Załącznik Nr 1 do SIWS

Załącznik Nr 1 do umowy

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

## Wstęp

Przedmiotem projektu jest wdrożenie elektronicznych usług publicznych i elektronicznej dokumentacji medycznej w podmiocie leczniczym. Dzięki projektowi ma zostać rozbudowany dostęp do e-usług publicznych na terenie gminy Lubawka.

Celem projektu jest podniesienie jakości i dostępności do usług medycznych świadczonych przez placówkę poprawa jakości życia pacjentów podmiotu leczniczego poprzez dostarczenie systemu informatycznego umożliwiającego uruchomienie e-usług, usprawniających komunikację pacjent-przychodnia.

Cele projektu mają zostać zrealizowane poprzez dostarczenie oprogramowania aplikacyjnego (Zintegrowany System Informatyczny, platforma e-usług) wraz niezbędnym oprogramowaniem systemowym i infrastrukturą sprzętową oraz wykonanie usług zapewniających pełne uruchomienie systemu informatycznego.

## Zakres zamówienia

Zamówienie obejmuje:

Dostawa licencji na Zintegrowany System Informatyczny (ZSI) dla minimum 25 użytkowników, obejmujący system Obsługi Przychodni i system Obsługi Laboratorium wraz z niezbędną bazą danych, infrastrukturą sprzętową i oprogramowaniem systemowym. System należy uruchomić (połączyć ze sobą) w 3 lokalizacjach

* Samodzielny Publiczny Zakład Opieki Zdrowotnej w Lubawce, ul. Kościuszki 19, 58-420 Lubawka
* Ośrodek Zdrowia, Miszkowice 68 a, 58-420 Lubawka
* Ośrodek Zdrowia, Chełmsko Śląskie ul. Lubawska 26, 58-420 Lubawka
1. Uruchomienie platformy e-usług dla pacjentów zintegrowanych z systemem ZSI.
2. Uruchomienie dostępu dla personelu i pacjentów do aplikacji mobilnych, umożliwiających komunikację z systemem ZSI.
3. Wykonanie usług wdrożeniowych.
4. Świadczenie usług gwarancyjnych

System ma pracować w oparciu o jedną wspólną bazę danych dla wszystkich lokalizacji. Serwer bazy danych ma zostać zainstalowany w siedzibie głównej.

I. Wykaz licencji oprogramowania aplikacyjnego - wymaganych do dostarczenia.

**System do Obsługi Przychodni:**

Stanowisko podstawowe – 18 szt.

Gabinet stomatologiczny (stanowisko) – 3 szt.

Rozliczenie prowizji lekarskich (moduł) – 1 szt.

Archiwum elektronicznej dokumentacji medycznej (moduł) – 1 szt.

Podpis cyfrowy (stanowisko) – 21 szt.

**System do Obsługi Laboratorium (LIS)**

Rejestracja stanowisko – 2 szt.

Kartoteki (moduł) – 1 szt.

Pracownia analityki stanowisko – 2 szt.

**Baza danych**

Licencja umożliwiająca uruchomienie bazy danych na zamawianym serwerze. Licencja bez limitu użytkowników, minimum 36 miesięcy gwarancji, dopuszczalne dostarczenie licencji umożliwiającej uruchomienie aplikacji jednego producenta.

**Licencje umożliwiające uruchomienie aplikacji na urządzeniach mobilnych:**

Mobilny moduł wspierający pracę lekarza POZ stanowisko – 1 szt.

Mobilny moduł wspierający pracę pielęgniarki POZ stanowisko – 1 szt.

Aplikacja komunikacyjna dla Pacjenta – bez ograniczeń liczby pacjentów, którzy mogą korzystać z aplikacji.

II. Wykaz usługi wymaganych do wykonania:

1. Przeprowadzenie analizy przedwdrożeniowej.
2. Dostawa sprzętu komputerowego do siedziby Zamawiającego, rozpakowanie sprzętu, podłączenie na wskazanych przez Zamawiającego stanowiskach roboczych, konfiguracja ustawień sieci komputerowej. Instalacja i konfiguracja niezbędnego oprogramowania, testy działania.
3. Dostawa licencji na oprogramowanie.
4. Instalacja systemu ZSI wraz z bazą danych na serwerze i stacjach roboczych wskazanych przez Zamawiającego.
5. Konfiguracja i uruchomienie połączeń do systemu ZSI w oddziałach zamiejscowych.
6. Konfiguracja, uruchomienie i testy zadań wykonujących kopie zapasowe.
7. Konfiguracja systemu ZSI zgodnie z ustaleniami analizy przedwdrożeniowej.
8. Podłączenie do systemu LIS urządzeń, na których są wykonywane badania laboratoryjne (analizatory). Podłączenie ma umożliwiać komunikację z analizatorem, co najmniej w zakresie odbioru i automatycznego zapisu w systemie wyników badań. Lista analizatorów do podłączenia z systemem LIS: Mindray BC-3200, Mindray Bs-120, Urometer 120, Koagulometr K-3002 Optic, i-Chrome.
9. Migracja danych z obecnego systemu informatycznego ze szczególnym uwzględnieniem ochrony danych osobowych/wrażliwych znajdujących się w obecnym systemie.
10. Migracja z dotychczas używanego systemu KAMSOFT S.A. KS-PPS ma objąć zakres danych niezbędny do prawidłowej pracy w nowym systemie. Zapewniona będzie po podpisaniu umowy pełna dostępność do bazy danych dla wybranego Wykonawcy.
11. Wszelkie koszty związane z migracją należy uwzględnić w ofercie (w tym koszty uzyskania niezbędnej wiedzy, dokumentacji, oprogramowania, prac programistyczno-wdrożeniowych, przygotowania odpowiednich interfejsów). Należy uwzględnić koszty prac do wykonania po stronie systemu obecnie używanego i docelowego. Zamawiający nie posiada praw autorskich do obecnego systemu, ani kodów źródłowych.
12. Zakres danych do przeniesienia:

- pełne dane pacjentów łącznie z adresami, kodami terytorialnymi,

- dane pracowników,

- dane placówek zewnętrznych kierujących pacjentów,

- dane personelu zewnętrznego kierującego pacjentów,

- deklaracje POZ,

- zrealizowane usługi,

- wszystkie dane niezbędne do kontynuowania i zapewnienia ciągłości rozliczeń z NFZ, możliwością wykonywania korekt do 5 lat wstecz, bez konieczności używania obecnego systemu, możliwe jest uzyskanie wszystkich plików z raportami o wykonanych świadczeniach ambulatoryjnych i szpitalnych (SWIAD) i komunikatami zwrotnymi do tych raportów, plików z deklaracjami POZ (DEKL) oraz raportami zwrotnymi, pliki z szablonami i rachunkami,

- listy pacjentów ewidencjonowanych w kolejkach oczekujących,

- dane ze skierowań,

- dane z wystawionych recept z możliwością kopiowania recepty,

- rozpoznania zarejestrowane pacjentom,

- daty wizyt pacjenta – z możliwością podglądu wprowadzonej dokumentacji medycznej z wybranej przez lekarza wizyty

- zapisane Historie Zdrowia i Choroby.

Dane muszą być przeniesione w sposób umożliwiający wyszukiwanie i sortowanie – nie mogą być przeniesione w postaci plików formatów graficznych, zrzutów ekranowych itp.

Wymagane jest przeprowadzenie dwóch importów danych do nowego systemu:

- testowego w celu weryfikacji importu danych do nowego systemu w terminie do 2 tygodni od daty podpisania umowy,

- importu do nowego systemu produkcyjnego w terminie uzgodnionym podczas analizy przedwdrożeniowej, termin nie może przekroczyć daty startu produkcyjnego systemu.

1. Uruchomienie platformy e-usług dla pacjentów wraz z podłączeniem do ZSI.
2. Uruchomienie dostępu dla aplikacji mobilnych wraz z podłączeniem do ZSI.
3. Szkolenie użytkowników:

System dla przychodni i e-usługi – minimum 40 roboczogodzin,

System dla laboratorium – minimum 16 roboczogodzin.

Szczegółowy harmonogram szkoleń zostanie ustalony i zatwierdzony przez Zamawiającego podczas analizy przedwdrożeniowej.

Szkolenia zostaną przeprowadzone w siedzibie Zamawiającego w dniach poniedziałek-piątek w godz. 8-15.

1. Start produkcyjny systemu.
2. Nadzór techniczny (bezpośrednio po starcie produkcyjnym, na miejscu w siedzibie Zamawiającego):

System dla przychodni i e-usługi – minimum 40 roboczogodzin,

System dla laboratorium – minimum 16 roboczogodzin.

Szczegółowy harmonogram nadzoru technicznego zostanie ustalony i zatwierdzony przez Zamawiającego podczas analizy przedwdrożeniowej.

## Próbka systemu

Wymagane dołączenie do oferty próbki systemu w postaci obrazu wirtualnego, umożliwiającego samodzielne przez Zamawiającego uruchomienie środowiska wg załączonej instrukcji.

Próbka musi być zgodna ze wszystkimi wymaganiami przedstawionymi w Zamówieniu.

Próbka nie może być pusta i musi posiadać min. 30 rekordów pacjentów i min. 5 pracowników medycznych (w tym lekarzy) wraz z przykładową strukturą organizacyjną placówki medycznej (przychodnia i laboratorium).

Pacjenci muszą posiadać zapisaną historię zdrowia i choroby.

Próbka musi być w formie niezmiennej od daty złożenia oferty i musi w pełni umożliwiać zademonstrowanie działania ZSI zgodnie z SIWZ. Próbka nie może być dostarczona jako link do strony internetowej/serwera itd.

Próbka nie może być dostarczona w formie prezentacji poglądowej.

Próbka ma zawierać w pełni działający, oferowany system.

Wykonawca zobowiązuje się na wezwanie Zamawiającego do przeprowadzenia prezentacji systemu na załączonej do oferty próbce – prezentacja ma się odbyć w terminie do 5 dni roboczych od wezwania przez Zamawiającego, czas trwania prezentacji do 6 godzin roboczych.

Brak w próbce jakiejkolwiek funkcji systemu zapisanej w SIWZ powoduje odrzucenie oferty w całości.

## Infrastruktura sprzętowa

### Serwer bazy danych z UPS – 1szt.

|  |  |
| --- | --- |
| Obudowa | -Typu Rack, wysokość maksymalna 1U;-Dostarczona wraz z szynami umożliwiającymi wysunięcie serwera z szafy rack |
| Płyta główna | -Dwuprocesorowa, wyprodukowana i zaprojektowana przez producenta serwera,możliwość instalacji procesorów dwunastordzeniowych;-Sumarycznie minimum 4 złącza PCI Express generacji 3 low profile, w tym minimum 2 złącza o prędkości x16 i 2 złącza o prędkości x8; -Możliwość integracji dedykowanej, wewnętrznej pamięci flash przeznaczonej dla wirtualizatora lub systemu operacyjnego o pojemności do 128GB (niezależne od dysków twardych); |
| Procesor  | -Zainstalowany jeden procesor 8-rdzeniowy w architekturze x86, bazowa częstotliwość procesora min. 2.10 GHz, liczba wątków min. 10, Cache min. 20 MB Cache.  |
| Pamięć RAM | -Zainstalowane 16 GB pamięci RAM typu DDR4 Registered, 2400Mhz -Wsparcie dla technologii zabezpieczania pamięci Advanced ECC, Memory Scrubbing, SDDC;-12 gniazd pamięci RAM na płycie głównej |
| Interfejsy sieciowe | -Karta LAN wyposażona minimum w interfejsy: 2x 1Gb/s LAN, ze wsparciem iSCSI i iSCSI boot i teamingu, RJ-45; |
| Dyski wewnętrzne | -Zainstalowane 4 dyski SAS 3.0 10K RPM SAS o pojemności 600 GB każdy, dyski Hotplug;-Minimum 4 wnęki dla dysków twardych Hotplug 3,5; |
|  Wspierane systemy operacyjne | Microsoft Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise, VMware |
| Porty | -zintegrowana karta graficzna ze złączem VGA;-5x USB, w tym minimum 2x USB 3.0 na panelu przednim, minimum 2x USB 3.0 dostępne z tyłu, 1x USB dostępne wewnątrz; Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera;-możliwość rozbudowy serwera o złącze 1x RS-232-C; |
| Zasilanie | -Redundantne zasilacze hotplug o sprawności 94% (tzw klasa Platinum) o mocy maksymalnej 450W; -Redundantne wentylatory hotplug; |
| Zarządzanie | - Wbudowane diody informujące o stanie serwera;-Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:• Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;• Dedykowana karta LAN 1 Gb/s (dedykowane złącze RJ-45 z tyłu obudowy) do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;• Dostęp poprzez przeglądarkę Web (także SSL, SSH)• Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii• Zarządzanie alarmami (zdarzenia poprzez SNMP)• Możliwość przejęcia konsoli tekstowej• Opcjonalne przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM)• Sprzętowy monitoring serwera w tym stanu dysków twardych i kontrolera RAID (bez pośrednictwa agentów systemowych) • Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.). |
| Gwarancja | 5 lat gwarancji w miejscu instalacji serwera |
| Dokumentacja, inne | -Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA (wymagane oświadczenie producenta serwera potwierdzające spełnienie wymagań dołączone do oferty).-Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w Polsce - Wymagane oświadczenie producenta serwera, że oferowany do przetargu sprzęt spełnia ten wymóg;-Oferent zobowiązany jest dostarczyć wraz z ofertą kartę produktową oferowanego serwera umożliwiającą weryfikację parametrów oferowanego sprzętu;-Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, (ogólnopolski numer o zredukowanej odpłatności 0-800/0-801, w ofercie należy podać nr telefonu) w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;-Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; |
| UPS | Min. 1500 V/1000W, line-interactive, czas przełączania na baterię 4 ms, gniazda utrzymania zasilania 4 x IEC320 C13 (10A) + 1x16A, złącze USB, oprogramowania zarządzające, obudowa Rack, gwarancja 24 miesiące producenta |

### Serwer aktualizacji/serwer terminali z UPS – 1szt.

|  |  |
| --- | --- |
| Obudowa | -obudowa typu Rack -wysokość nie więcej niż 1U-dostarczony wraz z szynami montażowymi do szafy rack |
| Płyta główna | -dedykowana serwerowa, wyprodukowana i zaprojektowana przez producenta serwera-minimum 3 sloty PCI Express w tym minimum 2 sloty generacji 3 o prędkości x8;-minimum 4 gniazda pamięci RAM DDR4 |
| Procesor  | -zainstalowany procesor osiągający w testach wydajności SPECint\_rate2006 min. 202 pkt.-Wymagane dołączenie do oferty pełnego protokołu testów SPEC dla oferowanego modelu serwera wyposażonego w oferowane procesory, protokół poświadczony przez producenta serwera; |
| Pamięć RAM | -nie mniej niż 8GB RAM DDR4-2133MHz -zabezpieczenie pamięci mechanizmem ECC-możliwość rozbudowy do minimum 64 GB RAM |
| Interfejsy sieciowe | Minimum 1 interfejs (fizyczny) 10Gb Ethernet |
| Dyski wewnętrzne | Min 2 dyski twarde o pojemności min 500 GB |
| Porty | -Minimum 6 portów USB 3.0 w tym 2 porty USB z przodu obudowy, minimum 4 porty w standardzie USB 3.0 z tyłu-port szeregowy, minimum dwa porty RJ45 -nie dopuszcza się stosowania przejściówek, adapterów oraz rozgałęziaczy i przedłużaczy. |
| Zasilacz | - zasilacz o mocy maksymalnej nie więcej niż 460W, o maksymalnej sprawności minimum 94%-nadmiarowy układ chłodzenia (redundancja typu N+1) |
| Zarządzanie zdalne, inwentaryzacja | Umieszczona z przodu chowana karta identyfikacyjna serwera zawierająca nazwę serwera, numer handlowy, numer seryjny, adresy MAC kart sieciowych-Zintegrowany trwale z płytą główną kontroler zdalnego zarządzania zgodny ze standardem IPMI 2.0 umożliwiający: • zdalne uruchomienie, wyłączenie i restart serwera, pełne zarządzanie sprzętowe: monitorowanie pracy kluczowych układów, wentylatorów, zasilaczy, napędów, temperatur, itp., logowanie błędów w zakresie ustalonym przez administratora• dostęp do interfejsu karty zarządzającej za pomocą przeglądarki MS Internet Explorer lub Mozilla Firefox bez konieczności instalowania jakiegokolwiek software specyficznego dla producenta sprzętu• Opcjonalne przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów (CD, DVD, FDD, klucz USB) i ich obrazów na poziomie sprzętowym (cyfrowy KVM)• Sprzętowy monitoring serwera w tym stanu dysków twardych i kontrolera RAID (bez pośrednictwa agentów systemowych) • połączenie z kartą zarządzającą musi być szyfrowane minimum 128 bitowym kluczem SSL• monitorowanie zużycia energii serwera w trybie rzeczywistym i wizualizacja raportów w postaci wykresów graficznych,• dedykowana karta LAN 1 Gb/s do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym serwera. • możliwość konfiguracji 16 niezależnych kont administracyjnych (dostępowych) do karty zarządzającej, logowanie aktywności użytkowników, wsparcie dla integracji z Active Directory i LDAP• wsparcie dla aktualizacji firmware karty zarzadzającej online, bez konieczności restartu serwera |
|  Wspierane systemy operacyjne | Microsoft Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise, VMware |
| Gwarancja | 5 lat w miejscu instalacji serwera |
| Inne | -Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane (wymagane oświadczenie producenta dołączone do oferty) oraz muszą być objęte gwarancją producenta, potwierdzoną przez oryginalne karty gwarancyjne;-Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w Polsce - Wymagane oświadczenie producenta serwera, że oferowany do przetargu sprzęt spełnia ten wymóg;-Oferent zobowiązany jest dostarczyć wraz z ofertą kartę produktową oferowanego serwera umożliwiającą weryfikację parametrów oferowanego sprzętu;-Ogólnopolska, telefoniczna infolinia/linia techniczna producenta komputera, (ogólnopolski numer o zredukowanej odpłatności 0-800/0-801, w ofercie należy podać nr telefonu) w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;-Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; |
| UPS | Min. 1000 V/600W, ilość gniazd wyjściowych Min. 4 x IEC320, złącze USB, obudowa wieżowa. Gwarancja producenta na elektronikę min. 24 miesiące, na akumulatory min. 12 miesięcy. Zasilacz powinien posiadać: Odporność na przeciążenia, Synchronizacja z siecią, dźwiękowa sygnalizacja rozładowania baterii. Czas podtrzymania przy obciążeniu 50% - 13 minut. |

### Stanowisko komputerowe – 20 szt.

|  |  |
| --- | --- |
| Typ | Komputer stacjonarny. |
| Procesor | Procesor klasy x86 lub szybszy zaprojektowany do pracy w komputerach stacjonarnych.Osiągający w teście Passmark CPU Mark średni wynik przynajmniej 3386. Do oferty należy dołączyć wydruk ze strony: http://cpubenchmark.net/cpu\_list.php |
| Zainstalowana pamięć RAM | Minimum 4 GBDDR4 |
| Dysk twardy | Pojemność minimum 120 GB.  |
| Karta graficzna | Grafika zintegrowana z płytą główną |
| Karta sieciowa | Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną.  |
| Napęd | Nagrywarka DVD +/-RW |
| Karta sieciowa | 10/100/1000 Ethernet RJ-45, zintegrowana z płytą główną |
| Karta dźwiękowa | Karta dźwiękowa zintegrowana z płytą główną |
| Porty na panelu przednim | 2x USB 2.0, 2x Audio. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, kart rozszerzeń itp. |
| Porty | Minimum 1 x VGA, Minimum 1 x HDMI, Minimum 1 x DVI |
| Klawiatura | Klawiatura USB w układzie polski programisty - trwale oznaczona logo producenta jednostki centralnej |
| Mysz | Mysz optyczna USB z dwoma przyciskami oraz rolką (scroll) trwale oznaczona logo producenta jednostki centralnej + podkładka pod mysz |
| System operacyjny | System operacyjny klasy PC nie wymagający aktywacji za pomocą telefonu lub Internetu, spełniający następujące wymagania poprzez natywne dla niego mechanizmy, bez użycia dodatkowych aplikacji:Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek;Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu;Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat)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 komputerInterfejs 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.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.Funkcje związane z obsługą komputerów typu TABLET PC, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego.Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika.Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.Wbudowany system pomocy w języku polskim;Wdrażanie IPSEC oparte na politykach – wdrapanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji;System posiada 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 2.0 , 3.0 , 3.5 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach;Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń;Graficzne środowisko instalacji i konfiguracji;Transakcyjny system plików pozwalający na stosowanie przydziałów na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe;Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogoweOprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej;Możliwość przywracania plików systemowych;System operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.)Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).Telefoniczne wsparcie techniczne w języku polskim w dni robocze od 8:00 do 17:00 zapewniony przez producenta lub dostawcę co najmniej przez 5 lat od chwili zakupuNa dysku twardym dedykowana partycja umożliwiająca szybkie odtworzenie fabrycznie skonfigurowanej wersji systemu (Recovery).Licencja systemu operacyjnego musi pochodzić z oficjalnego kanału dystrybucyjnego w Polsce, musi być nowa, a klucz nigdy wcześniej nie wykorzystywany ani aktywowany. |
| Certyfikaty i standardy | - Certyfikat ISO 9001:2015 na projektowanie i produkcje dla producenta sprzętu (załączyć dokument potwierdzający spełnianie wymogu)- Certyfiakt ISO 14001:2015 dla producenta sprzętu (załączyć dokument potwierdzający spełnianie wymogu)- Deklaracja zgodności CE (załączyć do oferty)- 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 (załączyć oświadczenie producenta). |
| Serwis i gwarancja | 3-letnia gwarancja producenta.Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera - dokumenty potwierdzające załączyć do oferty. |
| Wsparcie techniczne producenta | Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego oficjalnego przedstawiciela w Polsce.Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego - do oferty należy dołączyć link strony. |

### Monitor – 9 szt.

|  |  |
| --- | --- |
| Wielkość przekątnej ekranu/ Format | Minimum 19.5” |
| Podświetlenie | LED |
| Wielkość plamki | Maksimum 0.26 mm |
| Rozdzielczość | Min. 1600x900 pikseli przy 60 Hz |
| Częstotliwość (H/V) | 30-83KHz |
| Jasność | Minimum 200 cd/m2  |
| Czas odpowiedzi | Maximum 5 ms |
| Złącza minimum | 1x 15-stykowe złącze D-Sub,  |
| Gwarancja | 36  miesięcy |

### Urządzenie wielofunkcyjne sieciowe – 3szt.

|  |  |
| --- | --- |
| Prędkość druku | Min 40 str./min. |
| Rozdzielczość druku | Min 1200x1200dpi |
| Typ urządzenia | Mono |
| Funkcje | Urządzenie musi umożliwiać drukowanie, kopiowanie i skanowanie |
| Wyświetlacz | Wyświetlacz dotykowy, kolorowy |
| Pamięć | Min. 256MB |
| Technologia druku | Laserowa |
| Procesor | Min. 800 MHz |
| Połączenie | USB2.0, Ethernet (10Base-T/100Base-TX) |
| Materiały eksploatacyjne | Urządzenie musi umożliwiać montaż tonerów o dużej wydajności min. 8000 stron. W zestawie z urządzeniem musi być dostarczony toner o wydajności min. 2000 stron. |
| Gwarancja | 36  miesięcy |

### Urządzenie wielofunkcyjne gabinet – 9 szt.

|  |  |
| --- | --- |
| Prędkość druku | Min 40 str./min. |
| Rozdzielczość druku | Min 1200x1200dpi |
| Typ urządzenia | Mono |
| Funkcje | Urządzenie musi umożliwiać drukowanie, kopiowanie i skanowanie |
| Wyświetlacz | Wyświetlacz dotykowy, kolorowy |
| Pamięć | Min. 256MB |
| Technologia druku | Laserowa |
| Procesor | Min. 800 MHz |
| Połączenie | USB2.0, Ethernet (10Base-T/100Base-TX) |
| Materiały eksploatacyjne | Urządzenie musi umożliwiać montaż tonerów o dużej wydajności min. 8000 stron. W zestawie z urządzeniem musi być dostarczony toner o wydajności min. 2000 stron. |
| Gwarancja | 36  miesięcy |

### Stanowisko mobilne (tablet) – 1szt.

|  |  |
| --- | --- |
| Przekątna ekranu | Tablet z ekranem o przekątnej 255.4 mm (10,1") WUXGA (1920 x 1200) z interfejsem dotykowym. |
|
|  Rozdzielczość | 1920x1200 pikseli |
| Pamięć | 16GB |
| RAM | 2GB |
| Czytnik kart pamięci | microSD |
| Wyposażenie multimedialne | Wbudowana z przodu w obudowę kamera CMOS 2 MP z tyłu obudowy kamera CMOS 8 MP |
| Procesor | Procesor 8 rdzeniowy, zaprojektowany do pracy w tabletach, min. 1.6GHz |
| Interfejs | Wi-fi (802.11 a/b/g/n/ac), bluetooth, USB, LTE |
| Czujnik | Akcelerometr, Czujnik pola magnetycznego, Czujnik koloru RGB |
| Gwarancja | 36  miesięcy |

### Macierz dyskowa – 1szt.

|  |  |
| --- | --- |
| Procesor | Taktowanie zegara nie mniejsze niż 2.0GHz |
|
| Procesor liczba rdzeni | Nie mniej niż 4 |
| Pamięć RAM | Nie mniej niż 2GB |
| Pamięć RAM liczba slotów | Minimum 2 sloty |
| Pamięć RAM możliwość rozszerzenia | Nie mniej niż do 8GB |
| Pamięć Flash | Nie mniej niż 512MB |
| Liczba zatok na dyski twarde | Minimum 2 |
| Obsługiwane dyski twarde | 3.5" oraz 2.5" SATAZainstalowane dwa dyski twarde 3,5” 4TB |
| Porty LAN | Minimum 2 Gigabit Ethernet |
| Diody LED | Status, LAN, USB, HDD, |
| Złącza | Min. 2xUSB2.0, 2xUSB3.0, 1xHDMI |
| Typ obudowy | Tower |
| Zabezpieczenia | FTP z SSL/TLS (Explicit)Obsługa SFTP (tylko admin)Szyfrowanie AES 256-bitSzyfrowana zdalna replikacja (Rsync poprzez SSH)Import certyfikatu SSLPowiadomienia o zdarzeniach za pośrednictwem Email i SMS |
| Wirtualizacja | Możliwość uruchomienia maszyn wirtualnych z systemami Windows, Linux, Unix, Android bezpośrednio na urządzeniu bez wymogu zewnętrznego hosta wirtualizacji |
| Gwarancja | 36  miesięcy |

### System do backupu – 1szt.

|  |  |
| --- | --- |
| Rodzaj napędu | Zewnętrzny (jeden napęd + 4szt. wymiennych nośników) |
|
| Pojemność nośnika | 1TB |
| Format plików | NTFS/FAT |
| Liczba nośników | 4 szt. |
| Typ nośnika | RDX |
| Średni czas wyszukiwania / czas dostępu  | 15 ms |
| Interfejs | USB 3.0 |
| Oprogramowanie | TAK |
| Gwarancja | 36  miesięcy |

### Czytnik kodów kreskowych – 5szt.

|  |  |
| --- | --- |
| Rodzaj czytnika | Ręczny |
|
| Interfejs  | USB |
| Norma odporności (IP) | IP42 |
| Obsługiwane kody kreskowe | 1D, Postal (pocztowe), GS1 Databar, 2D |
| Bezpieczny upadek na twardą pow. [m] | 1.5m |
| Przycisk wyzwalający | TAK |
| Gwarancja | 36 miesięcy |

### Szafa z wyposażeniem.

|  |  |
| --- | --- |
| Rodzaj szafy | 19”, 27U, drzwi szklane z zamkiem, drzwi boczne demontowane – 1 szt. |
|
| Wyposażenie dodatkowe | Półki do szafy – 2szt., listwa zasilająca – 1szt. |
| Switch | RACK 48x10/100/1000 BaseTx (możliwe 2 szt. x24 porty) – 1 szt. |

## Oprogramowanie systemowe i narzędziowe.

### System operacyjny serwera – 2szt.

|  |  |
| --- | --- |
| System operacyjny | Microsoft Windows Server Standard 2012R2 lub równoważny. |
|

### Oprogramowanie dostępowe do serwera – 25 szt.

|  |  |
| --- | --- |
| Licencja dostępowa | Licencje dostępowe w celu podłączenia do systemu serwerowego – licencja na urządzenie |
|

### Oprogramowanie dla dostępu zdalnego do serwera – 8 szt.

|  |  |
| --- | --- |
| Licencja dostępowa zdalna | Licencje dostępowe zdalne w celu podłączenia do systemu domenowego – licencja na urządzenie |
|

### Oprogramowanie antywirusowe – 30 szt.

|  |  |
| --- | --- |
| Ogólne | 1. Licencja ważna 36 miesięcy
2. Pełne wsparcie dla systemu Windows XP SP3/Vista/Windows 7/Windows8/Windows 8.1/Windows 8.1 Update/10
3. Wsparcie dla 32- i 64-bitowej wersji systemu Windows.
4. Wersja programu dla stacji roboczych Windows dostępna zarówno w języku polskim jak i angielskim.
5. Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim.
6. Skuteczność programu potwierdzona nagrodami VB100 i AV-comparatives
 |
| Ochrona antywirusowa i antyspyware | 6. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.7. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.8. Wbudowana technologia do ochrony przed rootkitami.9. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.10. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.11. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.12. System ma oferować administratorowi możliwość definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym i jeśli tak – nie wykonywało danego zadania.13. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).14. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.15. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.16. Możliwość skanowania dysków sieciowych i dysków przenośnych.17. Skanowanie plików spakowanych i skompresowanych.18. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.19. Wykluczenie ze skanowania musi odbywać się nie tylko po nazwie pliku ale również ma być możliwe użycie symbolu wieloznacznego „\*” zastępującego dowolne znaki w ścieżce.20. Administrator ma możliwość dodania wykluczenia po tzw. HASH’u zagrożenia, wskazującego bezpośrednio na określoną infekcję a nie konkretny plik.21. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.22. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu. 23. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera.24. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.25. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.26. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.27. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego).28. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.29. Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 30. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.31. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.32. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.33. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Program musi umożliwić blokowanie danej strony internetowej po podaniu na liście całej nazwy strony lub tylko wybranego słowa występującego w nazwie strony.34. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora.35. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. 36. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.37. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.38. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta.39. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.40. Program musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.41. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym.42. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego. 43. W przypadku gdy stacja robocza nie będzie posiadała dostępu do sieci Internet ma odbywać się skanowanie wszystkich procesów również tych, które wcześniej zostały uznane za bezpieczne.44. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.45. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń mają być wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.46. Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika.47. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia. 48. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.49. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.50. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła.51. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło.52. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.53. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i administratora wraz z listą niezainstalowanych aktualizacji.54. Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.55. Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów.56. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.57. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.58. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM , urządzeń przenośnych oraz urządzeń dowolnego typu.59. Funkcja blokowania nośników wymiennych bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model.60. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia, dana funkcjonalność musi pozwalać na automatyczne wypełnienie właściwości urządzenia dla tworzonej reguły.61. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie brak dostępu do podłączanego urządzenia.62. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.63. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.64. Użytkownik ma posiadać możliwość takiej konfiguracji programu aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika65. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).66. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:• tryb automatyczny z regułami gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,• tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,• tryb oparty na regułach gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,• tryb uczenia się, w którym program uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach.• Tryb inteligentny – w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach.67. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.68. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.69. Oprogramowanie musi posiadać zaawansowany skaner pamięci.70. Program musi być wyposażona w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp.71. Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach.72. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa.73. Program ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie. 74. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.75. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami.76. Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji program zgłosi posiadanie nieaktualnej bazy sygnatur.77. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji.78. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http79. Program musi być wyposażona w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback).80. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).81. Program ma być w pełni zgodny z technologią CISCO Network Access Control.82. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełno ekranowym.83. W momencie wykrycia trybu pełno ekranowego aplikacja ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań aplikacji.84. Użytkownik ma mieć możliwość skonfigurowania programu tak aby automatycznie program włączał powiadomienia oraz zadania pomimo pracy w trybie pełnoekranowym po określonym przez użytkownika czasie.85. Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, kontroli stron Internetowych i kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania.86. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.87. Program musi posiadać możliwość utworzenia z poziomu interfejsu aplikacji dziennika diagnostycznego na potrzeby pomocy technicznej.88. Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline.89. Możliwość podejrzenia licencji za pomocą, której program został aktywowany. 90. W programie musi istnieć możliwość tymczasowego wstrzymania polityk wysłanych z poziomu serwera zdalnej administracji.91. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej.92. Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas po którym automatycznie zostają przywrócone dotychczasowe ustawienia.93. Administrator ma możliwość wstrzymania polityk na 10 min, 30 min, 1 godzinę i 4 godziny94. Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika.95. Program musi posiadać opcję automatycznego skanowania komputera po dokonaniu zmian z użyciem opcji wstrzymania polityki.96. Aplikacja musi posiadać funkcję ręcznej aktualizacji komponentów programu.97. Możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych.98. Program musi posiadać możliwość definiowana stanów aplikacji, jakie będą wyświetlane użytkownikowi np. powiadomień o wyłączonych mechanizmach ochrony czy stanie licencji.99. Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie. |
| Ochrona serwera plików Windows | 1. Wsparcie dla systemów: Microsoft Windows Server 2003, 2008, 2008 R2, 2012, 2012 R2, 2016 SBS 2003, SBS 2003 R2, SBS 2008, SBS 2011, Microsoft MultiPoint Server 2010, Microsoft MultiPoint Server 2011, Windows MultiPoint Server 2012.2. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.3. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.4. Wbudowana technologia do ochrony przed rootkitami i exploitami.5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.6. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.7. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu. Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).8. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.9. System antywirusowy ma mieć możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.10. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych.11. Użytkownik ma mieć możliwość zmiany ilości wątków skanowania w ustawieniach systemu antywirusowego.12. Możliwość skanowania dysków sieciowych i dysków przenośnych.13. Skanowanie plików spakowanych i skompresowanych.14. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.15. Program musi posiadać funkcjonalność pozwalającą na ograniczenie wielokrotnego skanowania plików w środowisku wirtualnym za pomocą mechanizmu przechowującego informacje o przeskanowanym już obiekcie i współdzieleniu tych informacji z innymi maszynami wirtualnymi.16. Aplikacja powinna wspierać mechanizm klastrowania.17. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).18. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS.19. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.20. Program ma umożliwiać użytkownikowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: pamięci masowych, płyt CD/DVD i pamięci masowych FireWire.21. Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model. 22. Aplikacja musi posiadać funkcjonalność, która automatycznie uzupełni elementy wymagane dla tworzenia reguł w oparciu o informacje dostępne z aktualnie podłączonego nośnika.23. Aplikacja ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, brak dostępu do podłączanego urządzenia.24. Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.25. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.26. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.27. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony.28. Dodanie automatycznych wyłączeń nie wymaga restartu serwera.29. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych.30. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji.31. W przypadku restartu serwera – usunięte z listy wyłączeń elementy mają być automatycznie uzupełnione.32. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego. 33. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line).34. Możliwość przeniesienia zainfekowanych plików w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.35. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.36. Możliwość skanowania wyłącznie z zastosowaniem algorytmów heurystycznych tj. wyłączenie skanowania przy pomocy sygnatur baz wirusów.37. Aktualizacje modułów analizy heurystycznej.38. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.39. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia. 40. Wysyłanie zagrożeń do laboratorium ma być możliwe z serwera zdalnego zarządzania i lokalnie z każdej stacji roboczej w przypadku komputerów mobilnych.41. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.42. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.43. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e mail.44. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy serwerze przy próbie dostępu do konfiguracji systemu antywirusowego był proszony o podanie hasła.45. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program ma pytać o hasło.46. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji ma być takie samo.47. System antywirusowy ma być w pełni zgodny z technologią CISCO NAC.48. System antywirusowy ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji.49. System antywirusowy ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie. Program ma także posiadać opcję dezaktywacji tego mechanizmu.50. Po instalacji systemu antywirusowego, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów.51. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.52. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.53. Program powinien umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: nośników CD/DVD oraz urządzeń USB.54. System antywirusowy ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach.55. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa.56. System antywirusowy ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie. 57. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.58. Aktualizacja dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP).59. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.60. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja). 61. Do każdego zadania aktualizacji można przypisać dwa różne profile z innym ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja). Przykładowo, domyślny profil aktualizuje z sieci lokalnej a w przypadku jego niedostępności wybierany jest profil rezerwowy pobierający aktualizację z Internetu.62. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 63. Aplikacja musi wspierać skanowanie magazynu Hyper-V64. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów65. Wykluczenie ze skanowania musi odbywać się nie tylko po nazwie procesu ale również ma być możliwe użycie symbolu wieloznacznego „\*” zastępującego dowolne znaki.66. Administrator ma możliwość dodania wykluczenia po tzw. HASH’u zagrożenia, wskazującego bezpośrednio na określoną infekcję a nie konkretny plik.67. Praca programu musi być niezauważalna dla użytkownika.68. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania.69. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. |
| Administracja zdalna | 1. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2003, 2008, 2012 oraz systemach Linux.2. Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance).3. Serwer administracyjny musi wspierać instalację w oparciu o co najmniej bazy danych MS SQL i MySQL.4. Serwer administracyjny musi oferować możliwość wykorzystania już istniejącej bazy danych MS SQL lub MySQL użytkownika.5. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji i konsoli w postaci jednego pakietu instalacyjnego lub każdego z modułów oddzielnie bezpośrednio ze strony producenta.6. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej.7. Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy występujące w sieci.8. Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6.9. Podczas logowania administrator musi mieć możliwość wyboru języka w jakim zostanie wyświetlony panel zarządzający.10. Zmiana języka panelu administracyjnego nie może wymagać zatrzymania lub reinstalacji oprogramowania zarządzającego.11. Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL.12. Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.13. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.14. Jeden centralny serwer centralnego zarządzania bez względu na wielkość sieci.15. Instalacja serwera administracyjnego powinna oferować wybór trybu pracy serwera w sieci w przypadku rozproszonych sieci –serwer pośredniczący (proxy) lub serwer centralny.16. Serwer proxy musi pełnić funkcję pośrednika pomiędzy lokalizacjami zdalnymi a serwerem centralnym.17. Serwer proxy musi być wyposażony we własną bazę danych, w której będą przechowywane dane z agentów na wypadek braku połączenia z serwerem centralnym.18. Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM.19. Serwer administracyjny musi oferować możliwość instalacji serwera http proxy pozwalającego na pobieranie aktualizacji baz sygnatur oraz pakietów instalacyjnych na stacjach roboczych bez dostępu do Internetu.20. Serwer http proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) najczęściej pobieranych elementów.21. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.22. Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy.23. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na stacjach roboczych z systemami Windows, Mac OS X oraz Linux oraz serwerach Windows.24. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na urządzeniach mobilnych z systemem Android.25. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware’ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci.26. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.27. Administrator musi posiadać możliwość zarządzania za pomocą dedykowanego agenta stacjami nie posiadającymi zainstalowanego programu zabezpieczającego.28. Agent musi przekazywać informacje na temat stanu systemu operacyjnego do serwera administracji zdalnej29. Agent musi posiadać możliwość pobrania listy zainstalowanego oprogramowania firm trzecich na stacji roboczej z możliwością jego odinstalowania.30. Serwer administracyjny musi oferować możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.31. Instalacja agenta musi odbywać się przy wykorzystaniu repozytorium producenta. Repozytorium powinno zawierać aktualne wersje agentów bez względu na rodzaj systemu operacyjnego.32. Instalacja agenta nie może wymagać określenia typu systemu (32 lub 64 – bitowy) oraz jego rodzaju (Windows, Mac, itp) a dobór odpowiedniego pakietu musi być w pełni automatyczny.33. Instalacja klienta na urządzeniach mobilnych musi być dostępna za pośrednictwem portalu WWW udostępnionego przez moduł MDM z poziomu urządzenia użytkownika.34. W przypadku braku zainstalowanego klienta na urządzeniu mobilnym musi istnieć możliwość jego pobrania ze sklepu Google Play.35. Administrator musi posiadać możliwość utworzenia listy zautoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.36. Serwer administracyjny musi oferować możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, nie komunikację za pośrednictwem wiadomości SMS.37. Serwer administracyjny musi oferować możliwość utworzenia polityk konfiguracji dla aplikacji zabezpieczającej na urządzeniu mobilnym.38. Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi.39. Administrator musi posiadać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli zarządzającej40. Dwu fazowa autoryzacja musi się odbywać za pomocą wiadomości SMS lub haseł jednorazowych generowanych na urządzeniu mobilnym za pomocą dedykowanej aplikacji.41. Administrator musi posiadać możliwość utworzenia użytkownika wbudowanego lub zintegrowanego z grupą z usługi Active Directory.42. Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp.43. Administrator musi posiadać możliwość nadania dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko do odczytu, odczyt/zapis.44. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.45. Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta bez konieczności logowania się do panelu administracyjnego.46. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności po jakim użytkownik zostanie automatycznie wylogowany.47. Dostępne zadania muszą być podzielone na dwie grupy: zadania klienta oraz zadania serwera.48. Zadania serwera obejmujące zadanie instalacji agenta, generowania raportów oraz synchronizacji grup.49. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej.50. Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji.51. Serwer administracyjny musi w przejrzysty sposób informować administratora o elementach zadań jakie są wymagane do jego uruchomienia a w przypadku jego braku wskazywać brakujące elementy konfiguracji.52. Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym.53. Serwer administracyjny musi oferować możliwość wyboru parametrów pakietu instalacyjnego zależnych od systemu operacyjnego oraz licencji na program zabezpieczający.54. Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu.55. Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką.56. Serwer administracyjny musi oferować możliwość utworzenia jednego zadania dla kilku klientów lub grupy.57. Serwer administracyjny musi oferować możliwość uruchomienia zadania automatycznie zgodnie z harmonogramem, po wystąpieniu nowego dziennika zdarzeń lub umieszczeniu nowego klienta w grupie dynamicznej.58. Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów.59. Grupy dynamiczne tworzone na podstawie szablonu określającego warunki jakie musi spełnić klient aby zostać umieszczony w danej grupie. Przykładowe warunki: Adresy sieciowe IP, Aktywne zagrożenia, Stan funkcjonowania/ochrony, Wersja systemu operacyjnego, itp.60. Serwer administracyjny musi oferować możliwość utworzenia polityk dla programów zabezpieczających i modułów serwera centralnego zarządzania.61. Serwer administracyjny musi oferować możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów. Serwer administracyjny musi oferować możliwość przypisania kilku polityk z innymi priorytetami dla jednego klienta.62. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej.63. Serwer administracyjny musi oferować możliwość nadania priorytetu „Wymuś” dla konkretnej opcji w konfiguracji klienta. Opcja ta nie będzie mogła być zmieniona na stacji klienckiej bez względu na zabezpieczenie całej konfiguracji hasłem lub w przypadku jego braku.64. Serwer administracyjny musi oferować możliwość ukrycia graficznego interfejsu użytkownika na stacji klienckiej i jego uruchomienia tylko przez administratora.65. Serwer administracyjny musi umożliwiać wyświetlenie polityk do których przynależy dana stacja robocza oraz ich edycję z poziomu właściwości samego klienta66. Serwer administracyjny musi oferować możliwość utworzenia własnych raportów lub skorzystanie z predefiniowanych wzorów.67. Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania.68. Serwer administracyjny musi oferować możliwość wyboru formy przedstawienia danych w raporcie w postaci tabeli, wykresu lub obu elementów jednocześnie.69. Serwer administracyjny musi oferować możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy, itp.70. Serwer administracyjny musi oferować możliwość określenia danych jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na elementach wykresu oraz ich odfiltrowania i posortowania.71. Serwer administracyjny musi być wyposażona w mechanizm importu oraz eksportu szablonów raportów.72. Serwer administracyjny powinien posiadać Panel kontrolny z raportami administratora, pozwalający na szybki dostępu do najbardziej interesujących go danych. Panel ten musi oferować możliwość modyfikacji jego elementów.73. Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym dostępnym z poziomu interfejsu konsoli WWW.74. Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub PS.75. Serwer administracyjny musi oferować możliwość skonfigurowania czasu automatycznego odświeżania raportu na panelu kontrolnym oraz umożliwiać jego odświeżenie na żądanie.76. Serwer administracyjny musi oferować możliwość tworzenia wielu zakładek panelu, w których będą widoczne wybrane przez administratora elementy monitorujące.77. Serwer administracyjny musi oferować możliwość maksymalizacji wybranego elementu monitorującego.78. Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.79. Serwer administracyjny musi oferować możliwość utworzenia własnych powiadomień lub skorzystanie z predefiniowanych wzorów.80. Powiadomienia muszą dotyczyć zmiany ilości klientów danej grupy dynamicznej, wzrostu liczby grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń lub skanowania lub stanu obiektu serwer centralnego zarządzania.81. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP.82. Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu.83. Serwer administracyjny musi oferować możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu.84. Serwer administracyjny musi oferować możliwość podłączenia serwera administracji zdalnej do portalu zarządzania licencjami dostępnego na serwerze producenta.85. Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji.86. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty.87. Serwer administracyjny musi oferować możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela.88. Narzędzie administracyjne musi być wyposażone w mechanizm wyszukiwania zarządzanych komputerów na podstawie co najmniej nazwy komputera, adresu IPv4 i IPv6 lub wyszukania konkretnej nazwy zagrożenia.89. Serwer administracyjny musi być wyposażona w machizm autodopasowania kolumn w zależności od rozdzielczości urządzenia na jakim jest wyświetlana.90. Administrator musi mieć możliwość określenia zakresu czasu w jakim dane zadanie będzie wykonywane (sekundy, minuty, godziny, dni, tygodnie).91. Serwer administracji musi umożliwić granulację uprawnień dla Administratorów w taki sposób, aby każdemu z nich możliwe było przyznanie oddzielnych uprawnień do poszczególnych grup komputerów, polityk lub zadań.92. Konfiguracja zestawów uprawnień musi umożliwiać przypisanie praw tylko do odczytu, odczytu i użycia, oraz prawo do zapisania zmian w ramach danego zadania lub polityki w konsoli ERA.93. Konsola webowa musi umożliwiać stronicowanie w widoku komputerów w celu ograniczenia liczby wyświetlanych maszyn na jednej stronie.94. Administrator musi mieć możliwość podłączenia do stacji roboczej z użyciem protokołu RDP bezpośrednio z poziomu konsoli ERA.95. Serwer musi wspierać wysyłanie logów do systemu SIEM IBM qRadar96. Musi istnieć mechanizm, umożliwiający dodawanie reguł do istniejących już w module firewalla lub harmonogramie. Takie reguły można umieścić na początku lub końcu istniejącej listy.97. Konsola administracyjna musi umożliwiać dodanie własnego logotypu do interfejsu webowego. |

## Usługi gwarancyjne

### Zintegrowany System Informatyczny

Okres gwarancji: 36 miesięcy od daty podpisania protokołu końcowego odbioru.

Warunki gwarancji:

1. Udostępnienie aktualnych opisów oprogramowania.
2. Usuwanie wad ukrytych Produktu, ujawnionych po dostarczeniu ZSI - poprzez udostępnienie nowej wersji.
3. Udostępnianie nowych wersji ZSI, poprawiających funkcjonalność i stabilność użytkowania.
4. Utrzymanie zgodności systemu z obowiązującymi przepisami prawnymi.
5. Dostarczenie aplikacji internetowej do przyjmowania i obsługi zgłoszeń.
6. Przyjmowanie zgłoszeń błędów w pierwszej kolejności przez aplikację internetową do obsługi zgłoszeń, telefon lub e-mail.
7. Klasyfikacja błędów:

- błąd krytyczny - oznacza nieprawidłowość ZSI, która powoduje brak możliwości użytkowania ZSI w obrębie ścieżek krytycznych, utraty danych lub ich spójności.

- błąd niekrytyczny – błąd powodujący działanie ZSI w sposób odmienny od instrukcji użytkownika, polegający na braku jednoznaczności opisu danych uzyskiwanych z ZSI.

Czasy usuwania błędów:

|  |  |
| --- | --- |
| Błąd krytyczny | Czas  |
| Czas reakcji | 4 godz. |
| Czas naprawy | 6 godz. |

|  |  |
| --- | --- |
| Błąd niekrytyczny | Czas |
| Czas reakcji | 6 godz. |
| Czas naprawy | 4 dni |

1. Konsultacje dni robocze (poniedziałek-piątek) 8-16, w zakresie użytkowania systemu poprzez internetowy system zgłoszeń, telefon, faks, e-mail).
2. Informowanie o nowych wersjach oprogramowania z opisem dokonywanych zmian – automatyczne na wskazany adres poczty elektronicznej.
3. Na dzień podpisania Protokołu odbioru przedmiotu zamówienia, ZSI musi działa poprawnie i musi być zgodny z obowiązującymi przepisami prawa.

### Sprzęt komputerowy

Okres gwarancji – minimum 36 miesięcy.

Warunki gwarancji:

1. Dostarczony sprzęt jest wolny od wad prawnych oraz od wad fizycznych, produkcyjnych, bądź wynikających z jakiegokolwiek działania lub zaniechania dostawcy.
2. Sprzęt musi być fabrycznie nowy (rok produkcji 2016 lub nowszy).
3. Zgłaszanie uszkodzeń w dni robocze poniedziałek-piątek od 8:00 do 16:00.
4. Brak obowiązku przekazywania sprzętu w opakowaniach fabrycznych.
5. Uszkodzone dyski twarde pozostają własnością Zamawiającego.
6. Pozostałe warunki zgodnie z warunkami gwarancyjnymi producenta sprzętu komputerowego.

## Asysta stanowiska dla Zintegrowanego Systemu Informatycznego.

Asysta dostępna w całym okresie trwania gwarancji na system ZSI.

Zakres asysty stanowiskowej świadczonej przez Wykonawcę:

1. Wsparcie przez połączenie zdalne podczas użytkowania ZSI, rozwiązywanie zgłoszonych problemów podczas eksploatacji systemu.
2. Konsultacje dotyczącego efektywnego wykorzystania ZSI i użytkowania platformy e-usług.
3. Wsparcie zdalne podczas zmian w konfiguracji ZSI.
4. Przywracanie działania systemu ZSI na serwerze i stacjach roboczych np. po wystąpieniu awarii sprzętu.
5. Wsparcie podczas instalowania nowych wersji oprogramowania.
6. Świadczenie w/w usług 1-5 w co najmniej w czasie 5 godz./miesięcznie /usługi wykonywane zdalnie lub telefonicznie/. W przypadku niewykorzystania 5 godzin możliwość wykorzystania godzin w miesiącu następnym.
7. Usługi świadczone w dni robocze poniedziałek-piątek w godzinach 08:00-16:00.