|  |  |  |
| --- | --- | --- |
| ***Wymagane parametry techniczne zamawianych zestawów komputerowych*** | | ***Parametry techniczne oferowanych zestawów komputerowych\**** |
| **Wymagania minimalne** | | |
| **Zestaw komputerowy** | | |
| **Typ** | Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta. |  |
| Zastosowanie | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych. | |
| Procesor - wydajność | Procesor wielordzeniowy ze zintegrowaną grafiką, osiągający w teście PassMark CPU Mark wynik min. 11.900 punktów, wynik dostępny na stronie: [https://www.cpubenchmark.net](https://www.cpubenchmark.net/) |  |
| Pamięć operacyjna RAM | 8GB DDR4 2666MHz non-ECC możliwość rozbudowy do min 32GB, jeden slot wolny |  |
| Parametry pamięci masowej | 3.5” 1 TB SATA 7200 |  |
| Karta graficzna | Oferowana karta graficzna musi osiągać w teście PassMark Performance Test co najmniej wynik 1050 punktów w G3D Rating, wynik dostępny na stronie: <http://www.videocardbenchmark.net/gpu_list.php> |  |
| Połączenie sieciowe | Dwuzakresowa IEEE 802.11, 10/100/1000 Base T, Bluetooth |  |
| Interfejsy | 6 x USB, w tym min.: 2 x USB 3.0 na przednim panelu |  |
| 1 x RJ45 LAN |  |
| 1 x HDMI lub Display Port |  |
| 1 x VGA |  |
| 1 x połączone gniazdo wyjścia słuchawkowego i wejścia mikrofonowego |  |
| wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp. |  |
| Napęd optyczny | DVD-+RW - w dedykowanej wnęce zewnętrznej slim |  |
| Zasilacz | Zasilacz o mocy min. 200W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100%.  Zasilacz w oferowanym komputerze musi się znajdować na stronie <http://www.plugloadsolutions.com/80pluspowersupplies.aspx>, do oferty należy dołączyć wydruk potwierdzający spełnienie wymogu 80plus, w przypadku, kiedy u producenta występuje kilka zasilaczy które są montowane na etapie produkcji w fabryce załączyć wydruki dla wszystkich zasilaczy.  Wydruki 80plus muszą być potwierdzone przez producenta lub dołączone oświadczenie producenta komputera, iż wskazane zasilacze przez wykonawcę spełniają 80plus. |  |
| Zabezpieczenia | Ukryty w laminacie płyty głównej układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu szybkiego menu boot umożliwiający jednoczesne przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. System oparty o funkcjonalności: testy uruchamiane automatycznie lub w trybie interaktywnym, możliwość powtórzenia testów, uruchamianie gruntownych testów, uruchamianie szybkich testów lub pojedynczego testu dla konkretnego podzespołu. Uruchamianie testów zdefiniowanych przez użytkownika, wyświetlanie wiadomości, które informują o stanie przeprowadzanych testów, wyświetlanie wiadomości o błędach, które informują o problemach napotkanych podczas testów. Test musi zawierać informację o nazwie komputera, wersji BIOS, numerze seryjnym komputera, podawać dokładne informacje o wszystkich zainstalowanych komponentach, a w szczególności zawierać informacje o numerze seryjnym, typie i pojemności dysku twardego, informacji o obrotach wentylatora CPU, informacji o procesorze w tym model i taktowanie, informacji o pamięci w tym wielkość podana w MB, obsadzenie w konkretnym banku, wykaz temperatur CPU, pamięci, temperatury panującej wewnątrz. System działający nawet w przypadku braku dysku twardego lub w przypadku jego uszkodzenia, pozwalający na uzyskanie wyżej wymienionych funkcjonalności, a w szczególności na przetestowanie: procesora i pamięci. |  |
| Rodzaj obudowy | Mini/Micro Tower lub SFF: z obsługą kart PCI Express wyposażona w min. 1 wnękę wewnętrznie umożliwiającą montaż dysku 3,5” lub 2 dysków 2,5”. Napęd optyczny w dedykowanej wnęce zewnętrznej slim. Obudowa fabrycznie przystosowana do pracy w orientacji poziomej i pionowej.  Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej oraz kłódki (oczko w obudowie do założenia kłódki).  Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie oraz musi być wpisany na stałe w BIOS. |  |
| Zgodność z systemami operacyjnymi | Oferowane modele komputerów muszą poprawnie współpracować z zamawianymi systemami operacyjnymi (jako potwierdzenie poprawnej współpracy Wykonawca dołączy do oferty dokument w postaci wydruku potwierdzający certyfikację rodziny produktów bez względu na rodzaj obudowy, dodatkowo potwierdzony przez producenta oferowanego komputera). |  |
| Wirtualizacja | Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w  BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu). |  |
| BIOS | BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera lub nazwę modelu oferowanego komputera.  Pełna obsługa BIOS za pomocą klawiatury i myszy.  BIOS wyposażony w automatyczną detekcję zmiany konfiguracji, automatycznie nanoszący zmiany w konfiguracji w szczególności: procesor, wielkość pamięci, pojemność dysku. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania (w tym również systemu diagnostycznego) i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: wersji BIOS, nr seryjnym komputera, dacie produkcji komputera, włączonej lub wyłączonej funkcji aktualizacji BIOS, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, aktywnym kanale – dual channel, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki, typie zainstalowanego procesora, ilości rdzeni zainstalowanego procesora, typowej prędkości zainstalowanego procesora, maksymalnej osiąganej prędkości zainstalowanego procesora, pamięci cache L2 zainstalowanego procesora, pamięci cache L3 zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dyskach twardych podpiętych do dostępnych na płycie głównej portów SATA oraz M.2, rodzajach napędów optycznych, MAC adresie zintegrowanej karty sieciowej, zintegrowanym układzie graficznym, kontrolerze audio.  Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń.  Możliwość ustawienia hasła użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) oraz uprawniającego do samodzielnej zmiany tego hasła przez użytkownika (bez możliwości zmiany innych parametrów konfiguracji BIOS) przy jednoczesnym zdefiniowanym haśle administratora i/lub zdefiniowanym haśle dla dysku twardego. Użytkownik po wpisaniu swojego hasła jest wstanie jedynie zmienić hasło dla dysku twardego.  Możliwość włączenia/wyłączenia kontrolera SATA (w tym w szczególności pojedynczo).  Możliwość włączenia/wyłączenia kontrolera audio.  Możliwość włączenia/wyłączenia układu TPM.  Możliwość włączenia/wyłączenia wzbudzania komputera za pośrednictwem portów USB.  Możliwość włączenia/wyłączenia funkcjonalności Wake On LAN i WLAN.  Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych włączenia lub wyłączenia funkcji VT dla Direct I/O.  Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych włączenia lub wyłączenia dodatkowych funkcji sprzętowych Virtual Machine Mnitor (MVMM).  Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne.  Możliwość przeglądania i kasowania zdarzeń przebiegu procedury POST. Funkcja ta obejmuje datę i godzinę oraz opis incydentu kodu wizualnego systemu diagnostycznego.  Funkcja pozwalająca na włączenie/wyłączenie automatycznego tworzenia recovery BIOS na dysku twardym lub na urządzeniu zewnętrznym podpiętym przez USB.  Funkcja bezpiecznego usuwania danych oparta o JEDEC.  Oferowany BIOS musi posiadać poza swoją wewnętrzną strukturą menu szybkiego boot’owania które umożliwia min.: uruchamianie systemu z serwera za pośrednictwem zintegrowanej karty sieciowej, wejścia do BIOS, upgrade BIOS bez konieczności uruchamiania systemu operacyjnego. |  |
| Certyfikaty i standardy | Certyfikat ISO9001 dla producenta sprzętu (załączyć dokument potwierdzający spełnianie wymogu)  Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001  Deklaracja zgodności CE (załączyć do oferty)  Certyfikat TCO, wymagana certyfikacja na stronie : <http://tco.brightly.se/pls/nvp/!tco_search> – załączyć do oferty wydruk ze strony  Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram. |  |
| Ergonomia | Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy dysku twardego (IDLE) wynosząca maksymalnie 22 dB (załączyć oświadczenie producenta). |  |
| **System operacyjny -** w ofercie wymagane jest podanie nazwy i wersji systemu operacyjnego | |  |
| System operacyjny | * Zainstalowany system operacyjny Windows 10 Professional PL lub równoważny spełniający poniższe wymagania. * Możliwość współpracy z oprogramowaniem wykorzystywanym przez Zamawiającego m. in. Symfonia firmy Sage, Small Business, Płatnik. * Zainstalowany system operacyjny musi być dedykowany dla komputerów klasy PC. * Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek. * Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – poprzez witrynę producenta systemu. * Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) - wymagane podanie nazwy strony serwera WWW. * Internetowa aktualizacja zapewniona w języku polskim. * Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. * Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe. * Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi). * Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer. * Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta. * Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu. * Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie, praca systemu w trybie ochrony kont użytkowników. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego. System wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych. * Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie. Aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych. * Wbudowany system pomocy w języku polskim. * Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). Możliwość zarządzania stacją roboczą poprzez polityki - przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji. * Wdrażanie IPSEC oparte na politykach - wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. * Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. * Wsparcie dla logowania przy pomocy smartcard. * Rozbudowane polityki bezpieczeństwa - polityki dla systemu operacyjnego i dla wskazanych aplikacji. * Narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk. * Wsparcie dla Sun Java i .NET Framework 1.1 i 2.0 i 3.0 - możliwość uruchomienia aplikacji działających we wskazanych środowiskach. * Wsparcie dla Jscript i VBScript - możliwość uruchamiania interpretera poleceń. * Zdalna pomoc i współdzielenie aplikacji - możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. * Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową. * Rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację. * Graficzne środowisko instalacji i konfiguracji. * Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. Quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. * Zarządzanie kontami użytkowników w sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe. Udostępnianie modemu. * Możliwość przywracania plików systemowych. * Funkcjonalność pozwalająca na identyfikację sieci komputerowych, do których jest system podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików ftp.). * Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu). Na dysku twardym partycja RECOVERY umożliwiająca odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. |  |
| **Pakiet biurowy -** w ofercie wymagane jest podanie nazwy i wersji pakietu biurowego: | |  |
|  | Zainstalowany pakiet biurowy spełniający poniższe wymagania:  Pakiet biurowy (wraz z licencją na czas nieokreślony, kluczem instalacyjnym tego oprogramowania): Microsoft Office 2016 PL (lub nowszy) lub innego oprogramowania biurowego równoważnego, zawierającego co najmniej: edytor tekstu, arkusz kalkulacyjny, program do tworzenia prezentacji multimedialnych, program do obsługi poczty elektronicznej oraz kalendarza, które charakteryzuje się następującymi cechami:   * Możliwość współpracy z oprogramowaniem wykorzystywanym przez Zamawiającego m. in. Symfonia firmy Sage, Small Business, Płatnik. * Całkowicie zlokalizowany w języku polskim interfejs, system komunikatów i podręcznej kontekstowej pomocy technicznej (w tym także on-line) w pakiecie. * Możliwość automatycznej instalacji komponentów (przy użyciu instalatora systemowego). * Możliwość zdalnej instalacji komponentów. * Możliwość prowadzenia dyskusji oraz subskrypcji dokumentów w sieci z automatycznym powiadomieniem o zmianach w dokumentach, oraz publikowanie dokumentów wprost  z komponentów pakietu np. arkusza kalkulacyjnego. * W systemach pocztowych - możliwość delegacji uprawnień do otwierania, drukowania, modyfikowania i czytania załączanych dokumentów i informacji. * Możliwość blokowania niebezpiecznej lub niechcianej poczty. * Automatyczne przesyłanie poczty na podstawie reguł, automatyczne odpowiedzi, potwierdzanie dostarczenia do skrzynki adresata oraz potwierdzanie otwarcia poczty u adresata. * Współpraca z systemem MS Exchange, w tym odbiór poczty, możliwość udostępniania kalendarza dla innych użytkowników. * Wsparcie dla formatu .xml w podstawowych aplikacjach. * Możliwość nadawania uprawnień do modyfikacji i formatowania dokumentów lub ich fragmentów. * Automatyczne wyróżnianie i aktywowanie hyperlinków w dokumentach podczas edycji i odczytu. * Możliwość automatycznego odświeżania danych pochodzących z Internetu w arkuszach kalkulacyjnych. * Możliwość dodawania do dokumentów i arkuszy kalkulacyjnych podpisów cyfrowych, pozwalających na stwierdzenie czy dany dokument/arkusz pochodzi z bezpiecznego źródła i nie został w żaden sposób zmieniony. * Możliwość zaszyfrowania danych w dokumentach i arkuszach kalkulacyjnych zgodnie ze standardem cryptoapi. * Możliwość automatycznego odzyskiwania dokumentów i arkuszy kalkulacyjnych w wypadku odcięcia dopływu prądu. * Prawidłowe odczytywanie i zapisywanie danych w dokumentach w formatach: .doc, .docx, xls, .xlsx, .ppt, .pptx, .pps, .ppsx, w tym obsługa formatowania, wykonywanie i edycję makr oraz kodu zapisanego w języku VisualBasic for application w plikach .xls, xlsx, formuł, formularzy w plikach wytworzonych w MS Office 2003, MS Office 2007, MS Office 2010 bez utraty danych oraz bez konieczności reformatowania dokumentów. * Prawidłowe otwieranie i zapisywanie plików o formatach doc, docx, .xls, xlsx, .ppt, pptx. .pps, .ppsx bez utraty parametrów i cech użytkowych, zachowane wszelkie formatowanie, umiejscowienie tekstów, liczb, obrazków, wykresów, odstępy między tymi obiektami i kolorów, działające makra. * Prawidłowa współpraca zapis, odczyt z plikami danych programów pocztowych w formacie .pst oraz prawidłowy import z formatu .dbx. * Wszystkie komponenty oferowanego pakietu biurowego (edytor, arkusz, klient poczty, kalendarz oraz program do prezentacji) muszą być integralną częścią tego samego pakietu, współpracować ze sobą (osadzanie i wymiana danych), posiadać jednolity interfejs oraz ten sam jednolity sposób obsługi. * Poprawna praca w systemach operacyjnych, w które może być wyposażony zamawiany zestaw, tj. 64 bitowych z rodziny Windows 7, Windows 8, Windows 8.1 lub równoważny. * W przypadku zaoferowanego oprogramowania równoważnego należy podać dokładną nazwę i wersję oferowanego produktu. * Zamawiający nie dopuszcza zaoferowania pakietów biurowych, programów i planów licencyjnych opartych o rozwiązania chmury oraz rozwiązań wymagających stałych opłat w okresie używania zakupionego produktu. |  |
| **Oprogramowanie antywirusowe** **-** w ofercie wymagane jest podanie nazwy i wersji oprogramowania antywirusowego | |  |
|  | Zamawiający posiada oprogramowanie Eset Endpoint Security w wersji 6, jeżeli zostanie zaproponowane rozwiązanie firmy Eset należy dostarczyć tylko licencję, natomiast jeżeli zaoferowane zostanie oprogramowanie równorzędne, to muszą być spełnione określone wymagania:  **Licencja na oprogramowanie antywirusowe:**   1. Okres trwania licencji od momentu dostarczenia zestawów komputerowych do Zamawiającego do 20.12.2020. Wymóg ważności licencji spowodowany jest końcem obecnie wykorzystywanego przez Zamawiającego oprogramowania antywirusowego.   **Informacje ogólne:**   1. Pełne wsparcie dla systemu Windows 7, 8, 8.1, 10. 2. Wsparcie dla 32- i 64-bitowej wersji systemu Windows. 3. Wersja programu dla stacji roboczych Windows dostępna w języku polskim 4. Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim. 5. Skuteczność programu potwierdzona nagrodami VB100 i AV-comparatives   **Ochrona antywirusowa i antyspyware:**   1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. 3. Wbudowana technologia do ochrony przed rootkitami. 4. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 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. 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 (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania). 9. Skanowanie „na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 10. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu. 11. Możliwość skanowania dysków sieciowych i dysków przenośnych. 12. Skanowanie plików spakowanych i skompresowanych. 13. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. 14. Wykluczenie ze skanowania musi odbywać się nie tylko po nazwie pliku ale również ma być możliwe użycie symbolu wieloznacznego „\*” zastępującego dowolne znaki w ścieżce. 15. Administrator ma możliwość dodania wykluczenia po tzw. HASH’u zagrożenia, wskazującego bezpośrednio na określoną infekcję a nie konkretny plik. 16. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu. 17. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu. 18. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera. 19. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji. 20. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera. 21. 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. 22. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego). 23. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail. 24. 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). 25. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. 26. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości   e-mail lub tylko do zainfekowanych wiadomości e-mail.   1. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie. 2. 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. 3. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora. 4. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. 5. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 6. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe. 7. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta. 8. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego. 9. Program musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. 10. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym. 11. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego. 12. W przypadku gdy stacja robocza nie będzie posiadała dostępu do sieci Internet ma odbywać się skanowanie wszystkich procesów również tych, które wcześniej zostały uznane za bezpieczne. 13. 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. 14. 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. 15. Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika. 16. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia. 17. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe. 18. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. 19. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła. 20. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło. 21. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo. 22. 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. 23. Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu. 24. 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. 25. 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. 26. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia, dana funkcjonalność musi pozwalać na automatyczne wypełnienie właściwości urządzenia dla tworzonej reguły. 27. 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. 28. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. 29. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika. 30. Użytkownik ma posiadać możliwość takiej konfiguracji programu aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika 31. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS). 32. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:     * tryb automatyczny z regułami gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,     * tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,     * tryb oparty na regułach gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,     * tryb uczenia się, w którym program uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach.     * Tryb inteligentny – w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach. 33. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego. 34. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól. 35. Oprogramowanie musi posiadać zaawansowany skaner pamięci. 36. Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp. 37. 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. 38. Funkcja generująca taki log ma oferować filtrowanie wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa. 39. 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. 40. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu. 41. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami. 42. Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji program zgłosi posiadanie nieaktualnej bazy sygnatur. 43. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji. 44. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http. 45. Program musi być wyposażony w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback). 46. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa). 47. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. 48. Program musi posiadać możliwość utworzenia z poziomu interfejsu aplikacji dziennika diagnostycznego na potrzeby pomocy technicznej. 49. Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline. 50. W trakcie instalacji program ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór co najmniej następujących modułów do instalacji: ochrona antywirusowa i antyspyware, kontrola dostępu do urządzeń, zapora osobista, ochrona poczty, ochrona protokołów, kontrola dostępu do stron internetowych, , Obsługa technologii Microsoft NAP. 51. W programie musi istnieć możliwość tymczasowego wstrzymania polityk wysłanych z poziomu serwera zdalnej administracji. 52. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej. 53. Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas po którym automatycznie zostają przywrócone dotychczasowe ustawienia. 54. Administrator ma możliwość wstrzymania polityk na 10 min, 30 min, 1 godzinę i 4 godziny 55. Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika. 56. Program musi posiadać opcję automatycznego skanowania komputera po dokonaniu zmian z użyciem opcji wstrzymania polityki. 57. Aplikacja musi posiadać funkcję ręcznej aktualizacji komponentów programu. 58. Program musi posiadać możliwość definiowana stanów aplikacji, jakie będą wyświetlane użytkownikowi np. powiadomień o wyłączonych mechanizmach ochrony czy stanie licencji. 59. Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 60. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika aż do momentu wykrycia zagrożenia. 61. Aplikacja musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu. 62. Administrator ma możliwość dodania wykluczenia na podstawie procesu, wskazującego bezpośrednio na określony plik wykonywalny. 63. Program musi oferować możliwość umieszczenia na liście wyłączeń ze skanowania wybranej ścieżki, w której znajdują się pliki i foldery, które mają zostać wyłączone ze skanowania. 64. Program musi oferować możliwość umieszczenia na liście wyłączeń ze skanowania obiektu co najmniej w oparciu o nazwę zagrożenia oraz jego lokalizację. 65. Program musi oferować możliwość umieszczenia na liście wyłączeń ze skanowania pliku, wskazując sumę kontrolną pliku (jego HASH). 66. Program musi oferować mechanizm przesyłania zainfekowanych plików do laboratorium producenta, celem ich analizy, przy czym administrator musi mieć możliwość określenia, czy wysyłane mają być wszystkie zainfekowane próbki lub wszystkie z wyłączeniem dokumentów. 67. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. 68. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów. 69. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego. 70. Administrator musi posiadać możliwość zastosowania reguł dla kontroli dostępu do stron w zależności od zdefiniowanego przedziału czasowego.   **Ochrona przed spamem**   1. Ochrona antyspamowa dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail. 2. Program ma umożliwiać uaktywnienie funkcji wyłączenia skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej. 3. Pełna integracja z programami pocztowymi MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail – antyspamowe funkcje programu dostępne są bezpośrednio z paska menu programu pocztowego. 4. Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego. 5. 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. 6. Możliwość definiowania swoich własnych folderów, gdzie program pocztowy będzie umieszczać spam. 7. Możliwość zdefiniowania dowolnego Tag-u dodawanego do tematu wiadomości zakwalifikowanej jako spam. 8. Program ma umożliwiać współpracę w swojej domyślnej konfiguracji z folderem „Wiadomości śmieci” obecnym w programie Microsoft Outlook. 9. 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”. 10. Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.   **Zapora osobista (personal firewall)**   1. Zapora osobista ma pracować w 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. 2. Program musi akceptować istniejące reguły w zaporze systemu Windows, zezwalające na ruch przychodzący. 3. Możliwość tworzenia list sieci zaufanych 4. Możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie 5. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego. 6. Możliwość wyboru jednej z 3 akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj o decyzję. 7. Możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń. 8. Możliwość zapisywania w dzienniku zdarzeń związanych z zezwoleniem lub zablokowaniem danego typu ruchu. 9. Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer w tym minimum dla strefy zaufanej i sieci Internet. 10. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 11. Program musi umożliwiać ochronę przed przyłączeniem komputera do sieci botnet. 12. Wykrywanie zmian w aplikacjach korzystających z sieci i monitorowanie o tym zdarzeniu. 13. Program ma oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6. 14. Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci. 15. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci 16. Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora. 17. 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. 18. Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS zarówno z wykorzystaniem adresów IPv4 jak i IPv6 19. Opcje związane z autoryzacją stref mają oferować opcje łączenia (np. lokalny adres IP i adres serwera DNS) w dowolnej kombinacji celem zwiększenia dokładności identyfikacji danej sieci. 20. Program musi możliwość ustalenia tymczasowej czarnej listy adresów IP, które będą blokowane podczas próby połączenia.   **Kontrola dostępu do stron internetowych**   1. Aplikacja musi być wyposażona w zintegrowany moduł kontroli odwiedzanych stron internetowych. 2. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane zdefiniowane reguły. 3. Dodawanie użytkowników musi być możliwe w oparciu o już istniejące konta użytkowników systemu operacyjnego. 4. Profile mają być automatycznie aktywowane w zależności od zalogowanego użytkownika. 5. Aplikacja musi posiadać możliwość filtrowania url w oparciu o co najmniej 140 kategorii i podkategorii. 6. Podstawowe kategorie w jakie aplikacja musi być wyposażony 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. 7. Moduł musi posiadać także możliwość grupowania kategorii już istniejących. 8. Lista adresów url znajdujących się w poszczególnych kategoriach musi być na bieżąco aktualizowana przez producenta. 9. Użytkownik musi posiadać możliwość wyłączenia integracji modułu kontroli dostępu do stron internetowych. 10. Aplikacja musi posiadać możliwość określenia uprawnień dla dostępu do kategorii url – zezwól, zezwól i ostrzeż, blokuj. 11. Program musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania określonej w regułach witryny.   **Administracja zdalna**   1. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2008 Small Business, 2012, 2016. 2. Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance). 3. Serwer administracyjny musi wspierać instalację w oparciu o co najmniej bazy danych MS SQL i MySQL. 4. Konsola administracyjna musi umożliwiać podgląd szczegółów dotyczących bazy danych takich jak serwer Bazy danych, nazwę bazy danych, aktualny rozmiar bazy danych, nazwę hosta bazy danych 5. Serwer administracyjny musi oferować możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych. 6. Serwer administracyjny musi oferować możliwość wykorzystania już istniejącej bazy danych MS SQL lub MySQL użytkownika. 7. Rozwiązanie ma być w pełni zgodne z rozporządzeniem RODO. 8. 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. 9. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej. 10. Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy występujące w sieci. 11. Konsola musi umożliwiać zarządzanie wszystkimi rozwiązaniami Producenta zabezpieczającymi przed zagrożeniami. 12. Konsola musi umożliwiać zarządzanie systemem dynamicznej ochrony przed zagrożeniami 13. Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6. 14. Podczas logowania administrator musi mieć możliwość wyboru języka w jakim zostanie wyświetlony panel zarządzający. 15. Zmiana języka panelu administracyjnego nie może wymagać zatrzymania lub reinstalacji oprogramowania zarządzającego. 16. Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL. 17. Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci. 18. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych. 19. Serwer administracyjny musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie „hardware fingerprint” 20. Jeden centralny serwer centralnego zarządzania bez względu na wielkość sieci. 21. Instalacja serwera administracyjnego powinna oferować możliwość pracy w sieci rozproszonej nie wymagając dodatkowego serwera proxy. 22. Rozwiązanie ma oferować możliwość komunikacji agenta przy wykorzystaniu http Proxy wbudowanego w serwer centralnego zarządzania bez wykorzystania dodatkowej maszyny Proxy. 23. Serwer musi pełnić funkcję pośrednika pomiędzy lokalizacjami zdalnymi a serwerem centralnym. 24. Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM. 25. Serwer administracyjny musi oferować możliwość konfiguracji polityk zabezpieczeń takich jak ograniczenia funkcjonalności urządzenia, blokadę usuwania aplikacji, konfigurację usługi Airprint, konfigurację ustawień Bluetooth, Wi-Fi, VPN dla urządzeń z systemem iOS 10 oraz 11 26. 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. 27. Serwer http proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) najczęściej pobieranych elementów. 28. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów. 29. Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy. 30. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na stacjach roboczych z systemami Windows, Mac OS X oraz Linux oraz serwerach Windows. 31. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na urządzeniach mobilnych z systemem Android. 32. Centralna administracja musi pozwalać na zarządzanie urządzeniami mobilnymi z systemem iOS. 33. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware’ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci. 34. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta. 35. Administrator musi posiadać możliwość zarządzania za pomocą dedykowanego agenta stacjami nie posiadającymi zainstalowanego programu zabezpieczającego. 36. Agent musi przekazywać informacje na temat stanu systemu operacyjnego do serwera administracji zdalnej. 37. Z poziomu konsoli zarządzania administrator ma mieć możliwość weryfikacji podzespołów bazowych zarządzanego komputera oraz weryfikację zainstalowanego oprogramowania firm trzecich na stacji dla systemów Windows, Mac oraz Linux z możliwością jego odinstalowania. 38. Serwer administracyjny musi oferować możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie. 39. Instalacja agenta musi odbywać się przy wykorzystaniu repozytorium producenta. Repozytorium powinno zawierać aktualne wersje agentów bez względu na rodzaj systemu operacyjnego. 40. Konsola ma oferować możliwość aktywacji oraz wdrożenie elementów systemu EDR producenta. 41. Instalacja agenta nie może wymagać określenia typu systemu (32 lub 64 – bitowy) oraz jego rodzaju (Windows, Mac, itp) a dobór odpowiedniego pakietu musi być w pełni automatyczny. 42. Instalacja klienta na urządzeniach mobilnych musi być dostępna za pośrednictwem portalu WWW udostępnionego przez moduł MDM z poziomu urządzenia użytkownika. 43. W przypadku braku zainstalowanego klienta na urządzeniu mobilnym musi istnieć możliwość jego pobrania ze sklepu Google Play. 44. Administrator musi posiadać możliwość utworzenia listy zautoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji. 45. 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. 46. Serwer administracyjny musi oferować możliwość utworzenia polityk konfiguracji dla aplikacji zabezpieczającej na urządzeniu mobilnym. 47. Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów serwera centralnego zarządzania do zarządzania stacjami roboczymi. 48. Administrator musi posiadać możliwość utworzenia użytkownika wbudowanego lub zintegrowanego z grupą z usługi Active Directory. 49. Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp. 50. Administrator musi posiadać możliwość nadania dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko do odczytu, odczyt/zapis. 51. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika. 52. Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta bez konieczności logowania się do panelu administracyjnego. 53. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności po jakim użytkownik zostanie automatycznie wylogowany. 54. Dostępne zadania muszą być podzielone na dwie grupy: zadania klienta oraz zadania serwera. 55. Zadania serwera obejmujące zadanie instalacji agenta, generowania raportów oraz synchronizacji grup. 56. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej. 57. 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. 58. Serwer administracyjny musi w przejrzysty sposób informować administratora o elementach zadań jakie są wymagane do jego uruchomienia, a w przypadku jego braku wskazywać brakujące elementy konfiguracji. 59. Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym. 60. Serwer administracyjny musi oferować możliwość wyboru parametrów pakietu instalacyjnego zależnych od systemu operacyjnego oraz licencji na program zabezpieczający. 61. Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu. 62. Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką. 63. Serwer administracyjny musi oferować możliwość utworzenia jednego zadania dla kilku klientów lub grupy. 64. Serwer administracyjny musi oferować możliwość uruchomienia zadania automatycznie zgodnie z harmonogramem, po wystąpieniu nowego dziennika zdarzeń lub umieszczeniu nowego klienta w grupie dynamicznej. 65. Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów. 66. Serwer administracyjny musi oferować możliwość utworzenia polityk dla programów zabezpieczających i modułów serwera centralnego zarządzania. 67. 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. 68. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej. 69. 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. 70. Serwer administracyjny musi umożliwiać wyświetlenie polityk do których przynależy dana stacja robocza oraz ich edycję z poziomu właściwości samego klienta   **Raportowanie i komunikacja z użytkownikiem**   1. Serwer administracyjny musi posiadać minimum 20 szablonów raportów przygotowanych przez producenta 2. Serwer administracyjny musi oferować możliwość utworzenia własnych raportów lub skorzystanie z predefiniowanych wzorów. 3. Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania. 4. Serwer administracyjny musi oferować możliwość wyboru formy przedstawienia danych w raporcie w postaci tabeli, wykresu lub obu elementów jednocześnie. 5. Serwer administracyjny musi oferować możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy, itp. 6. Serwer administracyjny musi oferować możliwość określenia danych jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na elementach wykresu oraz ich odfiltrowania i posortowania oraz zapisania szablonów stworzonych filtrów 7. Serwer administracyjny musi być wyposażony w mechanizm importu oraz eksportu szablonów raportów. 8. Serwer administracyjny powinien posiadać Panel kontrolny z raportami administratora, pozwalający na szybki dostępu do najbardziej interesujących go danych. Panel ten musi oferować możliwość modyfikacji jego elementów. 9. Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym dostępnym z poziomu interfejsu konsoli WWW. 10. Serwer administracyjny musi oferować możliwość wygenerowania raportu na podstawie danych z systemu EDR producenta. 11. Serwer administracyjny musi oferować możliwość wygenerowania raportu na podstawie informacje o zainstalowanych podzespołów w stacjach roboczych. 12. Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub PS. 13. Serwer administracyjny musi oferować możliwość skonfigurowania czasu automatycznego odświeżania raportu na panelu kontrolnym oraz umożliwiać jego odświeżenie na żądanie. 14. Serwer administracyjny musi oferować możliwość tworzenia wielu zakładek panelu, w których będą widoczne wybrane przez administratora elementy monitorujące. 15. Serwer administracyjny musi oferować możliwość maksymalizacji wybranego elementu monitorującego. 16. Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy. 17. Serwer administracyjny musi oferować możliwość utworzenia własnych powiadomień lub skorzystanie z predefiniowanych wzorów. 18. Serwer administracyjny musi oferować możliwość utworzenia własnych powiadomień na zasadzie „WYSIWYG” z wykorzystaniem istniejących zmiennych. 19. Powiadomienia mailowe mają być wysyłane w formacie HTML. 20. Powiadomienia muszą dotyczyć zmiany ilości klientów danej grupy dynamicznej, wzrostu liczby grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń lub skanowania lub stanu obiektu serwer centralnego zarządzania. 21. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP. 22. Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu.   **Wymagania dodatkowe**   1. Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji bądź korzystając z powiązanego konta systemu zarządzania licencjami. 2. W przypadku posiadania tylko jednej dodanej licencji do konsoli zarządzania ma być ona wybierana automatycznie podczas konfiguracji zadania. 3. Rozwiązanie ma oferować weryfikacji zainstalowanych komponentów bazowych urządzenia takich jak: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe, etc. 4. Serwer administracyjny musi oferować możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja. 5. Narzędzie administracyjne musi być wyposażone w mechanizm wyszukiwania zarządzanych komputerów na podstawie co najmniej nazwy komputera, adresu IPv4 i IPv6 lub wyszukania konkretnej nazwy zagrożenia. 6. W przypadku wystąpienia problemu rozwiązanie ma oferować możliwość przekierowania do wyszukiwarki Google z odwołaniem do konkretnego kodu błędu, który wystąpił w środowisku. 7. Serwer administracyjny oferować łatwy dostęp do zadań z poziomu menu kontekstowego w zależności od rodzaju urządzenia. 8. Administrator musi mieć możliwość podłączenia do stacji roboczej z użyciem protokołu RDP bezpośrednio z poziomu konsoli ERA. 9. Administrator musi otrzymywać powiadomienia o dostępnych aktualizacjach z poziomu interfejsu Konsoli administracyjnej. 10. Możliwość podejrzenia licencji za pomocą, której program został aktywowany. |  |
| **Monitor** - w ofercie wymagane jest podanie modelu, symbolu oraz producenta. | |  |
| Format ekranu monitora | Panoramiczny |  |
| Przekątna ekranu | 21,5” |  |
| Wielkość plamki | 0,248 mm |  |
| Typ panelu LCD | TFT IPS |  |
| Technologia podświetlenia | Edge-LED |  |
| Zalecana rozdzielczość obrazu | 1920x1080 pikseli |  |
| Częstotliwość odświeżania | 60Hz (przy zalecanej rozdzielczości) |  |
| Czas reakcji matrycy | 5 ms |  |
| Jasność | 250 cd/m2 |  |
| Kontrast | 1000:1 |  |
| Kąty widzenia:   * Poziomy: * Pionowy: | 178 stopni  178 stopni |  |
| Liczba wyświetlanych kolorów | 16,7 mln |  |
| Interfejsy | 1 x VGA  1 x HDMI/Display Port  3 x USB, w tym min. 2 x USB 3.0 |  |
| Podstawa | Regulowana wysokość, regulowany kąt pochylenia, regulacja kąta obrotu |  |
| Certyfikaty i standardy | Certyfikat TCO, wymagana certyfikacja na stronie: <http://tco.brightly.se/pls/nvp/!tco_search> – załączyć do oferty wydruk z strony  Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram. |  |
| **Peryferie** |  | |
| Klawiatura | Klawiatura USB w układzie QWERTY, z wydzieloną klawiaturą numeryczną. W ofercie wymagane jest podanie modelu, symbolu oraz producenta. |  |
| Urządzenie wskazujące | Mysz: optyczna, przewodowa (USB), 2 przyciski i rolka, 1000dpi. W ofercie wymagane jest podanie modelu, symbolu oraz producenta. |  |
| **Gwarancja i wsparcie techniczne** | | |
| Warunki gwarancji i wsparcia technicznego | Niezależnie od wybranego poziomu wsparcia technicznego:  Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.  Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.  Minimalny czas trwania wsparcia technicznego producenta wynosi 3 lata, z możliwością odpłatnego przedłużenia tego okresu do 4 lub 5 lat od daty dostawy.  Sposób realizacji usług wsparcia technicznego :   * Telefoniczne zgłaszanie usterek w dni robocze w godzinach 8-17. * Dedykowany bezpłatny portal online do zgłaszania usterek i zarządzania zgłoszeniami serwisowymi.   Wsparcie techniczne dla sprzętu będzie dostarczane zdalnie lub w miejscu instalacji urządzenia, w zależności od rodzaju zgłaszanej awarii.  W przypadku awarii zakwalifikowanej jako naprawa w miejscu instalacji urządzenia, część zamienna wymagana do naprawy i/lub technik serwisowy przybędzie na miejsce wskazane przez klienta na następny dzień roboczy od momentu skutecznego przyjęcia zgłoszenia przez Dział Wsparcia Technicznego.  Możliwość sprawdzenia aktualnego okresu i poziomu wsparcia technicznego dla urządzeń za pośrednictwem strony internetowej producenta.  Możliwość pobrania aktualnych wersji sterowników oraz firmware urządzenia za pośrednictwem strony internetowej producenta również dla urządzeń z nieaktywnym wsparciem technicznym.  Dostawca zapewni bezpłatne oprogramowanie do automatycznej diagnostyki i zdalnego zgłaszania awarii do serwisu. |  |
|  | Zamawiający wymaga aby z zestawem komputerowym zostało dostarczone kompletne okablowanie: kabel VGA i kabel HDMI/DisplayPort (kabel HDMI/DisplayPort w zależności od wyposażenia monitora i stacji roboczej w stosowne porty), kabel USB 3.0 (łączący monitor ze stacją roboczą), kable zasilające.  Dodatkowo należy dostarczyć minimum 10 sztuk nośnika instalacyjnego sytemu operacyjnego, np. na płycie DVD. |  |
| **Wymagania do kryterium oceny ofert** | |  |
| Jeden producent (P) | *tak/nie (dotyczy stacji roboczej, monitora, myszy, klawiatury)* |  |
| Czas realizacji (R) | *wpisać datę realizacji zamówienia* |  |
| Pakiet biurowy (B) | *wpisać nazwę i wersję oprogramowania biurowego* |  |
| Gwarancja NBD (G) | *tak/nie* |  |
| Oprogramowanie antywirusowe (A) | *wpisać nazwę i wersję oprogramowania antywirusowego* |  |

……………………………..……………

(podpis i pieczęć osoby uprawnionej)