

**Oznaczenie sprawy: 25/ZP/2020 Załącznik nr 2 do SIWZ**

**Stanowiska komputerowe 50 szt**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Lp** | **PARAMETR WYMAGANY** | | | **PARAMETR OFEROWANY** | |
|  | **Nazwa ,typ model,**  **Producent**  **Rok produkcji, miesiąc** | | | | |
|  | | **Wymagania techniczne** | | | |
| 1 | | Komputer | Komputer będzie wykorzystywany dla potrzeb aplikacji szpitalnych aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu. | |  |
| 2 | | Obudowa | Typu mini Tower z obsługą kart PCI Express wyłącznie o niskim profilu.  Fabrycznie umożliwiająca montaż min. 2 kieszeni: 1 szt. na napęd optyczny typu slim, 1 szt. 3,5”na standardowy dysk twardy  Wyposażona w czytnik kart multimedialnych  - Obudowa trwale oznaczona nazwą producenta, nazwą komputera, numerem MTM, PN, numerem seryjnym  - Wyposażona w budowany głośnik o mocy min. 1.5W | |  |
| 3 | | Zasilacz | Zasilacz maksymalnie 180W o sprawności minimum 85% | |  |
| 4 | | Chipset | Dostosowany do zaoferowanego procesora | |  |
| 5 | | Płyta główna | Zaprojektowana i wyprodukowana przez producenta komputera. Trwale oznaczona logo lub nazwą producenta na etapie produkcji płyty głównej.  Wyposażona w złącza min.:   * 1 x PCI Express 3.0 x16, * 1 x PCI Express 3.0 x1, * 2 x M.2 z czego min. 1 przeznaczona dla dysku SSD z obsługą PCIe NVMe | |  |
| 6 | | Procesor | Procesor klasy x86, zaprojektowany do pracy w komputerach stacjonarnych, Intel® Core™ i5-9400 lub równoważny na poziomie wydajności liczonej w punktach na podstawie PerformanceTest w teście CPU Mark według wyników opublikowanych na http://www.cpubenchmark.net/. Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu. | |  |
| 7 | | Pamięć operacyjna | Min. 8GB DDR4 2666 MHz z możliwością rozszerzenia do 32 GB  Ilość banków pamięci: min. 2 szt.  Ilość wolnych banków pamięci: min. 1 szt. | |  |
| 8 | | Dysk twardy | Min 256GB PCIe NVMe zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. | |  |
| 9 | | Napęd optyczny | Wbudowana nagrywarka DVDRW | |  |
| 10 | | Karta graficzna | Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki w trybie UMA (Unified Memory Access) – z możliwością dynamicznego przydzielenia pamięci. | |  |
| 11 | | Audio | Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. | |  |
| 12 | | Karta sieciowa | LAN 10/100/1000 Mbit/s z funkją PXE oraz Wake on LAN  Karta sieciowa WIFI ac + Bluetooth w wersji minimum 4.0 | |  |
| 13 | | Porty/złącza | Wbudowane porty/złącza:  Wideo różnego typu umożliwiające elastyczne podłączenie urządzenia bez stosowania przejściówek lub adapterów za pomocą min:  - 1 x VGA,  - 1 x DP,  - 1 x HDMI  Pozostałe porty/złącza:  - 8 x USB w tym:  - z przodu obudowy min. 4 x USB3.1  - z tyłu obudowy min. 4 x USB  - port sieciowy RJ-45,  - porty słuchawek i mikrofonu na przednim lub tylnym panelu obudowy  - port szeregowy  - czytnik kart pamięci 7-in-1  Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp. | |  |
| 14 | | Klawiatura/mysz | Klawiatura przewodowa USB w układzie US  Mysz przewodowa USB (scroll) | |  |
| 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 | | 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,  - AssetTag,  - 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 wentylatora w obudowie komputera  - napędach lub dyskach podłączonych do portów SATA oraz M.2 (model dysku i napędu optycznego)  Możliwość z poziomu Bios:  - wyłączenia/włączenia portów USB zarówno z przodu jak i z tyłu obudowy  - wyłączenia selektywnego (pojedynczego) portów SATA,  - wyłączenia karty sieciowej, karty audio, portu szeregowego,  - 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  - załadowania optymalnych ustawień Bios  - obsługa Bios za pomocą klawiatury i myszy | |  |
| 17 | | 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. | |  |
| 18 | | Certyfikaty i standardy | * Certyfikat ISO9001:2000 dla producenta sprzętu * ENERGY STAR * Deklaracja zgodności CE * Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki | |  |
| 19 | | Waga/rozmiary urządzenia | Waga urządzenia poniżej 6 kg  Wysokość nie może być większa niż 29cm (patrząc od frontu obudowy)  Szerokość nie może być większa niż 11cm (patrząc od frontu obudowy) | |  |
| 20 | | Gwarancja | 3 lata świadczona w miejscu użytkowania sprzętu (on-site)  Oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. | |  |
| 21 | | Wsparcie techniczne producenta | - możliwość weryfikacji u producenta konfiguracji fabrycznej zakupionego sprzętu  - Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta. | |  |
| 22 | | Wymagania dodatkowe | Zamawiający zastrzega sobie prawo sprawdzenia pełnej zgodności parametrów oferowanego sprzętu z wymogami niniejszej SIWZ. W tym celu Wykonawcy na wezwanie Zamawiającego dostarczą do siedziby Zamawiającego w terminie 10 dni od daty otrzymania wezwania, próbkę oferowanego sprzętu. W odniesieniu do programowania mogą zostać dostarczone licencje tymczasowe, w pełni zgodne z oferowanymi. Ocena złożonych próbek zostanie dokonana przez Komisję Przetargową na zasadzie spełnia / nie spełnia. Z badania każdej próbki zostanie sporządzony protokół. Pozytywna ocena próbki będzie oznaczała zgodność próbki (oferty) z treścią SIWZ. Niezgodność próbki z SIWZ chociażby w zakresie jednego parametru podlegającemu badaniu bądź nieprzedłożenie wymaganej próbki w sposób i terminie wymaganym przez Zamawiającego będzie oznaczało negatywny wynik oceny próbki i będzie skutkowało odrzuceniem oferty na podstawie art. 89 ust. 1 pkt 2 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2015 r. poz. 2164 ze zm.), tj. z uwagi na fakt, że treść oferty nie odpowiada treści specyfikacji istotnych warunków zamówienia. Szczegółowy sposób przygotowania i złożenia próbek zostanie dostarczony wykonawcom wraz z wezwaniem do złożenia próbek | |  |

**Monitory komputerowe 50 szt**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Lp.** | **PARAMETR WYMAGANY** | | | **PARAMETR OFEROWANY** | | **UWAGI** |
|  | **Nazwa ,typ model,**  **Producent**  **Rok produkcji, miesiąc** | | | | | |
|  | | **Wymagania techniczne** | | | | |
| **1** | | Rodzaj podświetlenia | WLED | |  | |
| 2 | | Typ panelu | VA | |  | |
| 3 | | Wielkość przekątne | Min. 23.5" | |  | |
| 4 | | Współczynnik kształtu | 16:9 | |  | |
| 5 | | Rozdzielczość | 1920 x 1080 | |  | |
| 6 | | Jasność | 250 cd/m² | |  | |
| 7 | | Czas reakcji | Max 6 ms (tryb normalny) | |  | |
| 8 | | Kąty widzenia: | 178/178 | |  | |
| 9 | | Złącza | VGA, HDMI, Jack 3.5 mm | |  | |
| 10 | | Zużycie energii w trybie aktywności/maksymalne: | 18 wat/ 22 wat | |  | |
| 11 | | Dodatkowe | Zintegrowane zarządzanie kablami | |  | |
| 12 | | Gwarancja | Min. 36 miesięcy | |  | |

**UPS – 1 szt.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | Opis wymagań  techniczno-funkcjonalnych | | |
|  | **Nazwa handlowa, typ model**  **Producent**  **Urządzenie fabrycznie nowe, rok produkcji, miesiąc** | | |
| **1** | Technologia | VFI (true on-line, podwójne przetwarzanie energii) |  |
| **2** | Moc znamionowa | 20kVA / 18kW |  |
| **3.** | Moc nominalna przy współczynniku mocy obciążenia od 0,9 indukcyjny do 0,9 pojemnościowy [kW] - bez obniżania mocy | 18kW |  |
| **4.** | Technologia prostownika | Moduły IGBT wysokiej częstotliwości |  |
| **5.** | Wyjściowy współczynnik mocy (PF) | 0,9 |  |
| **6.** | Napięcie wejściowe | 400 VAC lub 230 VAC |  |
| **7.** | Wejściowy współczynnik mocy | Przy wejściu 3-fazowym: ≥ 0,95  Przy wejściu 1-fazowym: ≥ 0,99 |  |
| **8.** | Tolerancja napięcia wejściowego | Przy wejściu 3-fazowym: dla 50% obciążenia (190-520)±5 VAC, dla 100% obciążenia (277-520)±5 VAC;  Przy wejściu 1-fazowym: 50% obciążenia (110-300)±5 VAC, 100% obciążenia (160-300)±5 VAC. |  |
| **9.** | Częstotliwość wejściowa | 40-70 Hz |  |
| **10.** | Minimalna sprawność AC-AC w trybie pracy on-line z obciążeniem 100% | 93% |  |
| **11.** | Minimalna sprawność w trybie ECO | 98% |  |
| **12.** | Możliwość rozbudowy mocy w okresie eksploatacji (praca równoległa) | do 6 jednostek |  |
| **13.** | Napięcie wyjściowe | 208V/210V/220V/230V/240 VAC (ustawiane z poziomu LCD) |  |
| **14.** | Częstotliwość wyjściowa | 50/60Hz (programowalna) |  |
| **15.** | Zintegrowane bezprzerwowe przełączniki obejściowe (by-pass) wewnątrz zasilacza UPS | Statyczny przełącznik,  ręczny odłącznik serwisowy |  |
| **16.** | Czas podtrzymania | 5 minut dla obciążenia 20kVA/16kW |  |
| **17.** | Intuicyjny panel LCD | TAK |  |
| **18.** | Stabilizacja napięcia wyjściowego | ±1% |  |
| **19.** | Zniekształcenia napięcia wyjściowego | ≤ 2% z obciążeniem liniowym  ≤ 5% z obciążeniem nieliniowym |  |
| **20.** | Współczynnik szczytu przy obciążeniu znamionowym | 3:1 |  |
| **21.** | Przeciążenie inwertera | 105%-125% przez 3 minuty  125% -150% przez 30 sekund  >150% przez 0,1 sekundy |  |
| **22.** | Złącze interfejsów | RS232 + USB |  |
| **23.** | Interfejs EPO (do wyłącznika ppoż.) | TAK |  |
| **24.** | Prąd ładowania | 7A |  |
| **25.** | Baterie | Szczelne, bezobsługowe,  w technologii AGM |  |
| **26.** | Możliwość oddzielnego zasilania linii bypassu wewnętrznego. | TAK |  |
| **27.** | Oprogramowanie zapewniające pełny monitoring, zarządzanie i automatyczny shut-down systemu operacyjnego | TAK |  |
| **28.** | Poziom hałasu w odległości 1m | ≤ 60 dBA |  |
| **29.** | Rejestr zdarzeń | TAK |  |
| **30.** | Spełnienie wszystkich obowiązujących norm bezpieczeństwa potwierdzone deklaracją zgodności CE | TAK |  |
| **31.** | Maks. wymiary szafy UPS (szer. x gł. x wys.) | 262 x 580 x 628 mm |  |
| **31.** | Maksymalne wymiary szafy bateryjnej  (szer. x gł. x wys.) | 250 x 592 x 576 mm |  |
| **33.** | Instrukcja w języku polskim | TAK |  |
| **34.** | Gwarancja | Min. 36 miesięcy |  |
| **35.** | Autoryzowany serwis producenta oferowanego zasilacza UPS przeprowadzi instalację i uruchomienie urządzenia na obiekcie oraz profesjonalne szkolenie z zakresu obsługi dla wyznaczonych przez zamawiającego pracowników | TAK |  |

**1.4 Szafa Rack** **– 1 szt.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Parametr** |  |  |
| 1 | Wysokość | 42U |  |
| 2 | Inne | Dedykowana do rozwiązań serwerowych, przystosowana do chłodzenia metodą przedmuchu, Drzwi przednie I tylne zamykane perforowane, Zdejmowane panele boczne. Drzwi tylne dzielone |  |

**Oprogramowanie antywirusowe– 133 szt.**

Pełne wsparcie dla systemu Windows Vista/Windows 7/Windows 8/Windows 8.1/Windows 10

2. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.

3. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.

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. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.

8. Możliwość skanowania dysków sieciowych i dysków przenośnych.

9. Skanowanie plików spakowanych i skompresowanych.

10. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.

11. Administrator ma możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji.

12. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.

13. 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).

14. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie.

15. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.

16. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

17. 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 oraz urządzeń przenośnych.

18. Funkcja blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.

19. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.

20. 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.

21. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:

* 1. • tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
  2. • tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
  3. • tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
  4. • 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,
  5. • tryb inteligentny, w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach.

22. 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 procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.

23. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić zagrożenie bezpieczeństwa.

24. Automatyczna, inkrementacyjna aktualizacja silnika detekcji.

25. Program wyposażony tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).

26. Program musi posiadać możliwość aktywacji przy użyciu co najmniej jednej z trzech metod: poprzez podanie poświadczeń administratora licencji, klucza licencyjnego lub aktywacji programu w trybie offline.

27. Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

28. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia zagrożenia.

29. Program musi umożliwiać ochronę przed dołączeniem komputera do sieci botnet.

**Ochrona serwera plików Windows**

1. Wsparcie dla systemów: Microsoft Windows Server 2019, Microsoft Windows Server 2016,Microsoft Windows Server 2012 R2, Microsoft Windows Server 2012, Microsoft Windows Server 2008 R2 SP1, Microsoft Windows Server 2008 SP2 (oparty na procesorze x86 i x64), Server Core (Microsoft Windows Server 2008 SP2, 2008 R2 SP1, 2012, 2012 R2, 2016).

2. Instalator musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji.

3. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.

4. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.

5. Wbudowana technologia do ochrony przed rootkitami i exploitami.

6. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych.

7. Aplikacja powinna wspierać mechanizm klastrowania.

8. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).

9. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: a. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,

b. tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,

c. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,

d. 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,

e. tryb inteligentny, w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach.

10. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS.

11. 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 oraz urządzeń przenośnych.

12. Funkcja blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.

13. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.

14. 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.

15. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.

16. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony.

17. Dodanie automatycznych wyłączeń nie wymaga restartu serwera.

18. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych.

19. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego.

20. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line).

21. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

22. 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 procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.

23. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić zagrożenie bezpieczeństwa.

24. Automatyczna, inkrementacyjna aktualizacja silnika detekcji.

25. Aplikacja musi wspierać skanowanie magazynu Hyper-V.

26. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów.

27. Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

28. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika aż do momentu wykrycia zagrożenia.

29. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych*.*

30. Administrator musi posiadać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.

31. Program musi umożliwiać ochronę przed przyłączeniem komputera do sieci botnet.

32. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.

33. Administrator ma możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji.

34. Aplikacja musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

35. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

36. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.

37. Program musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.

**Administracja zdalna**

1. Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2008 R2, 2012, 2016, 2019 oraz systemach Linux.

2. Serwer zarządzający musi być dostępny w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance) oraz dysku wirtualnego w formacie VHD.

3. Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.

4. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.

5. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.

6. Podczas logowania do konsoli, administrator musi mieć możliwość wyboru języka, w jakim zostanie wyświetlony interfejs.

7. Zmiana języka interfejsu konsoli nie może wymagać jej zatrzymania, ani reinstalacji.

8. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.

9. Serwer administracyjny musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.

10. Serwer administracyjny musi posiadać wsparcie dla „VDI” oraz „Golden Master Image”.

11. Serwer administracyjny musi posiadać możliwość podłączenia 250 000 hostów.

12. Administrator musi posiadać możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM.

13. Serwer administracyjny musi posiadać możliwość sprawdzenia lokalizacji dla urządzeń z systemami iOS.

14. Serwer administracyjny musi posiadać możliwość wdrożenia urządzenia z iOS z wykorzystaniem programu DEP.

15. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.

16. Serwer administracyjny musi posiadać możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi, host agenta wirtualnego.

17. Serwer administracyjny musi pozwalać na zarządzanie urządzeniami z systemem iOS.

18. Serwer administracyjny musi pozwalać na centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, zapora osobista, kontrola dostępu do stron internetowych, które działają na stacjach roboczych w sieci.

19. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.

20. Administrator musi posiadać możliwość zarządzania stacjami roboczymi za pomocą dedykowanego agenta, na których nie jest zainstalowane oprogramowanie zabezpieczające.

21. Z poziomu konsoli zarządzania administrator ma mieć możliwość weryfikacji podzespołów zarządzanego komputera (w tym przynajmniej: 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) oraz wylistowanie zainstalowanego oprogramowania firm trzecich dla systemów Windows oraz MacOS z możliwością jego odinstalowania.

22. Serwer administracyjny musi posiadać możliwość aktywacji oraz wdrożenie elementów systemu EDR tego samego producenta.

23. Administrator musi posiadać możliwość utworzenia użytkownika serwera administracyjnego.

24. Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.

25. Serwer administracyjny musi posiadać możliwość deinstalacji programu zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.

26. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.

27. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.

28. Serwer administracyjny musi posiadać minimum 170 szablonów raportów, przygotowanych przez producenta.

29. Serwer administracyjny musi posiadać możliwość utworzenia własnych raportów.

30. Serwer administracyjny musi posiadać możliwość wyboru formy przedstawienia danych w raporcie w tym przynajmniej: w postaci tabeli, wykresu lub obu elementów jednocześnie.

31. Serwer administracyjny musi posiadać możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy.

32. Serwer administracyjny musi posiadać możliwość określenia danych, jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na osiach wykresu oraz ich odfiltrowania i posortowania.

33. Serwer administracyjny musi być wyposażony w mechanizm importu oraz eksportu szablonów raportów.

34. Administrator musi posiadać możliwość wysłania powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.

35. Serwer administracyjny musi posiadać możliwość dodania licencji przynajmniej przy użyciu klucza licencyjnego, pliku offline licencji oraz konta systemu zarządzania licencjami.

36. Serwer musi umożliwić podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.

37. Serwer musi wspierać wysyłanie logów do systemu SIEM IBM qRadar w jego natywnym formacie.

38. Konsola administracyjna musi umożliwiać personalizację interfejsu webowego