Załącznik nr 1b do SIWZ

**Szczegółowy opis przedmiotu zamówienia dla Części II: „Dostawa rozmieszczenie i instalacja infrastruktury komputerowej na potrzeby wdrożenia e-usług w Szpitalu Miejskim św. Jana Pawła II w Elblągu” (Opis i wymagania techniczne dot. infrastruktury komputerowej)** – dotyczy przetargu nieograniczonego na w ramach projektu: Wdrożenie e-usług w Szpitalu Miejskim Św. Jana Pawła w Elblągu

# **1. Zasilacz awaryjny UPS – 2 sztuki**

|  |  |  |
| --- | --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Oferowane parametry techniczne** |
| **Parametry wyjściowe** |
| **Moc** | 1.98kW / 2.2kVA |  |
| **Nominalne napięcie**  | 208V, 230V |  |
| **Zniekształcenie napięcia** | Max 5% |  |
| **Topologia** | Line Interactive |  |
| **Przebieg fali** | Sinusoida |  |
| **Gniazda wyjściowe** | Przynajmniej:- 8x IEC 320 C13- 2x IEC 320 C19 |  |
| **Czas przełączania** | 6 ms typowe, 10 ms max |  |
| **Parametry wejściowe** |
| **Nominalne napięcie** | 208V, 230V |  |
| **Częstotliwość wejściowa** | 50/60 Hz +/-3 Hz (automatyczne wykrywanie) |  |
| **Zakres napięcia wejściowego w trybie podstawowym** | 140 - 280V |  |
| **Pozostałe wymagania** |
| **Typ akumulatora** | Bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu szczelny |  |
| **Typowy czas ładowania** | 3 godziny |  |
| **Czas podtrzymania** | Odpowiednio dla obciążenia 400/700/1000/1600/1980W:Min. 70/38/24.5/13/9 minut |  |
| **Interfejsy** | USB |  |
| **Panel sterowania** | Wyświetlacz statusu LED ze wskaźnikiem pracy online: Zasilanie akumulatorowe: Wskaźniki Wymień baterię i Przeciążenie, Wielofunkcyjna konsola sterownicza i informacyjna LCD |  |
| **Alarm dźwiękowy** | Alarm przy zasilaniu akumulatora: alarm przy bardzo niskim poziomie naładowania akumulatora: konfigurowalne opóźnienia |  |
| **Awaryjny wyłącznik zasilania** | Tak, wymagany |  |
| **Automatyczny test** | Wymagany okresowy autotest akumulatora który zapewnia wczesne wykrywanie konieczności wymiany |  |
| **Automatyczne włączenie UPS-a po powrocie zasilania** | Automatycznie uruchamia podłączony sprzęt w momencie wznowienia zasilania z sieci miejskiej. |  |
| **Akcesoria** | Zamawiający wymaga, aby urządzenia zostały dostarczone wraz z szynami do stelaża z 4 słupkami.  |  |
| **Oferowany produkt** | **Producent oferowanego sprzętu:** |  |
| **Model oferowanego sprzętu:** |  |

# **2. Dysk sieciowy NAS – 1 sztuka**

|  |  |  |
| --- | --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Oferowane parametry techniczne** |
| **Procesor** | Procesor z Mechanizm szyfrowania sprzętowego (AES-NI) 64-bit min. czterordzeniowy 2.4 GHz |  |
| **Pamięć** | Min. 2 GB DDR3 Całkowita liczba gniazd pamięci 2 |  |
| **Przechowywanie** | Maksymalny rozmiar pamięci - 64 TB (16 TB HDD x 4 sztuki) |  |
| **Porty zewnętrzne** | Min. 4 sztuki port LAN RJ-45 1GbE, USB 3.0 min. 2 porty, port eSATA min. 1 sztuka |  |
| **PCIe** | Rozszerzenie karty PCIe 1 x Gen2 x8 slot (x4 link) |  |
| **System plików** | Btrfs, EXT4, EXT3, FAT, NTFS, HFS+, exFAT |  |
| **Dyski** | Urządzenie musi posiadać zainstalowane 3 dyski twarde 3.5” o pojemności 10TB, prędkość obrotowa 7200 obr/minPamięć Cache 256 MB z zabezpieczeniami odporność na upadkiPrzystosowany do pracy ciągłej (24/7)Technologia NCQ, technologia RAIDZwiększona odporność na drgania  |  |
| **Elementy montażowe** | Urządzenie powinno zawierać elementy umożliwiające instalację w szafie rack |  |
| **Oferowany produkt** | **Producent oferowanego sprzętu:** |  |
| **Model oferowanego sprzętu:** |  |

# **3. Urządzenie klasy UTM – 1 sztuka**

Zamawiający jest w posiadaniu 1 sztuki urządzenia UTM - Fortigate 201E wraz z licencją: FOR-FC-10-00208-900-02-12 [S] FortiGate-201E UTM Bundle (8x5 FortiCare plus NGFW, AV, Web Filtering, Botnet IP/Domain and Antispam Services) 1 Year - (licencja wraz z serwisem ważna do 28.09.2020 roku)

Wykonawca musi dostarczyć identyczne urządzenie wraz z identyczną licencją i serwisem, zapewniające pracę w klastrze HA obydwu urządzeń. Dodatkowo Wykonawca musi dokupić wyrównanie licencji istniejącego urządzenia do ważności licencji urządzenia dostarczanego.

|  |  |  |
| --- | --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Oferowane parametry techniczne** |
| **Opis równoważności:** |
| **Porty** | Urządzenie musi posiadać:- min. 2 x WAN 10/100/1000 - min. 14 x LAN 10/100/1000Base-T - min. 4 x SFP |  |
| **Przepustowość** | Min.: - IPS 2.2 Gb/s, - NGFW 1.8 Gb/s, - Threat Protection 1.2 Gb/s, - CAPWAP (HTTP 64 KB) 1.5 Gb/s, - SSL-VPN 900 Mb/s |  |
| **Opóźnienie zapory** | Maksymalnie 3 μs |  |
| **Przepustowość zapory** | Min. 13.5 Mpps |  |
| **Domeny wirtualne** | min. (domyślne / maksymalne) 10/10 |  |
| **Lokalny dysk** | Min. 480GB |  |
| **Konfiguracje wysokiej dostępności** | Active / Active, Active / Passive, Clustering |  |
| **Temperatura robocza** | w zakresie 0-40 stopni Celsjusza |  |
| **Licencje** | Wymagana 2 letnia licencja AV, Web Filtering, Botnet IP/Domain and Antispam Services oraz wyrównanie licencji dla posiadanego przez Zamawiającego urządzenia.  |  |
| **Oferowany produkt** | **Producent oferowanego sprzętu:** |  |
| **Model oferowanego sprzętu:** |  |

# **4. Switch dystrybucyjny – 2 sztuki**

|  |  |  |
| --- | --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Oferowane parametry techniczne** |
| **Porty** | min. 48 RJ-45 autosensing 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3abType 1000BASE-T); Media Type: Auto-MDIX; Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only; Porty 1—8 muszą wspierać MACsec |  |
| 4 SFP+ 10GbE ports |  |
| 1 port expansion module slotWsparcie maximum 6 SFP+ port lub 2 1/10GBASE-T port lub 2 40GbE port w opcjonalnych modułach  |  |
| **Dodatkowe porty** | 1 podwójny szeregowy (RJ-45 lub mini USB) port konsoli |  |
| 1 port zarządzania poza pasmem RJ-45 |  |
| 1 port USB 2.0 |  |
| **Wentylator** | Kierunek przepływu powietrza z przodu (strona portu) do tyłu |  |
| **Pamięć i procesor** | Minimum:2 GB SDRAM; Packet buffer size: 4 MB,512 MB flash |  |
| **Maksymalna głębokość** | 40 cm |  |
| **Bezpieczeństwo** | UL 60950-1; EN 60825-1 Safety of LaserProducts-Part 1; EN 60825-2 Safety of LaserProducts-Part 2; IEC 60950-1; EN 60950-1; CAN/CSA-C22.2 No. 60950-1; FDA 21 CFR SubchapterJ; ROHS Compliance; AS/NZS 60950-1; GB 4943;EAC (EurAsian Conformity Certification) |  |
| **Dodatkowe wyposażenie** | Do każdego przełącznika dystrybucyjnego Wykonawca musi dostarczyć min. 4 sztuki transceiverów 1 GbE SFP do pracy ze światłowodem jednomodowym.  |  |
| **Oferowany produkt** | **Producent oferowanego sprzętu:** |  |
|  | **Model oferowanego sprzętu:** |  |

# **5. Switch dostępowy – 12 sztuk**

|  |  |  |
| --- | --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Oferowane parametry techniczne** |
| **Porty** | Min. 48 portów RJ-45 10/100/1000, 4 porty SFP |  |
| **Procesor** | Min. 800 MHz, min. pojemność bufora pakietów: 3 MB dynamicznie alokowanej |  |
| **Pamięć** | Min. 256 MB DDR3 DIMM |  |
| **Pamięci flash** | Min. 128 MB |  |
| **Przepustowość** | Min. 75 mln pakietów/s |  |
| **Pojemność przełączania** | Min 104 Gbps |  |
| **Możliwości łączenia kaskadowego** | Platforma wirtualna, 16 przełączników |  |
| **Zużycie energii** | Do 60W |  |
| **Funkcje** | IMC, CLI, przeglądarka internetowa, menu konfiguracyjne, zarządzanie pozapasmowe, IEEE 802.3 Ethernet MIB, Repeater MIB, Ethernet Interface MIB |  |
| **Pełny dupleks** | Tak |  |
| **Zarządzanie przez stronę www** | Tak |  |
| **Możliwość montażu w stelażu** | Tak |  |
| **Dodatkowe wyposażenie** | min. 1 sztuka transceivera 1 GbE SFP do pracy ze światłowodem jednomodowym do każdego przełącznika dostępowego. |  |
| **Oferowany produkt** | **Producent oferowanego sprzętu:** |  |
|  | **Model oferowanego sprzętu:** |  |

# 6. **Oprogramowanie do wykonywania backup’u – 1 komplet**

|  |  |  |
| --- | --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Oferowane parametry techniczne** |
| **Wymagania ogólne** | Licencja musi umożliwiać wykonywanie kopii bezpieczeństwa dla min. 8 serwerów fizycznych, 3 baz danych, 10 maszyn wirtualnych. |  |
| Support w wersji enterprise z nielimitowanym kontaktem emailowym i telefonicznym. |  |
| Program musi obsługiwać bazy danych Oracle oraz Microsoft SQL. |  |
| **Backup i przywracanie danych** | Oprogramowanie musi umożliwiać wykonywanie następujących czynności:1. Deduplikacja danych na źródle,
2. Backup przyrostowy Delta,
3. Backup różnicowy Delta,
4. Bare Metal Recovery,
5. Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji,
6. Retencja danych
7. Kreator projektów backupów - polityka backupu,
8. Projekty backupów,
9. Backup danych lokalnych - plikowy,
10. Backup MS Outlook,
11. Backup MS SQL,
12. Backup Firebird,
13. Backup dysków sieciowych,
14. Backup MS Exchange 2007 , 2010, 2013,
15. Backup MySQL,
16. Backup PostgreSQL,
17. Backup System State,
18. Backup Hyper-V,
19. Backup VMware,Backup VMware dla darmowych licencji,
20. Windows Operating System Backup – VHD,
21. Backup z wykorzystaniem skryptów pre i post,
22. Backup obrazu dysku - Obraz HDD,
23. Harmonogramy backupów,
24. Backup otwartych plików (VSS),
25. Filtr plików oraz folderów,
26. Domyślne wykluczenia zbędnych plików (pliki tymczasowe etc.),
27. Wyłączanie komputera po wykonaniu backupu,
28. Backup na prawach użytkownika systemu Windows,
29. Backup na prawach użytkownika AD,
30. Przywracanie danych do wskazanego katalogu,
31. Przywracanie danych do pierwotnej lokalizacji,
32. Przywracanie wybranej wersji pliku,
33. Możliwość backup-u z wykorzystaniem wielu rdzeni procesora,
34. Możliwość przywracania z wykorzystaniem wielu rdzeni procesora,
35. Przywracanie plików z określonego hosta,
36. Przywracanie plików z określonego projektu,
37. Przywracanie całych systemów operacyjnych,
38. Przywracanie Exchange bezpośrednio do serwera.
39. Przywracanie Hyper-V bezpośrednio do hosta maszyn,
40. Przywracanie Exchange 2013 na poziomie pojedynczej skrzynki,
41. Usuwanie plików przesłanych jako backup,
42. Usuwanie wybranej wersji pliku,
43. Wyszukiwanie plików w repozytorium użytkownika,
44. Nadpisywanie plików podczas ich przywracania.
 |  |
| **Konfiguracja oprogramowania** | Konfiguracja oprogramowania musi umożliwiać wykonywanie następujących czynności:1. Zmiana języka aplikacji,
2. Automatyczne logowanie,
3. Zapamiętywanie danych logowania,
4. Automatyczne uruchamianie programu przy starcie systemu,
5. Eksport oraz import konfiguracji do pliku,
6. Eksport oraz import konfiguracji na serwer,
7. Ograniczenie ilości przechowywanych wersji,
8. Ustawianie priorytetu dla procesu backupu,
9. Zmiana klucza szyfrującego,
10. Ustawienia proxy,
11. Ustawienia przepustowości/zajętości pasma,
12. Konfiguracja wydajności procesu backupu,
13. Możliwość ograniczenia obciążenia dysku twardego,
14. Możliwość wyłączenia zdalnego zarządzania.
 |  |
| **Bezpieczeństwo** | Program musi posiadać następujące funkcje:1. Szyfrowanie danych algorytmem AES 256 CBC zawsze po stronie komputera użytkownika,
2. Kompresja danych,
3. Transmisja po bezpiecznym protokole SSL,
4. Deklaracja domyślnego klucza szyfrującego,
5. Deklaracja klucza szyfrującego użytkownika,
6. Zmiana klucza szyfrującego,
7. Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji,
8. Obliczanie sumy kontrolnej SHA-1,
9. Zastępowanie nazwy pliku GUID-em,
 |  |
| **Dodatkowe funkcje** | 1. Shell Menu (menu kontekstowe systemu Windows),
2. Kreator pierwszego uruchomienia,
3. Rozbudowanie logi aplikacji kliencie oraz usługi,
4. Możliwość instalacji samej usługi – do zarządzania przez Management Center,
5. Automatycznie wyszukiwanie serwerów backupu w sieci,
6. Komunikaty z tray,
7. Wskazywanie statusu połączenia z serwerem,
8. Mechanizm łatwego raportowania błędów.
 |  |
| **Aplikacje serwerowe** | 1. Możliwość bezpośredniej instalacji oprogramowania na serwerze sieciowym NAS (nie jako maszyna wirtualna) bez potrzeby użycia serwera pośredniego
2. Magazyn danych jako jednostka logiczna,
3. Automatyzacja procesów związanych z uszkodzeniem magazynów
4. System sprawdzania integralności i spójności danych,
5. Narzędzie do cyklicznego oczyszczenia magazynów ze zbędnych plików,
6. Skalowalność oraz niezawodność,
7. Współpraca z API serwera NAS.
 |  |
| **Centralne zarządzanie** | 1. Zdalne zarządzanie aplikacjami klienckimi,
2. Tworzenie i edycja użytkowników,
3. Możliwość tworzenia grup i przypisywania użytkowników do wybranej grupy,
4. Zdalne tworzenie, na urządzeniach końcowych, projektów backupów podstawowych oraz zaawansowanych,
5. Automatycznie wyszukiwanie serwerów backupu w sieci ,
6. Wyzwalanie backupów na aplikacjach klienckich,
7. Edycja projektów backupów zapisanych na urządzeniach końcowych,
8. Przywracanie danych, które zostały poddane backupowi, na dowolne urządzenie,
9. Przywracanie danych, które zostały poddane backupowi, na komputer administratora,
10. Zdalna konfiguracja utylizacji zasobów komputera klienckiego przez aplikacje podczas wykonywania backupu,
11. Przypisywanie urządzeń do kont użytkowników,
12. Usuwanie urządzeń przypisanych do użytkowników,
13. Wgląd do dziennika zdarzeń poszczególnych użytkowników platformy,
14. Zarządzanie magazynami danych,
15. Grupowanie projektów w szablony,
16. Zarządzanie szablonami backupów,
17. Przesyłanie zdefiniowanych szablonów do aplikacji klienckich,
18. Zarządzanie sesjami backupu,
19. Integracja z Active Directory – mapowanie użytkowników,
20. Zdalna i cicha instalacja,
21. Pobieranie informacji na temat urządzeń użytkowników aplikacji klienckich,
22. Pobieranie aplikacji klienckich,
23. Wgląd do logów wszystkich usług platformy,
24. Możliwość raportowania błędów,
25. Generowanie raportów oraz wykresów,
26. Możliwość uruchomienia wykonanego obrazu dysku jako maszynę wirtualną bez konieczności użycia zewnętrznego wirtualizatora,
27. Możliwość przywrócenia obrazu na dowolny sprzęt z pendrive’a,
28. Możliwość uruchomienia obrazu na dowolnym sprzęcie, jako maszynę wirtualną za pośrednictwem pendrive’a,
29. Zarządzanie szablonami backupu,
30. Monitorowanie sesji,
31. Wykresy oraz statystyki,
32. Wskazywanie statusu połączenia z serwerem,
33. Możliwość definiowania wielu ścieżek jednoczesnego zapisu dla jednego magazynu – redundancja,
34. Możliwość ręcznego uruchomienia oczyszczenia magazynów ze zbędnych plików,
35. Archiwizacja danych - możliwość eksportu danych do wersji natywnej i ich zapisów w dowolnej lokalizacji - funkcja realizowana w całości przez serwer,
36. Możliwość zarządzania magazynami danych,
37. Kreator pierwszej konfiguracji systemu
 |  |
| **Wspierane systemy operacyjne** | 1. Microsoft Windows 7 i nowsze,
2. Microsoft Windows Server 2008 R2 i nowsze,
3. Unix/Linux,
4. OS X,
5. Novell NetWare 6.5.
 |  |
| **Dodatkowe wymagania** | 1. Ilość rdzeni, wątków i procesorów oraz pojemność macierzy nie jest w żaden sposób ograniczana przez licencje,
2. Licencja wieczysta z trzy letnim okresem wsparcia technicznego oraz dostępem do aktualizacji.
3. Wsparcie techniczne, świadczone jest bezpośrednio od producenta, w języku polskim.
 |  |
| **Oferowany produkt** | **Producent oferowanego oprogramowania:** |  |
| **Wersja oferowanego oprogramowania:** |  |

# **7. Zestaw komputerowy stacjonarny wraz z oprogramowaniem antywirusowym oraz oprogramowaniem biurowym – 76 kompletów**

|  |  |  |
| --- | --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Oferowane parametry techniczne** |
| **Stacja robocza** |
| **Zastosowanie** | Komputer stacjonarny, który będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna.  |  |
| **Wydajność obliczeniowa** | Procesor musi osiągać w teście wydajności PassMark PerformanceTest (wynik dostępny: http://www.passmark.com/products/pt.htm) co najmniej wynik 11600 punktów Passmark CPU Mark. |  |
| **Pamięć operacyjna** | 8GB DDR4 2666 MHz możliwość rozbudowy do min 32 GB.  |  |
| **Pamięć masowa** | Dysk SSD o pojemności min. 256GB, zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii bez dodatkowych nośników. |  |
| **Karta graficzna** | Grafika zintegrowana z procesorem umożliwiająca pracę na 3 monitorach ze wsparciem dla DirectX 12, Open CL 2.0, OpenGL 4.4 – z możliwością dynamicznego przydzielenia do 1,7 GB pamięci. |  |
| **Multimedia** | 1. Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition audio.
2. Port słuchawek i mikrofonu na przednim panelu, obudowa wyposażona w głośnik.
 |  |
| **Klawiatura i mysz** | Klawiatura USB w układzie QWERTY US.  |  |
| Mysz laserowa USB z trzema klawiszami oraz rolką (scroll). |  |
| **Zasilanie** | Zasilacz o mocy minimum 280W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 94%, przy 50% obciążeniu. |  |
| **Obudowa** | Obudowa typu SFF z obsługą kart PCI Express wyłącznie o niskim profilu, wyposażona w min. 3 kieszenie: 1 szt. 5,25” zewnętrzna typu SLIM, 1 szt. 3,5” wewnętrzna., 1 szt. 2,5 wewnętrzna |  |
| Wbudowany akustyczny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami. |  |
| **BIOS** | Możliwość odczytania informacji bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego nośników zewnętrznych dotyczących:1. modelu komputera,
2. nr seryjnego komputera,
3. wersji BIOS,
4. daty produkcji BIOS,
5. ilości, częstotliwości taktowania i sposobu obłożenia kanałów pamięciami RAM,
6. modelu płyty głównej,
7. nazwie komputera,
8. typie procesora wraz z informacją o częstotliwości traktowania,
9. producencie, modelu oraz pojemności zainstalowanego dysku twardego
10. MAC adresie zintegrowanej karty sieciowej.
 |  |
| Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego, (gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS). |  |
| Możliwość z poziomu BIOS-u włączenia/wyłączenia funkcji automatycznej aktualizacji BIOS-u. System musi umożliwiać zdefiniowanie adresu IP serwera TFTP w sieci lokalnej lub podanie nazwy serwera, w którego bezpośrednio z poziomu BIOS-u można dokonać aktualizacji BIOS-u. System musi umożliwiać również określenie częstotliwości sprawdzania dostępności nowszej wersji BIOS-u z częstotliwością co najmniej: raz dziennie, raz na tydzień, raz na miesiąc i raz na kwartał.  |  |
| Możliwość aktualizacji BIOS-u, w tym co najmniej: całkowite wyłączenie możliwości aktualizacji, możliwość aktualizacji za pomocą narzędzi producenta komputera lub mechanizmu Windows Update, możliwość aktualizacji jedynie za pomocą narzędzi producenta komputera. |  |
| Możliwość włączania/wyłączania sprzętowego wsparcia wirtualizacji w procesorze liczby aktywnych rdzeni procesora |  |
| Możliwość włączania/wyłączania technologii SpeedStep oraz Turbo. |  |
| Możliwość wyboru trybu pracy systemu chłodzenia komputera spośród co najmniej w trzech ustawień: automatyczny, maksymalna wydajność CPU oraz maksymalna prędkość wentylatorów. |  |
| Możliwość monitorowania temperatury rdzenia procesora, obudowy procesora oraz temperatury wewnątrz obudowy komputera oraz prędkości obrotowej wentylatora. |  |
| Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń |  |
| Możliwość ustawienia trybu pracy komputera po przywróceniu zasilania po awarii zasilania w co najmniej trzech trybach: pozostaje wyłączony, zawsze wyłączony, zawsze włączony, przywrócenie stanu z przed awarii |  |
| Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych, ustawienia hasła na poziomie systemu, administratora oraz dysku twardego (dla wszystkich rodzajów dysków twardych w tym dysków M.2). |  |
| Możliwość ustawienia poziomu zabezpieczenia BIOS-u za pomocą hasła co najmniej na dwóch poziomach:  - Standardowy: umożliwiający skasowanie hasła za pomocą zworki na płycie głównej - Silny: umożliwiający zresetowanie hasła jedynie poprzez interwencję serwisu |  |
| Możliwość włączenia/wyłączenia zintegrowanej karty dźwiękowej, karty sieciowej, modułu TPM z poziomu BIOS, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. |  |
| Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne. |  |
| Możliwość wyłączania portów USB w tym: wszystkich portów, tylko portów znajdujących się na przedzie obudowy, tylko tylnych portów, tylko zewnętrznych, wszystkich nieużywanych. W przypadku włączenia jedynie przednich lub jedynie tylnych lub jedynie używanych portów wymagana jest możliwość określenia czy włączone mają być jedynie porty USB do których podłączona jest klawiatura i mysz lub możliwość wyłączenia portów do których podłączone są pamięci masowe lub hub USB. |  |
| **Dodatkowe oprogramowanie** | Oprogramowanie dostarczone przez producenta komputera (w ofercie należy podać nazwę oprogramowania) pozwalające na zdalną inwentaryzację komputerów w sieci, lokalną i zdalną inwentaryzację komponentów komputera, umożliwiające co najmniej:1. informowanie administratora o otwarciu obudowy
2. zdalne wyłączanie, restart oraz hibernacje komputera w sieci,
3. otrzymywanie informacji WMI – Windows Management Interface,
4. tworzenie raportów stanu jednostki,
5. monitorowanie stanu komponentów: CPU, Pamięć RAM, HDD, wersje BIOS,
6. aktualizację BIOS do najnowszej wersji zarówno dla pojedynczej maszyny jak i grupy,
7. tworzenie kopii zapasowych BIOS wraz z ustawieniami
8. tworzenie indywidualnych numerów dla poszczególnych użytkowników,
9. włączenie lub wyłączanie BOOTowania portów USB
10. w pełni automatyczną instalację sterowników urządzeń opartą o automatyczną detekcję posiadanego sprzętu
 |  |
| Certyfikowane oprogramowanie umożliwiające w bezpieczny (bezpowrotny) sposób usunięcie danych z dysku twardego z poziomu BIOS-u bez względu na stań czy obecność systemu operacyjnego. W ofercie należy podać nazwę i producenta oprogramowania |  |
| **Ergonomia** | Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie jałowym (IDLE) wynosząca maksymalnie 20dB – wymagane dołączenie do oferty raportu z testów głośności wykonanych przez certyfikowane i niezależne od producenta laboratorium. |  |
| Obudowa w jednostce centralnej musi być otwierana bez konieczności użycia narzędzi (wyklucza się użycie standardowych wkrętów, śrub motylkowych) oraz powinna posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym producenta komputera. |  |
| Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej, kłódki (oczko w obudowie do założenia kłódki) oraz zamka na klucz nie wystającego poza linię obudowy. |  |
| Suma wymiarów obudowy (wysokość + szerokość + głębokość mierzona po krawędziach zewnętrznych) nie może wynosić więcej niż 700 mm. |  |
| **Zgodność z systemami operacyjnymi i standardami** | Oferowane modele komputerów muszą posiadać certyfikat Microsoft, potwierdzający poprawną współpracę oferowanych modeli komputerów z systemem operacyjnym Windows Pro 10 64bit. |  |
| **System operacyjny** | Licencja na system operacyjny Microsoft Windows 10 Professional PL, zainstalowany system operacyjny Microsoft Windows 10 Pro niewymagający aktywacji za pomocą telefonu lub Internetu w firmie Microsoft. Dołączony nośnik Recovery umożliwiający instalację systemu wersji 64 bitowej lub równoważny. *Opis równoważności*Zainstalowany system operacyjny spełniający poniższe wymagania:* + - Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek. Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet.
		- Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie nazwy strony serwera WWW.
		- Internetowa aktualizacja zapewniona w języku polskim.
		- Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.
		- Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe.
		- Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug &Play, Wi-Fi).
		- Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer.
		- Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta.
		- Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu.
		- Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
		- Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych.
		- Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.
		- Wbudowany system pomocy w języku polskim.
		- Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).
		- Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji.
		- Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.
		- Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
		- 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 1.1 i 2.0 i 3.0 lub programów równoważnych, tj. – umożliwiających uruchomienie aplikacji działających we wskazanych środowiskach.
		- Wsparcie dla JScript i VBScript lub równoważnych – możliwość uruchamiania interpretera poleceń.
		- Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.
		- Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową.
		- Rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację.
		- Graficzne środowisko instalacji i konfiguracji.
		- Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.
		- Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.
		- Udostępnianie modemu.
		- Oprogramowanie 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).
		- Zamawiający wymaga dostarczenia systemu operacyjnego w wersji 64-bit.

Licencja i oprogramowanie musi być nowe, nieużywane. |  |
| **Porty i złącza** | - 1 x DVI- 1 x Display Port- 2 x PS/2- 1 x RJ-45- 1 x Audio: line-in- 1 x Audio: line-out- 1 x Audio: mikrofon z przodu obudowy- 1 x Audio: słuchawki z przodu obudowy |  |
| 10 szt. USB w tym: minimum 4 porty z przodu obudowy (w tym min. 2 x USB 3.0), minimum 4 porty z tyłu obudowy (w tym min. 2 x USB 3.0), minimum 2 porty wewnątrz obudowy. Porty te muszą być wlutowane w płytę główną – nie dopuszcza się portów wyprowadzonych z płyty głównej na zewnątrz komputera za pomocą przewodów, taśm itp.Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp. |  |
| Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika) |  |
| Płyta główna z wbudowanymi złączami:1. 1 złącze PCI-Express 2.0 x4 (mech. x16)
2. 1 złącze PCI-Express 3.0 x16
3. 1 złącze M.2-2280 umożliwiający zamontowanie modułu SSD NVMe (PCI-Express 2.0)
 |  |
| Obsługa kart wyłącznie o niskim profilu, minimum 2 złącza DIMM z obsługą do 32GB DDR4 pamięci RAM, min. 3 złącz SATA 3.0 NCQ w tym min 1 złącze eSATA, płyta musi być trwale oznaczona logo producenta komputera |  |
| Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego (TPM co najmniej w wersji 2.0) |  |
| Nagrywarka DVD +/-RW  |  |
| **Oferowany produkt** | **Producent oferowanego sprzętu:** |  |
| **Model oferowanego sprzętu:** |  |
| **Monitor** |
| **Ekran** | Panoramiczny; ciekłokrystaliczny z aktywną matrycą IPS o przekątnej co najmniej min. 21,5”, powierzchnia matrycy utwardzana 3H |  |
| **Jasność** | min. 250 cd/m2 |  |
| **Kontrast** | min. 1000:1 |  |
| **Wielkość plamki** | 0,248 mm |  |
| **Kąty widzenia (pion/poziom)** | min. 178°/178 |  |
| **Czas reakcji matrycy** | maks. 5 ms |  |
| **Kolory** | min. 16.7mln |  |
| **Rozdzielczość** | min. 1920x1080 |  |
| **Powłoka powierzchni ekranu** | Przeciwodblaskowa, utwardzona |  |
| **Złącza** | 15-stykowe złącze D-Sub, DVI (z HDCP) oraz Display Port |  |
| 2 x złącza audio – wejście oraz wyjście |  |
| **Zużycie energii** | Średnie użycie energii 15 W, max.: 20 W, tryb uśpienia 0,16 W |  |
| **Zakres pochylenia monitora** | Przynajmniej od -5° do +22° |  |
| **Inne** | Usuwalna podstawa montażowa.  |  |
| Wbudowane 2 głośniki min. 1,5 W. |  |
| Kompatybilność z VESA 100mm. |  |
| Kensington Lock. |  |
| Dedykowany przycisk do włączenia trybu Eco z wizualną sygnalizacją aktywnego trybu. |  |
| Zasilacz wbudowany – nie dopuszcza się zasilaczy zewnętrznych. |  |
| Zamawiający wymaga, aby komputer oraz monitor pochodziły od jednego producenta. |  |
| **Oferowany produkt** | **Producent oferowanego sprzętu:** |  |
| **Model oferowanego sprzętu:** |  |
| **Licencje systemu antywirusowego do każdego oferowanego zestawu komputerowego** |
| **Ogólne** | Licencje muszą być kompatybilne z posiadanym przez Zamawiającego systemem ESET Endpoint Antivirus Suite – licencja na okres równy udzielonemu okresowi gwarancji na dostarczone zestawy komputerowe |  |
| **OPIS RÓWNOWAŻNOŚCI** |
| **Ogólne** | Pełne wsparcie dla systemu Windows 7/ Windows8/ Windows 8.1/ Windows 8.1 Update/ Windows 10. |  |
| Wsparcie dla 32- i 64-bitowej wersji systemu Windows. |  |
| Wersja programu dla stacji roboczych Windows dostępna zarówno w języku polskim jak i angielskim. |  |
| Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim. |  |
| Licencja na okres równy udzielonemu okresowi gwarancji na dostarczone zestawy komputerowe. |  |
| **Ochrona antywirusowa i antyspyware** | 1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
3. Wbudowana technologia do ochrony przed rootkitami.
4. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
6. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
7. System ma oferować administratorowi możliwość definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym i jeśli tak – nie wykonywało danego zadania.
8. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
9. Możliwość skanowania dysków sieciowych i dysków przenośnych.
10. Skanowanie plików spakowanych i skompresowanych.
11. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
12. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
13. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera.
14. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
15. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
16. 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.
17. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
18. 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).
19. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
20. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
21. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator.
22. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora.
23. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
24. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
25. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta.
26. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
27. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka).
28. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika).
29. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
30. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
31. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła.
32. 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.
33. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.
34. 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.
35. 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.
36. 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.
37. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.
38. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji.
39. 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.
40. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia, dana funkcjonalność musi pozwalać na automatyczne wypełnienie właściwości urządzenia dla tworzonej reguły.
41. 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.
42. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
43. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
44. 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.
45. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
46. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
47. Oprogramowanie musi posiadać zaawansowany skaner pamięci.
48. Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp.
49. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.
50. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami.
51. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji.
52. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http
53. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
54. Program ma być w pełni zgodny z technologią CISCO Network Access Control.
55. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełno ekranowym.
56. 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.
57. 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.
58. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
59. Program musi posiadać możliwość utworzenia z poziomu interfejsu aplikacji dziennika diagnostycznego na potrzeby pomocy technicznej.
60. Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline.
61. Aplikacja musi posiadać funkcję ręcznej aktualizacji komponentów programu.
62. Program musi posiadać możliwość definiowana stanów aplikacji, jakie będą wyświetlane użytkownikowi np. powiadomień o wyłączonych mechanizmach ochrony czy stanie licencji.
63. 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 ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
3. Wbudowana technologia do ochrony przed rootkitami i exploitami.
4. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
5. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
6. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
7. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych.
8. Możliwość skanowania dysków sieciowych i dysków przenośnych.
9. Skanowanie plików spakowanych i skompresowanych.
10. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
11. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
12. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS.
13. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
14. Program ma umożliwiać użytkownikowi blokowanie zewnętrznych nośników danych na stacji.
15. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
16. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
17. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony.
18. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji.
19. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line).
20. 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.
21. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka).
22. Możliwość skanowania wyłącznie z zastosowaniem algorytmów heurystycznych tj. wyłączenie skanowania przy pomocy sygnatur baz wirusów.
23. Aktualizacje modułów analizy heurystycznej.
24. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
25. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
26. 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.
27. 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.
28. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji ma być takie samo.
29. System antywirusowy ma być w pełni zgodny z technologią CISCO NAC.
30. 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.
31. 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.
32. 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.
33. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
34. 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).
35. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
36. 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).
37. Aplikacja musi wspierać skanowanie magazynu Hyper-V
38. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów
39. Administrator ma możliwość dodania wykluczenia po tzw. HASH’u zagrożenia, wskazującego bezpośrednio na określoną infekcję a nie konkretny plik.
40. Praca programu musi być niezauważalna dla użytkownika.
41. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania.
42. 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, 2016 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. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej.
6. Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy występujące w sieci.
7. Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6.
8. Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL.
9. Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.
10. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.
11. Jeden centralny serwer centralnego zarządzania bez względu na wielkość sieci.
12. 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.
13. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na stacjach roboczych z systemami Windows oraz Linux oraz serwerach Windows.
14. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware’ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci.
15. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.
16. Administrator musi posiadać możliwość zarządzania za pomocą dedykowanego agenta stacjami nie posiadającymi zainstalowanego programu zabezpieczającego.
17. Agent musi przekazywać informacje na temat stanu systemu operacyjnego do serwera administracji zdalnej
18. Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi.
19. Administrator musi posiadać możliwość utworzenia użytkownika wbudowanego lub zintegrowanego z grupą z usługi Active Directory.
20. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.
21. Dostępne zadania muszą być podzielone na dwie grupy: zadania klienta oraz zadania serwera.
22. Zadania serwera obejmujące zadanie instalacji agenta, generowania raportów oraz synchronizacji grup.
23. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej.
24. Serwer administracyjny musi oferować możliwość utworzenia jednego zadania dla kilku klientów lub grupy.
25. Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów.
26. 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.
27. Serwer administracyjny musi umożliwiać wyświetlenie polityk do których przynależy dana stacja robocza oraz ich edycję z poziomu właściwości samego klienta
28. Serwer administracyjny musi oferować możliwość utworzenia własnych raportów lub skorzystanie z predefiniowanych wzorów.
29. Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.
30. Serwer administracyjny musi oferować możliwość utworzenia własnych powiadomień lub skorzystanie z predefiniowanych wzorów.
31. 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.
32. Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu.
33. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty.
34. 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.
35. Konsola administracyjna musi umożliwiać dodanie własnego logotypu do interfejsu webowego.
 |  |
| **Oferowany produkt** | **Producent oferowanego oprogramowania:** |  |
| **Wersja oferowanego oprogramowania:** |  |
| **Licencje oprogramowania biurowego do każdego oferowanego zestawu komputerowego** |
| **Oprogramowanie biurowe** | Zintegrowany pakiet aplikacji biurowych musi zawierać:1. edytor tekstów,
2. arkusz kalkulacyjny,
3. narzędzie do przygotowania i prowadzenia prezentacji,
4. narzędzie do zarządzania informacją osobistą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami),
5. pełną polską wersję językową interfejsu użytkownika, w tym także systemu interaktywnej pomocy w języku polskim,
6. system aktualizacji darmowych poprawek bezpieczeństwa, przy czym komunikacja z użytkownikiem musi odbywać się w języku polskim,
7. dostępność w Internecie na stronach producenta biuletynów technicznych, w tym opisów poprawek bezpieczeństwa, w języku polskim, a także telefonicznej pomocy technicznej producenta pakietu biurowego świadczonej w języku polskim w dni robocze w godzinach od 8-19 – cena połączenia nie większa niż cena połączenia lokalnego,
8. publicznie znany cykl życia przedstawiony przez producenta dotyczący rozwoju i wsparcia technicznego – w szczególności w zakresie bezpieczeństwa co najmniej 5 lat od daty zakupu,
9. możliwość dostosowania pakietu aplikacji biurowych do pracy dla osób niepełnosprawnych np. słabo widzących, zgodnie z wymogami Krajowych Ram Interoperacyjności (WCAG 2.0).
 |  |
| **Edytor tekstów** | Edytor tekstów musi umożliwiać: 1. edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty,
2. wstawianie oraz formatowanie tabel,
3. wstawianie oraz formatowanie obiektów graficznych,
4. wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne),
5. automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków,
6. automatyczne tworzenie spisów treści,
7. formatowanie nagłówków i stopek stron,
8. śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie,
9. nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności,
10. określenie układu strony (pionowa/pozioma),
11. wydruk dokumentów,
12. wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną,
13. zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
 |  |
| **Arkusz kalkulacyjny** | Arkusz kalkulacyjny musi umożliwiać: 1. tworzenie raportów tabelarycznych,
2. tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych,
3. tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu,
4. tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice),
5. obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych,
6. zastosowanie narzędzi wspomagających analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych,
7. tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych,
8. wyszukiwanie i zamianę danych,
9. wykonywanie analiz danych przy użyciu formatowania warunkowego,
10. nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie,
11. nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności,
12. formatowanie czasu, daty i wartości finansowych z polskim formatem,
13. zapis wielu arkuszy kalkulacyjnych w jednym pliku,
14. zabezpieczanie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
 |  |
| **Narzędzie do przygotowywania i prowadzenia prezentacji** | Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać: 1. przygotowywanie prezentacji multimedialnych, które mogą być prezentowanie przy użyciu projektora multimedialnego,
2. drukowanie w formacie umożliwiającym robienie notatek,
3. zapisanie jako prezentacja tylko do odczytu,
4. nagrywanie narracji i dołączanie jej do prezentacji,
5. opatrywanie slajdów notatkami dla prezentera,
6. umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo,
7. umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego,
8. odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym,
9. tworzenie animacji obiektów i całych slajdów,
10. prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera.
 |  |
| **Narzędzie do zarządzania informacją prywatną** | Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:1. pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego,
2. przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych,
3. filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców,
4. tworzenie katalogów, pozwalających katalogować pocztę elektroniczną,
5. automatyczne grupowanie poczty o tym samym tytule,
6. tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy,
7. oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów,
8. ustalanie liczby wiadomości, które mają być synchronizowane lokalnie,
9. zarządzanie kalendarzem,
10. udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników,
11. przeglądanie kalendarza innych użytkowników,
12. zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach,
13. zarządzanie listą zadań,
14. zlecanie zadań innym użytkownikom,
15. zarządzanie listą kontaktów,
16. udostępnianie listy kontaktów innym użytkownikom,
17. przeglądanie listy kontaktów innych użytkowników,
18. przesyłanie kontaktów innym użytkowników.
 |  |
| **Oferowany produkt** | **Producent oferowanego oprogramowania:** |  |
| **Wersja oferowanego oprogramowania:** |  |

# 8. **Switch FC – 2 sztuki**

|  |  |  |
| --- | --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Oferowane parametry techniczne** |
| **Obudowa** | 19” 1U |  |
| **Porty** | Minimum 48 portów FC 16Gb/s. |  |
| Zamawiający wymaga 12 aktywnych portów FC oraz dostarczenie 12 wkładek 16Gb/s.  |  |
| Out-of-band 10/100/1000  |  |
| **Bezpieczeństwo** | Strefy VSAN: - Strefy wymuszone sprzętowo - Strefy jednostki logicznej (LUN) i strefy tylko do odczytuFC-SP do uwierzytelniania między hostami i przełącznikami Zabezpieczenia portów Dostęp do zarządzania: - SSHv2 - SNMPv3 - Listy ACL IP |  |
| **Dostępność** | Bezproblemowe aktualizacje oprogramowania  |  |
| Monitorowanie procesu i restartowanie procesu  |  |
| Usługi sieciowe Per-VSAN Nadmiarowe, wymienialne podczas pracy zasilacze  |  |
| Wymienialna na gorąco moduły SFP+ |  |
| **Oferowany produkt** | **Producent oferowanego sprzętu:** |  |
|  | **Model oferowanego sprzętu:** |  |

# 9. **Serwer – 2 sztuki**

|  |  |  |
| --- | --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Oferowane parametry techniczne** |
| **Obudowa** | Maksymalnie 1U RACK 19 cali (wraz z szynami montażowymi umożliwiającymi serwisowanie serwera w szafie rack bez wyłączania urządzenia) |  |
| **Procesor** | Procesor dziesięciordzeniowy, x86 - 64 bity, Intel Xeon 4210 (2.2GHz/10-core/85W) lub równoważny procesor dziesięciordzeniowy, osiągający w testach PassMark – CPU Mark wynik nie gorszy niż 15400 punktów W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie www.cpubenchmark.netPłyta główna wspierająca zastosowanie procesorów od 4 do 28 rdzeniowych, mocy do min. 205W i taktowaniu CPU do min. 3.6GHz. |  |
| **Liczba procesorów** | Obsługa min. 2 procesorów  |  |
| **Liczba zainstalowanych procesorów** | 2 sztuki procesorów opisanych powyżej |  |
| **Pamięć operacyjna** | 64 GB RDIMM DDR4 2666 MT/s w modułach o pojemności 32GB każdy.Płyta główna z minimum 24 slotami na pamięć i umożliwiająca instalację do minimum 3TB. Wsparcie dla Technologii Advanced ECC lub Memory Thermal Throttling |  |
| **Sloty rozszerzeń** | 2 aktywne gniazda PCI-Express generacji 3, w tym min. 1 slot x16 (szybkość slotu – bus width) |  |
| **Dysk twardy** | Zatoki dyskowe gotowe do zainstalowania 8 dysków SFF typu Hot Swap, SAS/SATA/SSD, 2,5”.Serwer wyposażony powinien być w 2 dyski SSD SFF (2.5in) o pojemności min. 480GB. |  |
| **Kontroler** | Serwer wyposażony w kontroler sprzętowy z min. 2GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę 8 napędów dyskowych SAS oraz obsługujący poziomy: RAID 0/1/10/5/50/6/60. |  |
| Serwer umożliwiający rozbudowę o sprzętowy kontroler RAID zapewniający obsługę RAID 0/1/10/5/50/6/60 z 4GB pamięci cache z podtrzymywaniem bateryjnym. |  |
| **Interfejsy sieciowe** | Minimum 4 wbudowane porty Ethernet 100/1000 Mb/s RJ-45 z funkcją Wake-On-LAN, wsparciem dla PXE, które nie zajmują gniazd PCIe opisanych w sekcji „Sloty rozszerzeń”. Minimum 2 porty FC 16Gb |  |
| **Karta graficzna** | Zintegrowana karta graficzna |  |
| **Porty** | 3 x USB 3.0 (w tym 1 porty wewnętrzny), 1x USB z przodu serwera, 1x VGAWewnętrzny slot na kartę micro SD. |  |
| Dodatkowy port VGA lub DisplayPort dostępny z przodu serwera |  |
| **Zasilacz** | 2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 495W. |  |
| **Chłodzenie** | Zestaw wentylatorów redundantnych typu hot-plug |  |
| **Pamięć micro SD/FLASH** | Zainstalowana karta pamięci micro SD/FLASH minimum 8GB. |  |
| **Napęd** | Możliwość instalacji wewnętrznego napędu DVD-ROM lub DVD-RW |  |
| **Karta/moduł zarządzający** | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca:1. zdalny dostęp do graficznego interfejsu Web karty zarządzającej,
2. zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera),
3. szyfrowane połączenie (SSL) oraz autentykacje i autoryzację użytkownika,
4. możliwość podmontowania zdalnych wirtualnych napędów,
5. wirtualną konsolę z dostępem do myszy, klawiatury,
6. wsparcie dla IPv6,
7. wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH,
8. możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer,
9. integracja z Active Directory,
10. możliwość obsługi przez dwóch administratorów jednocześnie,
11. wsparcie dla dynamic DNS.
 |  |
| **Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych** | 1. Microsoft Windows Server 2012 R2, 2016, 2019,
2. Red Hat Enterprise Linux (RHEL),
3. SUSE Linux Enterprise Server (SLES),
4. VMware ESXi 6.5 lub nowszy.
 |  |
| **Oferowany produkt** | **Producent oferowanego sprzętu:** |  |
| **Model oferowanego sprzętu:** |  |

# **10. Serwerowy System Operacyjny SSO – 2 sztuki licencji**

|  |  |  |
| --- | --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Oferowane parametry techniczne** |
| **Wymagania ogólne** | Oprogramowanie dla dwóch serwerów fizycznych - dwie sztuki licencji MS Windows Server Standard 2019 na 20 core lub równoważne. |  |
| 200 sztuk licencji dostępowych dla użytkownika współpracujących z dostarczanym systemem operacyjnym. |  |
| Licencja na serwerowy system operacyjny musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowiskach serwerowego systemu operacyjnego. |  |
| Dostarczenia licencja na oprogramowanie musi być w najnowszej wersji obecnie dostępnej na rynku. |  |
| **OPIS RÓWNOWAŻNOŚCI** |
| **Wymagania dla serwerowego systemu operacyjnego** | Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. |  |
| Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. |  |
| Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. |  |
| Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. |  |
| Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. |  |
| Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. |  |
| Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. |  |
| Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. |  |
| Wbudowane wsparcie instalacji i pracy na wolumenach, które:1. pozwalają na zmianę rozmiaru w czasie pracy systemu,
2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
4. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
 |  |
| Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. |  |
| Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. |  |
| Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET. |  |
| Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. |  |
| Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. |  |
| Dostępne dwa rodzaje graficznego interfejsu użytkownika:1. klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
2. dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
 |  |
| Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, |  |
| Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. |  |
| Mechanizmy logowania w oparciu o:1. login i hasło,
2. karty z certyfikatami (smartcard),
3. wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).
 |  |
| Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.. |  |
| Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). |  |
| Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. |  |
| Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. |  |
| Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). |  |
| Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. |  |
| Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:1. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
2. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
3. podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
4. ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
5. odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
6. bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
7. Zdalna dystrybucja oprogramowania na stacje robocze.
8. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
9. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
10. dystrybucję certyfikatów poprzez http,
11. konsolidację CA dla wielu lasów domeny,
12. automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
13. automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
14. Szyfrowanie plików i folderów.
15. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
16. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
17. Serwis udostępniania stron WWW.
18. Wsparcie dla protokołu IP w wersji 6 (IPv6),
19. Wsparcie dla algorytmów Suite B (RFC 4869),
20. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
21. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
22. dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
23. obsługi ramek typu jumbo frames dla maszyn wirtualnych,
24. obsługi 4-KB sektorów dysków,
25. nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra.
26. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API,
27. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode).
 |  |
| Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. |  |
| Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). |  |
| Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. |  |
| Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. |  |
| Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. |  |
| Zorganizowany system szkoleń i materiały edukacyjne w języku polskim. |  |
| **Oferowany produkt** | **Producent oferowanego oprogramowania:** |  |
| **Wersja oferowanego oprogramowania:** |  |

# **10. Macierz – 1 sztuka**

|  |  |  |
| --- | --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Oferowane parametry techniczne** |
| **Obudowa** | Macierz musi być przystosowana do montażu w szafie rack 19”, o wysokość maksymalnie 2U. |  |
| **Przestrzeń dyskowa** | Macierz musi posiadać minimum 10 dysków każdy o pojemności 6 TB i prędkości obrotowej min. 7200 obr/min. |  |
| **Możliwość rozbudowy** | Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 192 dysków twardych. |  |
| **Obsługa dysków** | Macierz musi obsługiwać dyski SSD, SAS i MDL SAS/NLSAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i MDL SAS/NLSAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5” jak również 3,5”. |  |
| **Sposób zabezpieczenia danych** | Macierz musi obsługiwać mechanizmy RAID zgodne z RAID1, RAID10, RAID5 lub RAID50 realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków twardych (tzw. wide-striping). |  |
| Macierz musi również umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID. |  |
| **Tryb pracy kontrolerów macierzowych** | Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe w sieci FC. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów FC. |  |
| **Pamięć cache** | Każdy kontroler macierzowy musi być wyposażony w minimum 6 GB pamięci cache, 12 GB sumarycznie w macierzy.  |  |
| Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 4 TB z wykorzystaniem dysków SSD. |  |
| Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem. |  |
| **Interfejsy** | Macierz musi posiadać, co najmniej 2 porty FC 16 Gb/s na kontroler. |  |
| **Zarządzanie** | Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej. |  |
| **Zarządzanie grupami dyskowymi oraz dyskami logicznymi** | Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej. |  |
| Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy.Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |  |
| **Thin Provisioning** | Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie Thin Provisioning. |  |
| **Wewnętrzne kopie migawkowe** | Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych.  |  |
| Musi istnieć możliwość dokupienia w przyszłości licencji, która rozszerzy możliwość tworzenia kopii migawkowych do minimum 512. |  |
| **Zdalna replikacja danych** | Macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy. |  |
| Aktualnie ta funkcjonalność nie jest wymagana. Musi istnieć możliwość dokupienia jej w przyszłości. |  |
| **Podłączanie zewnętrznych systemów operacyjnych** | Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami). |  |
| Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, Linux, VMware, Macierz musi posiadać wsparcie dla różnych systemów klastrowych |  |
| **Redundancja** | Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. |  |
| Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze. |  |
| Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy. |  |
| **Dodatkowe wymagania** | Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych. |  |
| **Inne** | Sprzęt musi pochodzić z oficjalnego kanału producenta - dostarczony przez certyfikowanego partnera producenta. Oświadczenie musi być przedstawione przez firmę dostarczającą. |  |
| **Oferowany produkt** | **Producent oferowanego sprzętu:** |  |
| **Model oferowanego sprzętu:** |  |

# **11. Usługi wdrożeniowe**

|  |  |  |
| --- | --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Oferowane usugi** |
| **Usługi wdrożeniowe** | Konfiguracja oraz podłączenie 76 stacji roboczych zgodnie z wymaganiami Zamawiającego. |  |
| Konfiguracja oraz instalacja infrastruktury serwerowej (2 serwery, 1 macierz dyskowa, 1 dysk sieciowy) zgodnie z wymaganiami Zamawiającego. |  |
| Konfiguracja oraz instalacja urządzeń sieciowych (1 x UTM plus spięcie z istniejącym UTM-em do pracy HA, 2 x switch FC, 2 x switch dystrybucyjny, 12 x switch dostępowy). |  |
| Wdrożenie oprogramowania do backupu zgodnie z wymaganiami Zamawiającego. |  |
| Konfiguracja oraz instalacja 2 x UPS zgodnie z wymaganiami Zamawiającego. |  |
| Centrum certyfikacji – Usługa wdrożenia wewnętrznego centrum certyfikacji obejmować będzie wygenerowanie podpisów niekwalifikowanych dla pracowników Szpitala, które będą służyć tylko i wyłącznie jako forma elektronicznego potwierdzenia sporządzenia danego dokumentu medycznego przez daną osobę personelu medycznego.  |  |
| **Wymagania** | Dostawca powinien dostarczyć min. 2 referencje potwierdzające posiadanie min. jednej osoby technicznej (wdrożeniowca) zajmującego się utrzymaniem podobnej wielkości infrastruktury tj. 2x UTM, 2 serwery, 1 macierz dyskowa, 2x switch przez okres minimum 3 lat. Referencje powinny potwierdzać realizację usług na rynku usług medycznych. |  |

# **12. Gwarancja**

Zamawiający wymaga zapewnienia minimum 36-miesięcznego okresu gwarancji na dostarczony sprzęt zgodnie z warunkami określonymi we Wzorze umowy (Dodatek nr 8b do SIWZ).