. Moduł musi posiadać także możliwość grupowania kategorii już istniejących.
87. Aplikacja musi posiadać możliwość określenia uprawnień dla dostępu do kategorii url – zezwól, zezwól i ostrzeż, blokuj.
88. Program musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania określonej w regułach witryny.

Ochrona serwera plików

48. Wsparcie dla systemów zaproponowanych przez Wykonawcę w ofercie.
49. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
50. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
51. Wbudowana technologia do ochrony przed rootkitami i exploitami.
52. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
53. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
54. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
55. System antywirusowy ma mieć możliwość wykorzystania wielu wątków

		skanowania w przypadku maszyn wieloprocesorowych. 56. Użytkownik ma mieć możliwość zmiany ilości wątków skanowania w ustawieniach systemu antywirusowego. 57. Możliwość skanowania dysków sieciowych i dysków przenośnych. 58. Skanowanie plików spakowanych i skompresowanych. 59. 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. 60. Aplikacja powinna wspierać mechanizm klastrowania. 61. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS). 62. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS. 63. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. 64. Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model i wersję modelu urządzenia. 65. 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. 66. Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. 67. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 68. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony. 69. Dodanie automatycznych wyłączeń nie wymaga restartu serwera. 70. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych. 71. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji. 72. W przypadku restartu serwera – usunięte z listy wyłączeń elementy mają być automatycznie uzupełnione. 73. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego. 74. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line). 75. 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. 76. 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. 77. 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. 78. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. 79. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail. 80. 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. 81. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji ma być takie samo. 82. 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. 83. 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. 84. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym. 85. 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. 86. 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. 87. 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. 88. 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). 89. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy. 90. Aplikacja musi wspierać skanowanie magazynu Hyper-V 91. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów 92. 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). 93. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).

		94. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. **Administracja zdalna** 53. Serwer administracyjny musi oferować możliwość instalacji na systemach zaproponowanych przez Wykonawcę w ofercie. 54. Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance). 55. 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. 56. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej. 57. Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6. 58. Podczas logowania administrator musi mieć możliwość wyboru języka w jakim zostanie wyświetlony panel zarządzający. 59. Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL. 60. Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci. 61. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych. 62. Instalacja serwera administracyjnego powinna oferować wybór trybu pracy serwera w sieci w przypadku rozproszonych sieci –serwer pośredniczący (proxy) lub serwer centralny. 63. Serwer proxy musi pełnić funkcję pośrednika pomiędzy lokalizacjami zdalnymi a serwerem centralnym. 64. Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM. 65. 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. 66. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów. 67. Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy. 68. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci. 69. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta. 70. Agent musi posiadać możliwość pobrania listy zainstalowanego oprogramowania firm trzecich na stacji roboczej z możliwością jego odinstalowania. 71. Serwer administracyjny musi oferować możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu

		oczekiwania na połączenie. 72. Instalacja klienta na urządzeniach mobilnych musi być dostępna za pośrednictwem portalu WWW udostępnionego przez moduł MDM z poziomu urządzenia użytkownika. 73. Administrator musi posiadać możliwość utworzenia listy zautoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji. 74. 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. 75. Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi. 76. Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp. 77. Administrator musi posiadać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli zarządzającej. 78. Dwu fazowa autoryzacja musi się odbywać za pomocą wiadomości SMS lub haseł jednorazowych generowanych na urządzeniu mobilnym za pomocą dedykowanej aplikacji. 79. Administrator musi posiadać możliwość nadania dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko do odczytu, odczyt/zapis. 80. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika. 81. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności po jakim użytkownik zostanie automatycznie wylogowany. 82. 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. 83. Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym. 84. Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu. 85. Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką. 86. Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów. 87. 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. 88. 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. 89. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej. 90. 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. 91. Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania. 92. Serwer administracyjny musi oferować możliwość wyboru formy przedstawienia danych w raporcie w postaci tabeli, wykresu lub obu elementów jednocześnie. 93. Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym dostępnym z poziomu interfejsu konsoli WWW. 94. Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub PS. 95. Serwer administracyjny musi oferować możliwość maksymalizacji wybranego elementu monitorującego. 96. Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy. 97. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP. 98. Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu. 99. Serwer administracyjny musi oferować możliwość podłączenia serwera administracji zdalnej do portalu zarządzania licencjami dostępnego na serwerze producenta. 100. Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji. 101. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty. 102. Serwer administracyjny musi być wyposażona w machizm auto dopasowania kolumn w zależności od rozdzielczości urządzenia na jakim jest wyświetlana. 103. Administrator musi mieć możliwość określenia zakresu czasu w jakim dane zadanie będzie wykonywane (sekundy, minuty, godziny, dni, tygodnie). 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.
17.	Oprogramowanie biurowe	Pakiet biurowy musi zawierać co najmniej: a) Edytor tekstów, b) Arkusz kalkulacyjny, c) Narzędzie do przygotowania i prowadzenia prezentacji,

		d) Narządziedozarządzaniapocztąelektroniczną,kalendarzamiizadaniami Ogólne: a) Interfejs w języku polskim, b) wbudowana pomoc kontekstowa, c) możliwość instalacji na dostarczonym sprzęcie i systemie operacyjnym Edytor tekstów: a) konwersja, pełna edycja i zapis plików w formatach: txt, rtf, doc, docx, odt, xml (wraz z atrybutami), b) edycja i formatowanie tekstu (m.in. tabel, obiektów graficznych, wzorów matematycznych, osadzania wykresów z arkusza kalkulacyjnego), c) tworzenie szablonów dokumentów, d) wbudowany słownik języka: polskiego, angielskiego oraz niemieckiego, e) wbudowana biblioteka obiektów graficznych i symboli, f) wbudowany mechanizm automatycznego sprawdzania pisowni oraz poprawności gramatycznej w ww. językach, g) edycja nagłówków i stopek, h) automatyczne numerowanie rozdziałów, tabel i rysunków, i) automatyczne tworzenie spisu treści, przypisów i odnośników do tekstu, j) śledzenie wprowadzonych zmian, k) zabezpieczenie plików hasłem (zarówno do odczytu jak i edycji), l) tworzenie korespondencji seryjnej, m) tworzenie makr, n) podgląd graficzny oraz wydruk dokumentów Arkusz kalkulacyjny: a) konwersja, pełna edycja i zapis plików w formatach: txt, csv, xls, xlsx, xml (wraz z atrybutami), b) tworzenie arkuszy kalkulacyjnych obejmujących dane tekstowe, liczbowe, walutowe, procentowe, ułamkowe oraz czasowe, c) tworzenie formuł obejmujących operacje: tekstowe, matematyczne, logiczne, statystyczne oraz operacje na danych finansowych i czasowych, d) tworzenie formuł obejmujących: wyszukiwanie danych, operacje na tabelach, e) tworzenie i osadzania wykresów (m.in. punktowych, liniowych, kolumnowych, słupkowych, warstwowych, kołowych, 3D), f) formatowanie warunkowe komórek arkusza, g) śledzenie formuł oraz automatyczna weryfikacja ich poprawności, h) tworzenie tabel przestawnych, i) raporty z wykorzystaniem wyszukiwania warunkowego, j) automatyczne filtrowania danych, k) automatyczne pobieranie danych z zewnętrznych źródeł: plików tekstowych, plików XML, arkuszy kalkulacyjnych, baz danych, l) zapis wielu arkuszy w jednym pliku, m) tworzenie szablonów dokumentów, n) wbudowany słownik języka: polskiego, angielskiego oraz niemieckiego, o) tworzenie oraz edycji nagłówków i stopek, p) osadzanie:symboli,tabel,rysunków,obiektówgraficznychorazwzorówmatem

		atycznych, q) zabezpieczenie plików hasłem (zarówno do odczytu jak i edycji), r) tworzenie korespondencji seryjnej, s) tworzenie makr, t) podgląd graficzny oraz wydruk dokumentów, Narzędzie do przygotowania i prowadzenia prezentacji: a) konwersja,pełnaedycjaizapisplikówwformatach:ppt,pptx,odp,xml(wrazzatrybutami), b) edycja i formatowanie tekstu (m.in. tabel, obiektów graficznych, wzorów matematycznych, osadzania wykresów z arkusza kalkulacyjnego), c) tworzenie szablonów prezentacji, d) tworzenie animacji dla pojedynczych elementów jak i całych slajdów, e) wbudowana biblioteka obiektów graficznych i symboli, f) elementy multimedialne (m.in. rysunków, obiektów graficznych, tabel, nagrań dźwiękowych oraz filmów), g) formatowanie tekstów, obiektów graficznych oraz tabel, h) umieszczanie notatek oraz podkładu dźwiękowego, i) wsparcie dla prowadzącego prezentacje (licznik czasu, obsługa projektora multimedialnego i konfiguracji dwumonitorowej), j) wbudowany słownik języka: polskiego, angielskiego oraz niemieckiego, k) wbudowany mechanizm automatycznego sprawdzania pisowni oraz poprawności gramatycznej w ww. językach, l) tworzenie oraz edycji nagłówków i stopek, m) zabezpieczenie plików hasłem (zarówno do odczytu jak i edycji), n) podgląd graficzny oraz wydruk dokumentów (z możliwością wydruku kilku slajdów na jednej stronie oraz notatkami), Narzędzie do zarządzania pocztą elektroniczną, kalendarzami i zadaniami: a) pełna obsługa plików w formacie.pst, b) obsługa poczty elektronicznej w oparciu o protokoły: SMTP/MIME, SMTPS, POP3, POP3S, IMAP, c) automatyczne filtrowanie poczty, d) edycja i formatowanie tekstu wiadomości, e) tworzenie i obsługa katalogów, f) tworzenie szablonów dokumentów, g) tworzenie automatycznych reguł zarządzających pocztą, h) oznaczanie wybranej poczty zdefiniowanymi atrybutami, i) importobsługawielukalendarzy(wtymkalendarzyzdalnychwformacieiCal), j) udostępnianie kalendarza innym użytkownikom, k) tworzenieizarządzaniezdarzeniami(zmożliwościąustawieniaprzypomnień), l) automatyczne wysyłanie i odbieranie informacji o spotkaniach, m) tworzenie i zarządzanie zadaniami, n) tworzenieizarządzanielistąkontaktową(wtymtworzeniagrupodbiorców), o) odbiór i wysyłanie elektronicznych wizytówek w formacie vCard, p) wbudowany słownik języka: polskiego, angielskiego oraz niemieckiego, q) podgląd graficzny oraz wydruk dokumentów.

		Inne Licencja dożywotnia na pakiet biurowy Zamawiający nie dopuszcza pakietów biurowych , których użytkowanie wymaga okresowego wykupywania licencji na użytkowanie, tzw. opłaty abonamentowe
18.	BIOS	BIOS zgodny ze specyfikacją UEFI - Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych informacji o: modelu komputera, PN, numerze seryjnym, Asset Tag, MAC Adres karty sieciowej, wersja Biosu wraz z datą produkcji, zainstalowanym procesorze, jego taktowaniu i ilości rdzeni, ilości pamięci RAM wraz z taktowaniem, stanie pracy wentylatora na procesorze, stanie pracy wentylatorów w obudowie komputera, napędach lub dyskach podłączonych do portów M.2 oraz SATA (model dysku twardego i napędu optycznego) Możliwość z poziomu Bios: wyłączenia/włączenia selektywnego (pojedynczo) portów USB zarówno z przodu jak i z tyłu obudowy; wyłączenia kontrolera selektywnego (pojedynczego) portów SATA; konfiguracji kontrolera SATA; wyłączenia karty sieciowej, karty audio, portu szeregowego, wbudowanego głośnika, PXE; możliwość ustawienia portów USB w jednym z dwóch trybów: 1. użytkownik może kopiować dane z urządzenia pamięci masowej podłączonego do pamięci USB na komputer ale nie może kopiować danych z komputera na urządzenia pamięci masowej podłączone do portu USB 2. użytkownik nie może kopiować danych z urządzenia pamięci masowej podłączonego do portu USB na komputer oraz nie może kopiować danych z komputera na urządzenia pamięci masowej ustawienia hasła: administratora, Power-On, HDD; blokady aktualizacji BIOS bez podania hasła administratora; wglądu w system zbierania logów (min. Informacja o update Bios, błędzie wentylatora na procesorze, wyczyszczeniu logów) z możliwością czyszczenia logów; alertowania zmiany konfiguracji sprzętowej komputera; wyboru trybu uruchomienia komputera po utracie zasilania (włącz, wyłącz, poprzedni stan); ustawienia trybu wyłączenia komputera w stan niskiego poboru energii; zdefiniowania trzech sekwencji botujących (podstawowa, WOL, po awarii); załadowania optymalnych ustawień BIOS, obsługa BIOS za pomocą klawiatury i myszy bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.
19.	Zintegrowany System Diagnostyczny	Wizualny system diagnostyczny producenta działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera umożliwiający na wykonanie diagnostyki następujących podzespołów: • wykonanie testu pamięci RAM • test dysku twardego • test monitora • test magistrali PCI-e • test portów USB • test płyty głównej Wizualna lub dźwiękowa sygnalizacja w przypadku błędów któregokolwiek z

		powyższych podzespołów komputera. Ponadto system powinien umożliwiać identyfikacje testowanej jednostki i jej komponentów w następującym zakresie: • PC: Producent, model • BIOS: Wersja oraz data wydania Bios • Procesor : Nazwa, taktowanie • Pamięć RAM : Ilość zainstalowanej pamięci RAM, producent oraz numer seryjny poszczególnych kości pamięci • Dysk twardy: model, numer seryjny, wersja firmware, pojemność, temperatura pracy • Monitor: producent, model, rozdzielczość System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera.
20.	Certyfikaty i standardy	- Certyfikat ISO9001:2000 dla producenta sprzętu – ENERGY STAR 6.1 - Deklaracja zgodności CE - Głośność jednostki mierzona z pozycji operatora z umiejscowieniem komputera na biurku w trybie IDLE 23 dB - dołączyć certyfikat lub dokument potwierdzający głośność jednostki - Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki
21.	Waga/rozmiary urządzenia	Waga urządzenia max. 7kg Suma wymiarów nie może przekraczać: 735mm
22.	Bezpieczeństwo i zdalne zarządzanie	- Złącze typu Kensington Lock umożliwiające zastosowanie zabezpieczenia fizycznego w postaci linki metalowej uniemożliwiającej również otwarcie obudowy - Dedykowane oczko na kłódkę umożliwiającą zastosowanie zabezpieczenia fizycznego przed otwarciem obudowy - Moduł TPM 2.0
23.	Oprogramowanie	Dedykowane oprogramowanie producenta sprzętu umożliwiające automatyczna weryfikacje i instalację sterowników oraz oprogramowania użytkowego producenta w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralna bazą sterowników i oprogramowania użytkowego producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika. Oprogramowanie musi być wyposażone w moduł rejestru zdarzeń, w którym znajdują się informacje o tym kiedy i jakie sterowniki zostały zainstalowane na danej maszynie. Oprogramowanie musi zapewniać również ustawienie automatycznego uaktualnienia wszystkich sterowników we wskazanym dniu miesiąca.
24.	Gwarancja	minimum 3 lata świadczona w miejscu użytkowania sprzętu (on-site) z gwarantowanym czasem reakcji w następnym dniu roboczym. Oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie

		zobowiązania związane z serwisem. Sprzęt musi być wyprodukowany nie wcześniej niż w II połowie 2017 roku.
25.	Wsparcie techniczne producenta	Dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej. Możliwość weryfikacji na stronie producenta konfiguracji fabrycznej zakupionego sprzętu. Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.
26.	Dodatkowe	Przewód Patchcord UTP kategorii 6A, RJ 45, długość 3 metry

1.2.2. Monitor – 10 sztuk

L.p.	Parametr	Charakterystyka (wymagania minimalne)
1.	Przekątna ekranu i wymiary aktywnego obszaru wyświetlania	21,5“ 476 mm x 268 mm
2.	zalecana rozdzielczość	1920 x 1080 (Full HD)
3.	Typowy pobór mocy / w trybie Power management	19 W / 0,5 W
4.	złącza	VGA, HDMI
5.	kontrast typowy	600 : 1
6.	kontrast ACR	10 000 000 : 1
7.	Jasność typowa	200 cd/m2
8.	wielkość plamki	0,248 mm
9.	Czas reakcji	5 ms
10.	Kąt widzenia przy CR>10	poziomo/pionowo: min. 90°/65°
11.	Regulacja cyfrowa OSD	TAK
12.	Certyfikaty i standardy	- CE, - EnergyStar 6.0 - TCO - EPEAT Silver Załączyć certyfikaty do oferty.
13.	Gwarancja	minimum 36 miesięcy

1.3. Zestawy- stanowiska komputerowe laptopy- 10 sztuk

Lp.	Parametr	Charakterystyka (wymagania minimalne)
1.	Komputer	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego notebooka.
2.	Ekran	Matryca TFT 15,6" z podświetleniem w technologii LED, powłoka antyrefleksyjna Anti-Glare - rozdzielczość: HD 1366x768, 220nits, kontrast 350:1; Kąt otwarcia matrycy min.180 stopni.
3.	Obudowa	Komputer wykonany z materiałów o podwyższonej odporności na uszkodzenia mechaniczne oraz przystosowana do pracy w trudnych warunkach termicznych, charakteryzujący się wzmocnioną konstrukcją, tzw. „business rugged", według normy Mil-Std-810G tj. taki, który zaliczył (co najmniej) następujące testy z wynikiem pozytywnym: - Uderzenia- Metoda 516.6; - Zmienna Temperatura- Metoda 503.5 - Wilgotność- Metoda 507.5 W celu potwierdzenia, że oferowana dostawa odpowiada wymaganiom określonym przez zamawiającego, należy przedstawić: Oświadczenie Wykonawcy potwierdzone oświadczeniem lub innym dokumentem pochodzącym od producenta, potwierdzające, że komputer spełnia standardy MIL-STD-810G, i pozytywnie przeszedł testy w zakresie minimum wyżej wymienionych. Komputer wyposażony w czujnik otwarcia obudowy zabezpieczający przed nieautoryzowanym dostępem. Praca czujnika konfigurowana z poziomu BIOS.
4.	Chipset	Dostosowany do zaoferowanego procesora
5.	Płyta główna	Zaprojektowana i wyprodukowana przez producenta komputera wyposażona w interfejsy SATA III (6 Gb/s), M.2 do obsługi dysków SATA lub WWAN.
6.	Procesor	Procesor klasy x86, 2 rdzeniowy, zaprojektowany do pracy w komputerach przenośnych, taktowany zegarem co najmniej 2,4 GHz, pamięcią cache L3 co najmniej 3 MB lub równoważny wydajnościowo osiągający wynik co najmniej 3800 pkt w teście SysMark w kategorii PassMark CPU Mark, według wyników opublikowanych na stronie http://www.cpubenchmark.net
7.	Pamięć operacyjna	Min 4GB z możliwością rozbudowy do 32GB, rodzaj pamięci DDR4, 2133MHz. Komputer wyposażony w minimum dwa banki pamięci umożliwiające pracę w trybie dual-channel.
8.	Dysk twardy	Min 256GB SSD M.2 NVMe zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii.
9.	Napęd optyczny	Wbudowana nagrywarka DVD

10.	Karta graficzna	Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki. Karta graficzną osiągająca min. 930 pkt w teście Videocard Benchmark (http://www.videocardbenchmark.net/)
11.	Audio/Video	Wbudowana, zgodna z HD Audio, wbudowane głośniki stereo min 2x 1.5W, wbudowane dwa mikrofony, sterowanie głośnością głośników za pośrednictwem wydzielonych klawiszy funkcyjnych na klawiaturze, wydzielony przycisk funkcyjny do natychmiastowego wyciszania głośników oraz mikrofonu (mute), kamera HD720p pracująca przy niskim oświetleniu.
12.	Karta sieciowa	10/100/1000 – RJ 45
13.	Porty/złącza	4xUSB 3.1 Gen 1 (jeden z możliwością ładowania urządzeń zewnętrznych poprzez port USB przy wyłączonym komputerze), złącze słuchawek i mikrofonu (combo), VGA, Mini Display Port, RJ-45, czytnik kart multimedialnych (min. SD/SDHC/SDXC/MMC), czytnik kart chipowych, dedykowane złącze dokowania umieszczone w spodniej części notebooka (nie dopuszcza się replikatora portów podłączanego poprzez port USB), Smart card reader. Złącze umożliwiające podpięcie linki antykradzieżowej.
14.	Dokowanie	Dedykowane złącze stacji dokującej dostępne od spodu notebooka, wyposażone w systemem chroniącym styki przed zanieczyszczeniem.
15.	Klawiatura	Klawiatura odporna na zalanie, układ US, z wbudowanym trackpointem, touchpad z obsługą gestów. Klawiatura posiada wydzieloną część numeryczną.
16.	WiFi	Wbudowana karta sieciowa, pracująca w standardzie AC 2x2
17.	Bluetooth	Wbudowany moduł Bluetooth 4.1
18.	Modem LTE	Możliwość rozbudowy notebooka o zintegrowany z obudową komputera modem LTE wraz ze slotem na kartę typu SIM (nie dopuszcza się modemów wykorzystujących Express card oraz USB port)
19.	Bateria	Notebook wyposażony baterie o pojemności min. 48 Wh - pozwalające na nieprzerwaną pracę urządzenia do 14 godziny – załączyć test Mobile Mark 2014 lub kartę katalogową oferowanego komputera potwierdzającą czas pracy na zasilaniu bateryjnym.
20.	Zasilacz	Zasilacz zewnętrzny maks. 45W
21.	System operacyjny	System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim

		4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.

		21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)." 24. Wbudowany mechanizm wirtualizacji typu hypervisor." 25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 34. Możliwość tworzenia wirtualnych kart inteligentnych. 35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38. Mechanizmy logowania w oparciu o: a. Login i hasło,

		b. Karty inteligentne i certyfikaty (smart card), c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN e. Certyfikat/Klucz i uwierzytelnienie biometryczne 39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń
22.	Oprogramowanie antywirusowe	1. Pełne wsparcie dla systemu zaproponowanego przez Wykonawcę w ofercie– LICENCJA NA OKRES MINIMUM 36 MIESIĘCY 2. Wersja programu dla stacji roboczych dostępna zarówno w języku polskim jak i angielskim. **Ochrona antywirusowa i antyspyware** 3. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 4. Wbudowana technologia do ochrony przed rootkitami. 5. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 6. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 7. System ma oferować administratorowi możliwość definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym i jeśli tak – nie wykonywało danego zadania. 8. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami 9. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu. 10. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu. 11. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu. 12. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera. 13. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.

		14. 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. 15. 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). 16. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. 17. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail. 18. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie. 19. 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. 20. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. 21. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 22. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe. 23. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta. 24. Program musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. 25. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym. 26. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego. 27. 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. 28. 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. 29. Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika. 30. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła. 31. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo. 32. 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. 33. Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów. 34. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku. 35. 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. 36. 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. 37. 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. 38. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. 39. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika. 40. Użytkownik ma posiadać możliwość takiej konfiguracji programu aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika 41. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS). 42. Oprogramowanie musi posiadać zaawansowany skaner pamięci. 43. Program musi być wyposażona w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp.

		44. 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. 45. 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. 46. 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. 47. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu. 48. Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji program zgłosi posiadanie nieaktualnej bazy sygnatur. 49. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji. 50. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http 51. Program musi być wyposażona w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (roll back). 52. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa). 53. 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. 54. Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli stron Internetowych i kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania. 55. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. 56. Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline. 57. W programie musi istnieć możliwość tymczasowego wstrzymania polityk wysłanych z poziomu serwera zdalnej administracji. 58. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej. 59. 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.

Ochrona przed spamem

60. Program ma umożliwiać uaktywnienie funkcji wyłączenia skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej.
61. Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego.
62. Możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną wiadomość i odwrotnie oraz ręcznego dodania wiadomości do białej i czarnej listy z wykorzystaniem funkcji programu zintegrowanych z programem pocztowym.
63. Możliwość definiowania swoich własnych folderów, gdzie program pocztowy będzie umieszczać spam.
64. Możliwość zdefiniowania dowolnego Tag-u dodawanego do tematu wiadomości zakwalifikowanej jako spam.
65. Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną zmieni jej właściwość jako „nieprzeczytana" oraz w momencie zaklasyfikowania wiadomości jako spam na automatyczne ustawienie jej właściwości jako „przeczytana".
66. Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.

Zapora osobista (personal firewall)

67. Zapora osobista ma pracować jednym z 4 trybów:
    - tryb automatyczny – program blokuje cały ruch przychodzący i zezwala tylko na znane, bezpieczne połączenia wychodzące, jednocześnie umożliwia utworzenie dodatkowych reguł przez administratora
    - tryb interaktywny – program pyta się o każde nowe nawiązywane połączenie i automatycznie tworzy dla niego regułę (na stałe lub tymczasowo),
    - tryb oparty na regułach – użytkownik/administrator musi ręcznie zdefiniować reguły określające jaki ruch jest blokowany a jaki przepuszczany,
    - tryb uczenia się – umożliwia zdefiniowanie przez administratora określonego okresu czasu w którym oprogramowanie samo tworzy odpowiednie reguły zapory analizując aktywność sieciową danej stacji.
68. Program musi akceptować istniejące reguły w zaporze systemu zaproponowanej przez Wykonawcę w ofercie, zezwalające na ruch przychodzący
69. Możliwość tworzenia list sieci zaufanych.
70. Możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie
71. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego.
72. Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer w tym minimum dla strefy zaufanej i sieci Internet.
73. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci

		oraz wykrywaniem aktywności wirusów sieciowych. 74. Program musi umożliwiać ochronę przed przyłączeniem komputera do sieci botnet. 75. Wykrywanie zmian w aplikacjach korzystających z sieci i monitorowanie o tym zdarzeniu. 76. Program ma oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6. 77. Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci. 78. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci 79. Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowaniu sieci bezprzewodowej lub jego braku, aktywności połączenia bezprzewodowego lub jego braku, konkretny interfejs sieciowy w systemie. 80. Program musi możliwość ustalenia tymczasowej czarnej listy adresów IP, które będą blokowane podczas próby połączenia. 81. Program musi posiadać kreator, który umożliwia rozwiązać problemy z połączeniem. **Kontrola dostępu do stron internetowych** 82. Aplikacja musi być wyposażona w zintegrowany moduł kontroli odwiedzanych stron internetowych. 83. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane zdefiniowane reguły. 84. Profile mają być automatycznie aktywowane w zależności od zalogowanego użytkownika. 85. Podstawowe kategorie w jakie aplikacja musi być wyposażona to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii. 86. Moduł musi posiadać także możliwość grupowania kategorii już istniejących. 87. Aplikacja musi posiadać możliwość określenia uprawnień dla dostępu do kategorii url – zezwól, zezwól i ostrzeż, blokuj. 88. Program musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania określonej w regułach witryny. **Ochrona serwera plików** 95. Wsparcie dla systemów zaproponowanych przez Wykonawcę w ofercie. 96. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 97. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware,

		dialer, phishing, narzędzi hakerskich, backdoor, itp. 98. Wbudowana technologia do ochrony przed rootkitami i exploitami. 99. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 100. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 101. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 102. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych. 103. Użytkownik ma mieć możliwość zmiany ilości wątków skanowania w ustawieniach systemu antywirusowego. 104. Możliwość skanowania dysków sieciowych i dysków przenośnych. 105. Skanowanie plików spakowanych i skompresowanych. 106. 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. 107. Aplikacja powinna wspierać mechanizm klastrowania. 108. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS). 109. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS. 110. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. 111. Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model i wersję modelu urządzenia. 112. 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. 113. Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. 114. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 115. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony. 116. Dodanie automatycznych wyłączeń nie wymaga restartu serwera. 117. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych. 118. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji. 119. W przypadku restartu serwera – usunięte z listy wyłączeń elementy mają być automatycznie uzupełnione. 120. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego.

		121. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line). 122. 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. 123. 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. 124. 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. 125. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. 126. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail. 127. 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. 128. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji ma być takie samo. 129. 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. 130. 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. 131. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym. 132. 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. 133. 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. 134. 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. 135. 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). 136. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy. 137. Aplikacja musi wspierać skanowanie magazynu Hyper-V 138. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów 139. 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). 140. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 141. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. **Administracja zdalna** 104. Serwer administracyjny musi oferować możliwość instalacji na systemach zaproponowanych przez Wykonawcę w ofercie. 105. Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance). 106. 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. 107. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej. 108. Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6. 109. Podczas logowania administrator musi mieć możliwość wyboru języka w jakim zostanie wyświetlony panel zarządzający. 110. Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL. 111. Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci. 112. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych. 113. Instalacja serwera administracyjnego powinna oferować wybór trybu pracy serwera w sieci w przypadku rozproszonych sieci –serwer pośredniczący (proxy) lub serwer centralny. 114. Serwer proxy musi pełnić funkcję pośrednika pomiędzy lokalizacjami zdalnymi a serwerem centralnym. 115. Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM. 116. 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. 117. Komunikacja pomiędzy poszczególnymi modułami serwera musi

		być zabezpieczona za pomocą certyfikatów. 118. Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy. 119. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci. 120. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta. 121. Agent musi posiadać możliwość pobrania listy zainstalowanego oprogramowania firm trzecich na stacji roboczej z możliwością jego odinstalowania. 122. Serwer administracyjny musi oferować możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie. 123. Instalacja klienta na urządzeniach mobilnych musi być dostępna za pośrednictwem portalu WWW udostępnionego przez moduł MDM z poziomu urządzenia użytkownika. 124. Administrator musi posiadać możliwość utworzenia listy zautoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji. 125. 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. 126. Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi. 127. Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp. 128. Administrator musi posiadać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli zarządzającej. 129. Dwu fazowa autoryzacja musi się odbywać za pomocą wiadomości SMS lub haseł jednorazowych generowanych na urządzeniu mobilnym za pomocą dedykowanej aplikacji. 130. Administrator musi posiadać możliwość nadania dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko do odczytu, odczyt/zapis. 131. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika. 132. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności po jakim użytkownik zostanie automatycznie wylogowany. 133. 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. 134. Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu

		dostępnego w Internecie lub zasobie lokalnym. 135. Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu. 136. Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką. 137. Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów. 138. 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. 139. 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. 140. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej. 141. 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. 142. Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania. 143. Serwer administracyjny musi oferować możliwość wyboru formy przedstawienia danych w raporcie w postaci tabeli, wykresu lub obu elementów jednocześnie. 144. Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym dostępnym z poziomu interfejsu konsoli WWW. 145. Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub PS. 146. Serwer administracyjny musi oferować możliwość maksymalizacji wybranego elementu monitorującego. 147. Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy. 148. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP. 149. Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu. 150. Serwer administracyjny musi oferować możliwość podłączenia serwera administracji zdalnej do portalu zarządzania licencjami dostępnego na serwerze producenta. 151. Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji. 152. Serwer administracyjny musi posiadać możliwość dodania dowolnej

		ilości licencji obejmujących różne produkty. 153. Serwer administracyjny musi być wyposażona w machizm auto dopasowania kolumn w zależności od rozdzielczości urządzenia na jakim jest wyświetlana. 154. Administrator musi mieć możliwość określenia zakresu czasu w jakim dane zadanie będzie wykonywane (sekundy, minuty, godziny, dni, tygodnie). 155. 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.
23.	Oprogramowanie biurowe	Pakiet biurowy musi zawierać co najmniej: a) Edytor tekstów, b) Arkusz kalkulacyjny, c) Narzędzie do przygotowania i prowadzenia prezentacji, d) Narządziedozarządzaniapocztąelektroniczną,kalendarzamiizadaniami Ogólne: a) Interfejs w języku polskim, b) wbudowana pomoc kontekstowa, c) możliwość instalacji na dostarczonym sprzęcie i systemie operacyjnym Edytor tekstów: a) konwersja, pełna edycja i zapis plików w formatach: txt, rtf, doc, docx, odt, xml (wraz z atrybutami), b) edycja i formatowanie tekstu (m.in. tabel, obiektów graficznych, wzorów matematycznych, osadzania wykresów z arkusza kalkulacyjnego), c) tworzenie szablonów dokumentów, d) wbudowany słownik języka: polskiego, angielskiego oraz niemieckiego, e) wbudowana biblioteka obiektów graficznych i symboli, f) wbudowany mechanizm automatycznego sprawdzania pisowni oraz poprawności gramatycznej w ww. językach, g) edycja nagłówków i stopek, h) automatyczne numerowanie rozdziałów, tabel i rysunków, i) automatyczne tworzenie spisu treści, przypisów i odnośników do tekstu, j) śledzenie wprowadzonych zmian, k) zabezpieczenie plików hasłem (zarówno do odczytu jak i edycji), l) tworzenie korespondencji seryjnej, m) tworzenie makr, n) podgląd graficzny oraz wydruk dokumentów Arkusz kalkulacyjny: a) konwersja, pełna edycja i zapis plików w formatach: txt, csv, xls, xlsx, xml (wraz z atrybutami), b) tworzenie arkuszy kalkulacyjnych obejmujących dane tekstowe, liczbowe, walutowe, procentowe, ułamkowe oraz czasowe, c) tworzenie formuł obejmujących operacje: tekstowe, matematyczne, logiczne, statystyczne oraz operacje na danych finansowych i czasowych, d) tworzenie formuł obejmujących: wyszukiwanie danych, operacje na tabelach,

		e) tworzenie i osadzania wykresów (m.in. punktowych, liniowych, kolumnowych, słupkowych, warstwowych, kołowych, 3D), f) formatowanie warunkowe komórek arkusza, g) śledzenie formuł oraz automatyczna weryfikacja ich poprawności, h) tworzenie tabel przestawnych, i) raporty z wykorzystaniem wyszukiwania warunkowego, j) automatyczne filtrowania danych, k) automatyczne pobieranie danych z zewnętrznych źródeł: plików tekstowych, plików XML, arkuszy kalkulacyjnych, baz danych, l) zapis wielu arkuszy w jednym pliku, m) tworzenie szablonów dokumentów, n) wbudowany słownik języka: polskiego, angielskiego oraz niemieckiego, o) tworzenie oraz edycji nagłówków i stopek, p) osadzanie:symboli,tabel,rysunków,obiektówgraficznychorazwzorówmatematycznych, q) zabezpieczenie plików hasłem (zarówno do odczytu jak i edycji), r) tworzenie korespondencji seryjnej, s) tworzenie makr, t) podgląd graficzny oraz wydruk dokumentów, Narzędzie do przygotowania i prowadzenia prezentacji: a) konwersja,pełnaedycjaizapisplikówwformatach:ppt,pptx,odp,xml(wrazzatrybutami), b) edycja i formatowanie tekstu (m.in. tabel, obiektów graficznych, wzorów matematycznych, osadzania wykresów z arkusza kalkulacyjnego), c) tworzenie szablonów prezentacji, d) tworzenie animacji dla pojedynczych elementów jak i całych slajdów, e) wbudowana biblioteka obiektów graficznych i symboli, f) elementy multimedialne (m.in. rysunków, obiektów graficznych, tabel, nagrań dźwiękowych oraz filmów), g) formatowanie tekstów, obiektów graficznych oraz tabel, h) umieszczanie notatek oraz podkładu dźwiękowego, i) wsparcie dla prowadzącego prezentacje (licznik czasu, obsługa projektora multimedialnego i konfiguracji i dwumonitorowej), j) wbudowany słownik języka: polskiego, angielskiego oraz niemieckiego, k) wbudowany mechanizm automatycznego sprawdzania pisowni oraz poprawności gramatycznej w ww. językach, l) tworzenie oraz edycji nagłówków i stopek, m) zabezpieczenie plików hasłem (zarówno do odczytu jak i edycji), n) podgląd graficzny oraz wydruk dokumentów (z możliwością wydruku kilku slajdów na jednej stronie oraz notatkami), Narzędzie do zarządzania pocztą elektroniczną, kalendarzami i zadaniami: a) pełna obsługa plików w formacie.pst, b) obsługa poczty elektronicznej w oparciu o protokoły: SMTP/MIME, SMTPS, POP3, POP3S, IMAP, c) automatyczne filtrowanie poczty, d) edycja i formatowanie tekstu wiadomości,

		e) tworzenie i obsługa katalogów, f) tworzenie szablonów dokumentów, g) tworzenie automatycznych reguł zarządzających pocztą, h) oznaczanie wybranej poczty zdefiniowanymi atrybutami, i) importiobsługawielukalendarzy(wtymkalendarzyzdalnychwformacieiCal), j) udostępnianie kalendarza innym użytkownikom, k) tworzenieizarządzaniezdarzeniami(zmożliwościąustawieniaprzypomnień), l) automatyczne wysyłanie i odbieranie informacji o spotkaniach, m) tworzenie i zarządzanie zadaniami, n) tworzenieizarządzanielistąkontaktową(wtymtworzeniagrupodbiorców), o) odbiór i wysyłanie elektronicznych wizytówek w formacie vCard, p) wbudowany słownik języka: polskiego, angielskiego oraz niemieckiego, q) podgląd graficzny oraz wydruk dokumentów. Inne Licencja dożywotnia na pakiet biurowy Zamawiający nie dopuszcza pakietów biurowych , których użytkowanie wymaga okresowego wykupywania licencji na użytkowanie, tzw. opłaty abonamentowe
24.	BIOS	BIOS zgodny ze specyfikacją UEFI. Możliwość odczytania z BIOS bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych następujących informacji: wersji BIOS wraz z datą; nr seryjnym komputera; ilości pamięciami RAM; typie procesora i jego prędkości; MAC adresu zintegrowanej karty sieciowej; unikalnych nr inwentarzowych tzw. Asset Tag'ów; nr seryjnym płyty głównej komputera Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności: - Możliwość Wyłączania/Włączania technologii antykradzieżowej - Możliwość autentykacji użytkownika w BIOS z wykorzystaniem czytnika linii papilarnych - Możliwość konfiguracji pracy czujnika otwarcia obudowy w taki sposób aby przy próbie otwarcia obudowy komputera i próbie jego uruchomienia pojawiał się monit o podanie hasła supervisor'a zapisanego w BIOS. - Możliwość ustawienia hasła dla twardego dysku - Możliwość ustawienia hasła na starcie komputera tzw. POWER-On Password - Możliwość ustawienia minimalnych wymagań dotyczących długości hasła POWER-On oraz hasła dysku twardego. - Możliwość włączania/wyłączania wirtualizacji z poziomu BIOSU - Możliwość ustawienia kolejności bootowania oraz wyłączenia poszczególnych urządzeń z listy startowej. - Możliwość Wyłączania/Włączania: zintegrowanej karty sieciowej, mikrofonu, zintegrowanej kamery, portów USB, Czytnika kart chipowych, bluetooth - Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych, ustawienia hasła na poziomie Administratora oraz możliwość ustawienia takiej zależności, że widok użytkownika pozwala na podgląd ustawień, ale nie ma możliwości wprowadzania zmian w BIOS.

		- Możliwość niezależnego włączenia/wyłączenia płytki dotykowej oraz track pointa Możliwość ustawienia konieczności podania hasła Administratora przy próbie aktualizacji BIOS
25.	Oprogramowanie dodatkowe	Oprogramowanie umożliwiające aktualizacje sterowników oraz podsystemu zabezpieczeń poprzez Internet. Oprogramowanie do wykonania kopii bezpieczeństwa systemu operacyjnego i danych użytkownika na dysku twardym, zewnętrznych dyskach, sieci, CD-ROM-ie oraz ich odtworzenie po ewentualnej awarii systemu operacyjnego bez potrzeby jego reinstalacji. Oprogramowanie w wersji polskiej lub angielskiej.
26.	Certyfikaty i standardy	- Certyfikat ISO9001:2000 dla producenta sprzętu - Certyfikat EPEAT na poziomie co najmniej GOLD. - ENERGY STAR 6.1 - Oferowane modele komputerów muszą posiadać certyfikat Microsoft, potwierdzający poprawną współpracę oferowanych modeli komputerów z ww. systemem operacyjnym (wydruk ze strony Microsoft WHCL) - Deklaracja zgodności CE - Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki
27.	Waga/Wymiary	Waga urządzenia z baterią podstawową max 2,5 kg, suma wymiarów urządzenia max 700 mm.
28.	Szyfrowanie i bezpieczeństwo	Komputer wyposażony w moduł TPM 2.0 Notebook wyposażony w czujnik otwarcia obudowy zabezpieczający przed nieautoryzowanym dostępem do notebooka. Czujnik musi sygnalizować próbę nieautoryzowanego dostępu do wnętrza komputera. Praca czujnika konfigurowana z poziomu BIOS w ten sposób, że przy ustawionym haśle SUPERVISOR w przypadku nieautoryzowanego otwarcia obudowy hasło to będzie wymagane do podania przy próbie uruchomienia notebooka. Zamawiający uzna za równoważne dostarczenie linki zabezpieczającej typu Kensington zamykanej w taki sposób, że nie będzie możliwe otwarcie obudowy notebooka gdy linka zabezpieczająca zostanie umieszczona i zamknięta z wykorzystaniem kluczyka w dedykowanym slocie Kensington
29.	Gwarancja	minimum 3 lata świadczona w miejscu użytkowania sprzętu (on-site) z gwarantowanym czasem reakcji w następnym dniu roboczym. Oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. Sprzęt musi być wyprodukowany nie wcześniej niż w II połowie 2017 roku.
30.	Wsparcie techniczne producenta	Dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej. Możliwość weryfikacji na stronie producenta konfiguracji fabrycznej zakupionego sprzętu. Możliwość weryfikacji na stronie producenta posiadanej/wykupionej gwarancji.

		Możliwość weryfikacji statusu naprawy urządzenia po podaniu unikalnego numeru seryjnego. Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.
31.	Dodatkowe	Przewód Patchcord UTP kategorii 6A, RJ 45, długość 3 metry

1.4. Drukarka laserowa- 60 sztuk

L.p.	Parametr	Charakterystyka (wymagania minimalne)	
1.	Drukowanie	Szybkość drukowania w A4	40 str./min w mono
		Czas pierwszego wydruku	Poniżej 4,5 sekund
		Rozdzielczość	1200 x 1200 dpi
		Języki druku	Emulacja PostScript3, PCL5e, PCL6 (XL), EPSON FX, IBM ProPrinter, XPS, PDF(v1.7)
		Czcionki drukarki	87 skalowanych czcionek PCL i 136 czcionek PostScript, 2 czcionki bitmapowe, OCR-A/B Czcionki rastrowe: Czcionki Epson FX i IBM PPR o różnych rozmiarach
		Dupleks	Automatyczny
2.	Interfejs i oprogramowanie	Złącza	Port USB 2.0, Ethernet 10/100/1000
		Kompatybilność z systemami operacyjnymi	Zaproponowanymi przez Wykonawcę w ofercie
		Dodatkowe oprogramowanie	Oprogramowanie producenta drukarki lub równoważne do monitorowania wykorzystania urządzenia oraz nakładania ograniczeń posiadające następujące funkcje: - funkcjonować w środowisku zaproponowanym przez Wykonawcę w ofercie; - obsługiwać zarówno drukarki sieciowe (czyli podłączone do sieci Ethernet poprzez wbudowaną w drukarkę wewnętrzną kartę sieciową) jak i drukarki podłączone lokalnie (przez port USB) - podawać nazwy użytkowników (np. ich loginy) drukujących poszczególne wydruki; - podawać nazwy drukowanych plików, liczbę stron, datę i godzinę przeprowadzenia danego wydruku; - możliwość wpisania kosztów materiałów eksploatacyjnych, oraz kosztu użycia zwykłej kartki, folii i nalepek; - podawać koszt przeprowadzonego wydruku z możliwością rozróżnienia wydruków o małym i dużym pokryciu (wymagane jest rozróżnianie przynajmniej 5 różnych poziomów pokrycia, i przyznawanie im

			odpowiednich kosztów); - możliwość nakładania ograniczeń ilościowych na liczbę drukowanych stron oraz na koszty wydruku, w ujęciu dziennym, tygodniowym i miesięcznym.
3.	Podawanie papieru	Pojemność papieru	Podajnik 1: 250 arkuszy 80 g/m2; Podajnik uniwersalny: 100 arkuszy 80 g/m2; Możliwość instalacji dodatkowego podajnika papieru o pojemności 530 arkuszy 80g/m2 Maksymalna pojemność podajników: 880 arkuszy 80/m2
		Format papieru	Podajnik 1: A4, A5, B5(JIS), A6, Letter, Legal 13, Legal 14, Executive, Statement; Podajnik 2: A4, A5, B5(JIS), Letter, Legal 13, Legal 14, Executive; Podajnik wielofunkcyjny: A4, A5, B5(JIS), A6, Letter, Legal 13, Legal 14, Executive, Statement, Koperty: Monarch, Com-9, Com-10, DL, C5, C6, 4 x 6”, 5 x 7”; Druk dwustronny: A4, B5(JIS), Letter, up to Legal 14, Executive
		Gramatura papieru	Podajnik 1/2: Od 60 do 120 g/m2; Podajnik uniwersalny: Od 60 do 163 g/m2; Druk dwustronny: Od 60 do 120 g/m2 Podajnik uniwersalny: 60 – 163 g/m2
		Odbiornik papieru	Do 150 arkuszy stroną zadrukowaną do dołu Do 100 arkuszy stroną zadrukowaną do góry
4.	Pozostałe parametry techniczne:	Pamięć	Standardowa pamięć: 512 MB RAM, 3.0GB eMMC
		Obciążenie	Maksymalne obciążenie do 80 000 stron miesięcznie
5.	Wymaganie dodatkowe:	Gwarancja	minimum 3 lata gwarancji producenta drukarki
		Wymagane dokumenty::	Certyfikat ISO 9001:2008 dla producenta oferowanego sprzętu. Certyfikat ISO 140001:2004 dla producenta oferowanego sprzętu.
		Materiały eksploatacyjne:	Wymagana rozdzielność bębna i tonera.
		Wydajność materiałów eksploatacyjnych	Urządzenie dostarczone z tonerem o wydajności 2000 str. zgodnie z ISO/ISC 19752. Urządzenie powinno mieć możliwość zastosowania tonerów o wydajności: 3 000 , 7 000 oraz 12000 stron zgodnie z ISO/ISC 19752.
		Inne	Przewód USB o długości 1,8 metra do podłączenia urządzenia z komputerem

1.5. Urządzenie wielofunkcyjne A4 monochromatyczne (drukarka, skaner, kopiarka, fax) - 10 sztuk

L.p.	Parametr	Charakterystyka (wymagania minimalne)
1.	Drukowanie	Szybkość drukowania- 33 str./min Szybkość druku dwustronnego- 18 str/min Czas pierwszego wydruku- 6,5 sekund Rozdzielczość- 1200 x 1200 dpi Języki druku- PCL5e, PCL6, IBM-PPR, Epxon-FX,XPS Zespół drukowania- Dupleks mechaniczny
2.	Skanowanie	Rozdzielczość skanowania- 600 x 600 dpi Szybkość skanowania- Do 6 s/stronę w kolorze, 2s/stronę w czerni Głębia kolorów- Wejście 48 bit/Wyjście 24 bit Podawanie dokumentów- Automatyczny podajnik dokumentów wraz z duplexem na 50 arkuszy, skaner płaski Format- M-TIFF, PDF, XPS, JPEG, GIF, PNG Książka adresowa- LDAP, 300 adresów e-mail, 20 grup adresowych Skanowanie do- FTP, HTTP, E-mail, TWAIN, CIFS, pamięci USB,
3.	Kopiowanie	Czas wykonania pierwszej kopii- 10 sekund Szybkość kopiowania- do 33 kopii/min Rozdzielczość kopiowania- do 600 x 600dpi Zmniejszanie/powiększanie- Zoom 25-400% Maksymalna liczba kopii- 99
4.	Faksowanie	Złącza- RJ11 x 2 (Line/Tel), PSTN, Linia PBX Szybkość- ITU-T G3(Super G3) do 33,6kbps, do 2 s/str. Szybkie wybieranie- 16 przycisków szybkiego wybierania, 300 numerów Lista rozgłaszania- Maksimum 100 Pamięć stron- 4MB
5.	Interfejs i oprogramowanie	Złącza- Port USB 2.0, Ethernet 10/100/1000BaseTX Komunikacja bezprzewodowa- Tak, moduł bezprzewodowej karty sieciowej wbudowanej w urządzenie. Kompatybilność z systemami operacyjnymi zaproponowanymi przez Wykonawcę w ofercie. Dodatkowe oprogramowanie- Oprogramowanie producenta drukarki lub równoważne do monitorowania wykorzystania urządzenia oraz nakładania ograniczeń posiadające następujące funkcje: - funkcjonować w środowisku zaproponowanym przez Wykonawcę w ofercie; - obsługiwać zarówno drukarki sieciowe (czyli podłączone do sieci Ethernet poprzez wbudowaną w drukarkę wewnętrzną kartę sieciową) jak i drukarki podłączone lokalnie (przez port USB i/lub LPT) - podawać nazwy użytkowników (np. ich loginy) drukujących poszczególne wydruki; - podawać nazwy drukowanych plików, liczbę stron, datę i godzinę przeprowadzenia danego wydruku; - możliwość wpisania kosztów materiałów eksploatacyjnych, oraz kosztu użycia zwykłej kartki, folii i nalepek; - podawać koszt przeprowadzonego wydruku z możliwością rozróżnienia wydruków o małym i dużym pokryciu (wymagane jest rozróżnianie

		przynajmniej 5 różnych poziomów pokrycia, i przyznawanie im odpowiednich kosztów); - możliwość nakładania ograniczeń ilościowych na liczbę drukowanych stron oraz na koszty wydruku, w ujęciu dziennym, tygodniowym i miesięcznym.
6.	Podawanie papieru	Pojemność papieru- Podajnik 1: 250 arkuszy 80 g/m2; Podajnik uniwersalny: 100 arkuszy 80 g/m2; Możliwość instalacji dodatkowego podajnika papieru o pojemności 530 arkuszy 80g/m2 Format papieru- Podajnik 1: A4, A5, B5, A6 Podajnik uniwersalny: A4, A5, B5, A6, Monarch, Com-9, Com-10, DL, C5, C6, Druk dwustronny: A4, B5 Gramatura papieru- Podajnik 1: 60 – 120 g/m2; Druk dwustronny: 60 – 120 g/m2; Podajnik uniwersalny: 60 – 120 g/m2 Podajnik skanera: 60 – 105 g/m2 Odbiornik papieru- Do 150 arkuszy stroną zadrukowaną do dołu
7.	Pozostałe parametry techniczne:	Pamięć (RAM)- Standardowa pamięć RAM: 512 MB Obciążenie- Maksymalne obciążenie do 60 000 stron miesięcznie
8.	Wymaganie dodatkowe:	Gwarancja- minimum 3 lata gwarancji drukarki Oświadczenie producenta sprzętu, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. Certyfikat ISO 9001:2008 producenta oferowanego sprzętu, Certyfikat ISO 140001:2004 producenta oferowanego sprzętu, Materiały eksploatacyjne- Wymagana rozdzielność bębna i tonera. Toner startowy na 2 tys. stron zgodnie z normą ISO/ISC 19752 Urządzenie dostarczone musi być fabrycznie nowe, skonfigurowane, gotowe do pracy wraz z tonerem(-ami) umożliwiającym wydruk przynajmniej 7 000 stron A4 przy pokryciu zgodnie z normą ISO/ISC 19752. Toner musi być tego samego producenta co drukarka, nie mogą być regenerowane.
9.	Inne	Przewód USB o długości 1,8 metra do podłączenia urządzenia z komputerem

1.6. Urządzenie wielofunkcyjne A4 kolorowe (drukarka, skaner, kopiarka, fax)- 10 sztuk

L.p.	Parametr	Charakterystyka (wymagania minimalne)
1.	Drukowanie	Szybkość drukowania w A4- 26 str./min w kolorze, 30 str./min w mono Czas pierwszego wydruku- 9 sekund Rozdzielczość- 1200 x 600 dpi Czcionki druku- 87 skalowanych czcionek PCL i 80 czcionek PostScript Języki druku- PCL5c, PCL6, PostScript 3 (emulacja), IBM-PPR, Epxon-FX, XPS Zespół drukowania- Dupleks mechaniczny
2.	Skanowanie	Rozdzielczość skanowania- 60 x 600 dpi Szybkość skanowania- Do 26 str./min kolor, do 30 str./min w czerni Głębia kolorów- Wejście 30 bit/Wyjście 24 bit Podawanie dokumentów- Automatyczny podajnik dokumentów wraz z

		duplexem na 50 arkuszy, skaner płaski Format- M-TIFF, PDF, XPS, JPEG, Książka adresowa- LDAP lub 200 adresów e-mail i 20 grup adresowych Skanowanie do- FTP, HTTP, E-mail, TWAIN, CIFS, pamięci USB
3.	Kopiowanie	Czas wykonania pierwszej kopii- 14 sekund Szybkość kopiowania- Do 26 str./min kolor, do 30 str./min w czerni Rozdzielczość kopiowania- do 600 x 600dpi Zmniejszanie/powiększanie- Zoom 25-400% Maksymalna liczba kopii- 99
4.	Faksowanie	Złącza- RJ11 x 2 (Line/Tel), PSTN, Linia PBX Szybkość- ITU-T G3(Super G3) do 33,6kbps, do 3 s/str. Szybkie wybieranie- 16 przycisków szybkiego wybierania, 100 numerów Lista rozgłaszania- Maksimum 100 Pamięć stron- 250 MB
5.	Interfejs i oprogramowanie	Złącza- Port USB 2.0, Ethernet 10/100/1000BaseTX Kompatybilność z systemami operacyjnymi zaproponowanymi przez Wykonawcę w ofercie; Dodatkowe oprogramowanie- Oprogramowanie producenta drukarki lub równoważne do monitorowania wykorzystania urządzenia oraz nakładania ograniczeń posiadające następujące funkcje: - wymaga się aby aplikacja pracowała w środowisku zaproponowanym przez Wykonawcę w ofercie; - aplikacja powinna obsługiwać zarówno drukarki sieciowe (czyli podłączone do sieci Ethernet poprzez wbudowaną w drukarkę wewnętrzną kartę sieciową) jak i drukarki podłączone lokalnie (przez port USB i/lub LPT), - aplikacja powinna rejestrować nazwy użytkowników (np. ich loginy) drukujących poszczególne wydruki; - aplikacja powinna rejestrować i w ramach raportów podawać nazwy drukowanych plików, liczbę stron, datę i godzinę przeprowadzenia danego wydruku; -aplikacja w zakresie modułu administracyjnego powinna pozwolić na indywidualne określenie kosztów materiałów eksploatacyjnych, oraz kosztu użycia zwykłej kartki, folii i innych nośników dla poszczególnych urządzeń lub grup urządzeń; - aplikacja powinna w zakresie funkcji raportowych podawać koszt zrealizowanego wydruku z możliwością rozróżnienia wydruków o małym i dużym pokryciu (wymagane jest rozróżnianie przynajmniej 5 różnych poziomów pokrycia); - w przypadku współpracy z urządzeniami kolorowymi w ramach funkcji ograniczenia dostępu aplikacja powinna mieć możliwość blokowania druku kolorowego (a w przypadku urządzeń wielofunkcyjnych kopii kolor) - aplikacja lub dostarczone urządzenia powinny mieć możliwość automatycznej konwersji drukowanych plików na postać czarno-biała dla użytkowników z założoną blokadą druku w kolorze; - aplikacja powinna umożliwić nałożenie ograniczeń ilościowych na liczbę drukowanych stron w ujęciu dziennym, tygodniowym lub miesięcznym.
6.	Podawanie papieru	Pojemność papieru- Podajnik 1: 250 arkuszy 80 g/m2;

		Podajnik uniwersalny: 100 arkuszy 80 g/m2; Podajnik skanera: 50 arkuszy 80 g/m2; Możliwość instalacji dodatkowego podajnika papieru o pojemności 530 arkuszy 80g/m2 Format papieru- Podajnik 1: A4, A5, B5, A6 Podajnik uniwersalny: A4, A5, B5, A6, Monarch, Com-9, Com-10, DL, C5, nośniki (baner) do 130 cm długości Druk dwustronny: A4, B5, A5 Gramatura papieru- Podajnik 1: 64 – 176 g/m2; Druk dwustronny: 64 – 176 g/m2; Podajnik uniwersalny: 64 – 220 g/m2 Podajnik skanera: 60 – 105 g/m2 Odbiornik papieru- Do 150 arkuszy stroną zadrukowaną do dołu D0 100 arkuszy stroną zadrukowaną do góry
7.	Pozostałe parametry techniczne:	Pamięć (RAM)- Standardowa pamięć RAM: 1GB Szybkość procesora- 660 MHz Obciążenie- Maksymalne obciążenie do 45 000 stron miesięcznie
8.	Wymaganie dodatkowe:	Gwarancja- minimum 3 lata gwarancji drukarki Wymagane dokumenty: Oświadczenie producenta sprzętu, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. Certyfikat ISO 9001:2008 producenta oferowanego sprzętu Certyfikat ISO 14001:2004 producenta oferowanego sprzętu Materiały eksploatacyjne- Wymagana rozdzielność bębna i tonera. Tonery startowe na 1 tys. stron (toner czarny i tonery kolorowe) zgodnie z normą ISO/ISC 19752 oraz normą ISO/IEC 19798. Urządzenie dostarczone musi być fabrycznie nowe, skonfigurowane, gotowe do pracy wraz z tonerem(-ami).
9.	Inne	Przewód USB o długości 1,8 metra do podłączenia urządzenia z komputerem

1.7. Urządzenie wielofunkcyjne A3 monochromatyczne- 6 sztuk

L.p.	Parametr	Charakterystyka (wymagania minimalne)
1.	Typ	Nabiurkowa lub wolnostojąca (połączony tryb czytniko-kopiarki)
2.	Maksymalny rozmiar oryginału	A3
3.	Rozmiary kopii	Kaseta 1, 3 i 4: A3, A4, A4R, A5R Format niestandardowy: 139,7–297 mm x 182–432 mm Kaseta 2: A3, A4, A4R, A5R, koperta (z opcjonalnym podajnikiem kopert D1) Podajnik ręczny: A3, A4, A4R, A5R, koperty Format niestandardowy: 99–297 mm x 148–432 mm
4.	Rozdzielczość	Odczyt: 600 × 600 dpi Kopiowanie: 600 × 600 dpi

		Drukowanie: 600 × 600 dpi, 1200 x 1200 dpi (tylko sterownik UFRII-LT) Liczba tonów: 256 odcieni
5.	Prędkość Kopii/Druku	A4: 20 str. na minutę (tryb czarno-biały) A3: 15 str. na minutę (tryb czarno-biały)
6.	Powiększanie	Powiększenie: 25–400% Stałe: 25%, 50%, 70%, 100%, 141%, 200%, 400%
7.	Czas pierwszej kopii	Tryb czarno-biały: 6,4 s
8.	Czas rozgrzewania	30 s
9.	Wielokrotne kopie/wydruki	1–999
10.	Duplikowanie	Standard
11.	Wagi papieru	Kaseta: 64–90 g/m² Podajnik ręczny: 64–128 g/m² Druk dwustronny: 64–80 g/m²
12.	Pojemność papieru	Kaseta 1: 250 arkuszy (80 g/m²), Podajnik ręczny: 100 arkuszy (A4, A4R, A5; 80 g/m²), 50 arkuszy (A3; 80 g/m²) Opcjonalnie: 550 arkuszy x 2 kasety (80 g/m²) Całkowita pojemność: 2000 arkuszy
13.	Procesor	400 MHz
14.	Pamięć	256 MB
15.	Interfejs	Ethernet (100Base-TX/10Base-T), 1 port USB Host I/F 2.0, 1 port USB Device 1.0
16.	Źródło zasilania	220–240 V (prąd zmienny), 50/60 Hz, 3,3 A
17.	Wymiary	Suma wymiarów nie może przekraczać: 193 cm (z pokrywą szyby) Suma wymiarów nie może przekraczać: 203 cm (z podajnikiem DADF)
18.	Waga	Maksymalnie 52 kg
19.	Gwarancja	minimum 36 miesięcy
20.	Inne	Przewód USB o długości 1,8 metra do podłączenia urządzenia z komputerem
21.	Oprogramowanie	Kompatybilność z systemami operacyjnymi zaproponowanymi przez Wykonawcę w ofercie; Oprogramowanie producenta drukarki lub równoważne do monitorowania wykorzystania urządzenia oraz nakładania ograniczeń posiadające następujące funkcje: - wymaga się aby aplikacja pracowała w środowisku zaproponowanym przez Wykonawcę w ofercie; - aplikacja powinna obsługiwać zarówno drukarki sieciowe (czyli podłączone do sieci Ethernet poprzez wbudowaną w drukarkę wewnętrzną kartę sieciową) jak i drukarki podłączone lokalnie (przez port USB i/lub LPT),
22.	Materiały eksploatacyjne	Toner startowy na 2 tys. stron zgodnie z normą ISO/ISC 19752 Urządzenie dostarczone musi być fabrycznie nowe, skonfigurowane, gotowe do pracy wraz z tonerem(-ami).

1.8. Tablet- 11 sztuk

L.p.	Parametr	Charakterystyka (wymagania minimalne)
1.	Ekran	• Dotykowy • Rozdzielczość natywna nie mniejsza niż 1280x800 pikseli • Przekątna ekranu od 9 do 11 cali • Jasność co najmniej 600 nitów
2.	Procesor	Co najmniej 2 rdzenie, 1,5 Ghz
3.	Obudowa	• Posiadająca normę szczelności co najmniej IP67 • Powłoka dezynfekowana roztworem z zawartością alkoholu • Wytrzymująca upadek z min. 1,2 m
4.	Układ graficzny	Zintegrowany
5.	Pamięć RAM	Co najmniej 1GB
6.	Pamięć wewnętrzna	• Co najmniej 16GB • Możliwość rozszerzenia pamięci kartą typu MicroSD SDHC
7.	Bateria	Bateria typu „hot-swap” umożliwiająca wymianę baterii bez przerywania pracy urządzenia
8.	Czas pracy na baterii	Co najmniej 8h
9.	Temperatura pracy	Co najmniej -10 do nie więcej niż +50°C
10.	Komunikacja	• Wireless 802.11 a/b/g/n • Bluetooth 4.0 • GPS • 3G • Wbudowany czytnik kart HF RFID/NFC
11.	Czytnik kodów kreskowych	Wbudowany w urządzenie czytnik kodów kreskowych 1D i 2D
12.	Złącza	• Port ładowania i/lub multimedialny • USB i microUSB • Mini Jack 3.5mm
13.	System operacyjny	Zapewniający odpowiednią funkcjonalność dla systemu dostarczonego przez Wykonawcę
14.	Kamera	• Przednia co najmniej 1.2Mp • Tylna co najmniej 5.0Mp z auto-fokusem
15.	Inne	• Gwarancja co najmniej 36-m-ce • Mikrofon, głośniki • Waga nie większa niż 970g • Urządzenie musi być zakupione w oficjalnym, polskim kanale dystrybucyjnym

1.9. Drukarka kodów paskowych- 5 sztuk

L.p.	Parametr	Charakterystyka (wymagania minimalne)
1.	Rodzaj druku	Drukarka termiczna
2.	Rozdzielczość druku [dpi]	300dpi (12 pkt)
3.	Maksymalna długość	550 mm

	druku	
4.	Minimalna długość druku	77 mm
5.	Prędkość druku [mm/s]	51 mm/sek
6.	Szerokość druku [mm]	19,05 mm, 25,4 mm, 30,16 mm
7.	Ilość pamięci FLASH	8 MB
8.	Ilość pamięci RAM	16 MB
9.	Dostępne interfejsy	USB oraz szeregowy
10.	Parametry środowiskowe	- Temperatura użytkowa: -40° do 60°C - Temperatura przechowywania: 0° do 21°C przy wilgotności względnej 35% do 50%
11.	Parametry elektryczne	Uniwersalny zasilacz (zgodny z PFC) 100–240 V (AC), 50–60 Hz
12.	Wydruk kodów kreskowych	Kody liniowe: Codabar, Code 11, Code 39, Code 93, Code 128, EAN-8, EAN-13, EAN-14, GS1 DataBar™ (dawniej RSS), Industrial 2-of-5, Interleaved 2-of-5, Logmars, MSI, Plessey, Postnet, Standard 2-of-5, UPC-A, UPC-E, UPC-A i UPC-E z rozszerzeniami EAN 2- lub 5-cyfrowymi Dwuwymiarowe: Aztec Code, Codablock, Code 49, Data Matrix, MaxiCode, MicroPDF417, PDF417, QR Code
13.	Normy	Emisje: FCC część 15, punkt B, VCCI, C-Tick • Emisje i odporność: (CE): EN 55022 klasa B i EN 55024 • Bezpieczeństwo: CB Scheme IEC 60950-1:2001, TÜV NRTL • Zasilanie: IEC 60601-1:1995
14.	Nośnik	opaski na rękę posiadają powłokę antybakteryjną ze srebrem - białe
15.	Zestaw rozruchowy	opaski dla dorosłych - 25 mm x 279 mm x 6 szt, opaski: dla dzieci - 25 mm x 178 mm. x 2szt, dla noworodków - 19 mm x 195 mm x 2szt
16.	Gwarancja	minimum 36 miesiące

1.10. Skaner dowodów osobistych- 5 sztuk

L.p.	**Parametr**	**Charakterystyka (wymagania minimalne)**
1.	Sensor CCD	24 bit/pixels-RGB, 8 bit/pixels (podczerwień) 450DPI
2.	Odczyt	Strefy MRZ z dowodu osobistego i paszportu Strefy VIZ z dowodu osobistego, prawo jazdy oraz karty studenckiej Kodów kreskowych: 1D- UPC-A, EAN8, EAN13, Code39, Code128, Interleaved 2 of 5 2D- PDF 417, Data Matrix, QR Code, Aztec Code ICAO 9303
3.	SDK	C/C++, C#, Visual Basic 6.0, VB.NET, Delphi Java
4.	Obsługiwane systemy operacyjne	Kompatybilne z zaproponowanymi przez Wykonawcę w ofercie.
5.	Budowa	Brak części ruchomych
6.	Okno skanowania	4 mm szkło hartowane
7.	Interfejs	USB z odłączanym kablem komunikacyjnym
8.	Zabezpieczenia	Gniazdo Kensington
9.	Wymiary	Suma wymiarów nie może przekraczać (mm): 350
10.	Zasilanie	Poprzez port USB
11.	Sygnalizacja	Wizualna- 3 programowalne diody LED
12.	Gwarancja	minimum 36 miesiące

1.11. Videorejestracja do modułu e-tłumacz migowy – 1 sztuka

L.p.	Parametr	Charakterystyka (wymagania minimalne)
1.	Kamera	Przetwornik CMOS,720p HD
2.	Przetwornik Mpix	4 Mpix
3.	Rozdzielczość	1280x800 , 30 klatek/sek.
4.	Zoom cyfrowy	4 – krotny
5.	Mikrofon	Mono wbudowany
6.	Złącze	USB 2.0
7.	Format	16:9 - panoramiczny
8.	Technologie	TrueColor, automatyczna korekta obrazu barwy I koloru dla zmiennego oświetlenia, plug&play , oprogramowanie do nagrywania I odtwarzania materiału wideo, Ekranowanie magnetyczne
9.	Wsparcie dla Systemów	Kompatybilność dla systemów operacyjnych zaproponowanych przez Wykonawcę w ofercie.
10.	Głośniki	Stereo - 2 szt.
11.	Pasmo przenoszenia	50-17000 Hz
12.	Moc	większa od 8 W (RMS) na głośnik
13.	Gwarancja	minimum 36 miesiące

1.12. Karty Chipowe - 350 sztuk

L.p.	Parametr	Charakterystyka (wymagania minimalne)
1.	Typ karty	Intelligentna chipowa , pojemność 256-Byte EEPROM
2.	Zabezpieczenie	Zabezpieczenie przed zapisem, programowany cod bezpieczeństwa (PSC) zabezpieczenie przed zapisem pierwszych 32 adresów (bajt 0 ... 31) pamięci danych
3.	Oranizacja pamięci	256 x8bit EEPROM, 32X1bit pamięć bezpiecznika
4.	Waga	Max. 70g
5.	Temperatura pracy	-40 / + 80 ° C dla chipa, -25 / + 80 ° C dla modułu
6.	Zasilanie	Napięcie zasilania 5 V+-10%
7.	Prąd zasilania	Max 3 mA (typowy 600 µA)
8.	Czas wymazywania / zapisu EEPROM	Max . <5 ms
9.	Ochrona ESD typowa	Min 4.000 V
10.	EEPROM Trwałość minimum wymazywania / zapisu	100 000 cykli wymazywania / zapisu
11.	Gwarancja	Minimum 36 miesęcy

1.13. Skaner kodów kreskowych- 45 sztuk

L.p.	Parametr	Charakterystyka (wymagania minimalne)
1.	Obsługiwane kody kreskowe	1D
2.	Dostępne interfejsy	USB, PS/2, RS-232
3.	Kabel komunikacyjny	USB
4.	Maksymalna odległość odczytu (cm)	43
5.	Technologia odczytu	Laser jednoliniowy
6.	Temperature pracy	Od 0°C do 50°C
7.	Bezpieczny upadek na twardą powierzchnię (m)	1,5
8.	Sygnalizacja	Dźwiękowa oraz świetlna
9.	Wymagany kontrast kodu (%)	20
10.	Wymiary (cm)	Suma wymiarów nie może przekraczać 30 cm
11.	Temperatura składowania	Od -40°C do 70°C
12.	Dopuszczalna wilgotność otoczenia (%)	Od 5% do 95%
13.	Norma odporności (IP)	IP30
14.	Gwarancja	minimum 36 miesiące