Opis Przedmiotu Zamówienia

Dostawa sprzętu teleinformatycznego wraz z wzrostem dostępności eUsług w obszarze zdrowia świadczonych przez Okręgowy Szpital Kolejowy w Katowicach

Katowice, 15 maja 2023 r.

Spis treści

Słownik pojęć

Na potrzeby niniejszego postępowania stosuje się następujące pojęcia i definicje:

1. Administrator - Użytkownik konfigurujący i zarządzający Systemem i Infrastrukturą.
2. Analiza – dokumenty opracowane przez Wykonawcę, mające na celu doprecyzowanie sposobu realizacji wymagań Zamawiającego, zasad i metod realizacji Umowy oraz wskazanie i szczegółowe opisanie Produktów;
3. API - Application Programming Interface, interfejs programowania aplikacji – jest to sposób rozumiany, jako ściśle określony zestaw reguł i ich opisów, w jaki programy komunikują się między sobą. API definiuje się na poziomie kodu źródłowego dla takich składników oprogramowania jak np. aplikacje, biblioteki czy system operacyjny. Zadaniem API jest dostarczenie odpowiednich specyfikacji podprogramów, struktur danych, klas obiektów i wymaganych protokołów komunikacyjnych.
4. Architektura systemu teleinformatycznego – opis składników systemu teleinformatycznego, powiązań i relacji pomiędzy tymi składnikami.
5. ASI – Administrator Systemów informatycznych – stanowisko lub zespół posiadające uprawnienia administratora systemów IT.
6. Backup – wykonanie kopii bezpieczeństwa danych pozwalających na odtworzenie i przywrócenie Bazy Danych i Systemu po wystąpieniu awarii w przypadku utraty lub uszkodzenia oryginalnych danych; jakość odtworzonych danych powinna być dostosowana do ustalonego uprzednio poziomu ryzyka, który poniesie Zamawiający.
7. Baza Danych – zbiór wszystkich danych zewidencjonowanych za pomocą Systemu.
8. Czas dostarczenia rozwiązania - Okres czasu od wysłania Zgłoszenia do usunięcia przyczyny problemu lub zastosowania Rozwiązania Zastępczego.
9. Czas Roboczy – czas pracy liczony w Dni Robocze, w którym świadczona jest pomoc telefoniczna przy eksploatacji Systemu.
10. Dokumentacja – dokument papierowy lub elektroniczny opisujący System i zasady użytkowania Systemu. Wszelka dokumentacja sporządzona przez Wykonawcę dostarczona i modyfikowana w wyniku realizacji umowy.
11. Dostępność – właściwość określająca, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w założonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym .
12. Dysfunkcja – zbiorcze określenie dla nieprawidłowości rozumianych jako niezgodność z Dokumentacją lub też uciążliwość w pracy z Systemem.
13. Dzień Roboczy – dzień kalendarzowy od poniedziałku do piątku z wyłączeniem świąt i dni ustawowo wolnych od pracy.
14. EDM – Elektroniczna Dokumentacja Medyczna zgodnie z zapisami ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia.
15. ePUAP – Elektroniczna Platforma Usług Administracji Publicznej https://epuap.gov.pl
16. Godziny robocze – czas pracy liczony w Dni Robocze w godzinach 7:30 – 15:30.
17. HA – (ang. High Availability) - tryb wysokiej dostępności to sposób zapewnienia, że system lub aplikacja będzie dostępna dla użytkowników przez większość czasu. Technikami HA można nazwać klastrowanie, replikacja, redundancja, monitorowanie, plan awaryjny.
18. Integralność – właściwość polegająca na tym, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony .

19. Kategoria Dysfunkcji - kategoria, do której kwalifikowane jest Zgłoszenie Serwisowe dotyczące Dysfunkcji. Opisane szczegółowo w Załączniku nr 3 do Umowy.
20. Konsultant serwisowy – osoba fizyczna posiadająca odpowiednie kwalifikacje uprawniające do realizowania Serwisu.
21. Moduł systemu – kompletny zestaw narzędzi informatycznych obejmujących wszystkie warstwy architektury systemu, który dostarcza aplikację przeznaczoną dla użytkownika końcowego do realizacji określonych dziedzin działalności Zamawiającego.
22. Naprawa – modyfikacja Systemu usuwająca Dysfunkcję Systemu.
23. Obejście - tymczasowe rozwiązanie pozwalające na prawidłowe wykorzystanie oprogramowania bez usuwania wykrytego błędu przy zachowaniu integralności bazy danych.
24. Okno Serwisowe – przerwa w działaniu systemu w godzinach pracy [tj. pomiędzy 7:30 a 15:30] w dni robocze Zamawiającego, mająca na celu umożliwienie prowadzenie prac serwisowych wymagających czasowego wyłączenia systemu [np. aktualizacja].
25. Oprogramowanie aplikacyjne – Dziedzinowy system informatyczny klasy HIS [Hospital Information System] na którego bazie zbudowane będą e-Usługi jak również samo oprogramowanie e-Usług i Portalu.
26. Oprogramowanie standardowe – Każde oprogramowanie niezbędne, poza oprogramowaniem aplikacyjnym niezbędne do działania Systemu.
27. P1, P2 – Programy monitorowane i realizowane przez CSIOZ (systemy zewnętrzne)
28. Pomoc Telefoniczna – świadczenie konsultacji telefonicznej dotyczące szeroko pojętej eksploatacji Systemu.
29. Portal Usług Elektronicznych – portal udostępniający usługi elektroniczne dostarczane przez System dla użytkowników wewnętrznych i zewnętrznych
30. Prace Serwisowe - działania Wykonawcy mające na celu realizację Zgłoszenia Serwisowego.
31. Procedura – schemat postępowania w jaki winien być realizowany określony fragment Przedmiotu Umowy.
32. Przedmiot Umowy – całokształt zagadnień realizowanych w ramach Umowy ukierunkowanych na osiągnięcie Celu Umowy.
33. Publikacja – udostępnienie Systemu zawierającego zmienioną funkcjonalność.
34. PZ ePUAP – Profil Zaufany ePUAP
35. Realizacja Zgłoszenia Serwisowego - zakończenie Prac Serwisowych, w wyniku których przywrócono Stan Funkcjonalności.
36. Serwer – sprzęt komputerowy, na którym zainstalowana jest baza danych lub aplikacje wykorzystywane przez System.
37. Serwis – usługa o charakterze technicznym, organizacyjnym, doradczym i szkoleniowym, przeznaczona do zapewnienia stabilnej pracy Systemu.
38. Stan Funkcjonalności - stan Systemu, w którym nie występują Dysfunkcje.
39. Strony Umowy – uogólnione pojęcie stosowane zamiennie do określenia Zamawiającego i Wykonawcy jednocześnie.
40. System – Łączne określenie dla oprogramowania i sprzętu – objętego wdrożeniem oraz umową serwisową z Wykonawcą, bez względu na nazwę handlową. Obejmujący Platformę systemowo-sprzętową, Oprogramowania aplikacyjne oraz inne oprogramowanie niezbędne do działania e-Usług realizowanych w niniejszym zamówieniu.

41. System zewnętrzny - Każdy System informatyczny niebędący przedmiotem Zamówienia a oddziaływujący na przedmiot zamówienia.
42. Update – aktualizacja Systemu w wyniku zmian przepisów, związanych bezpośrednio i pośrednio z systemem ochrony zdrowia, w zakresie tej samej wersji Systemu.
43. Upgrade – nowa wersja Systemu związana ze stworzeniem nowej funkcjonalności.
44. Usługi elektroniczne (e-Usługi) – usługi, których świadczenie odbywa się za pomocą Internetu, jest zautomatyzowane (może wymagać niewielkiego udziału człowieka) i zdalne. Od usługi w ujęciu tradycyjnym, e-Usługę odróżnia brak udziału człowieka po drugiej stronie oraz świadczenie na odległość.
45. Użytkownik - Osoba, która jest pracownikiem Zamawiającego, posiada swój unikalny login i hasło.
46. Wdrożenie – opisane Umową świadczenia Wykonawcy mające na celu wykonanie Systemu
47. Web Service - Usługa sieciowa dostarczająca określoną funkcjonalność poprzez sieci Internet, niezależnie od platformy sprzętowej i implementacji.
48. Wersja – okresowa Publikacja Systemu uwzględniająca Naprawy i zmiany dokonane w okresie od poprzedniej Publikacji Systemu. Wydanie Wersji obejmuje również opis nowej Funkcjonalności Systemu.
49. Wykonawca – wybrany w drodze zamówienia publicznego podmiot realizujący niniejszy przedmiot zamówienia.
50. Zdalny dostęp – możliwość realizacji usług wsparcia, wdrożenia i gwarancji związanych z systemem z dowolnego miejsca za pośrednictwem bezpiecznego połączenia internetowego.
51. Zgłoszenie Serwisowe – Dysfunkcja, o której Wykonawca został powiadomiony drogą mailową.

Wstęp

Niniejszy dokument stanowi Opis Przedmiotu Zamówienia (OPZ) w zakresie dostawy i wdrożenia sprzętu służącego realizacji projektu w Szpitalu. Wszystkie parametry techniczne określone w niniejszym OPZ określają minimalne wymagania stawiane oferowanym urządzeniom. Wykonawca nie ma prawa żądać dodatkowego wynagrodzenia jeśli dostarczone elementy systemów posiadały będą większą funkcjonalność niż wymagana niniejszym OPZ.

1. Ogólny zarys projektu

Zakresem Zamówienia jest dostawa i wdrożenie wszystkich elementów niezbędnych do realizacji projektu, którego celem jest poprawienie dostępności do wysokiej jakości e-Usług publicznych w obszarze zdrowia w województwie śląskim (m.in. e-Rejestracja, e-Dokumentacja, e – Opieka). Osią projektu i jego głównym beneficjentem będzie pacjent. W wyniku realizacji projektu poprawi się dostępność do elektronicznych danych medycznych w regionie poprzez stworzenie w województwie śląskim ujednoliconego i spójnego systemu informatycznego pozwalającego na składowanie, przetwarzanie i udostępnianie danych medycznych w postaci elektronicznej.

W ramach projektu wyodrębnione zostały trzy obszary:

- dostosowanie infrastruktury i oprogramowania celem spełnienia wymogów platformy,
- wymiana danych poprzez serwery komunikacyjne,
- wykorzystanie danych celem podniesienia jakości świadczonych usług dla pacjenta.

Zamówienie obejmuje:

1. Dostawę rozwiązań zbierania i analizy logów, systemu ochrony i akceleracji sieciowych (serwery dedykowane na którym też zostaną postawione rozwiązania do zbierania i analizowania logów) oraz sprzętowe rozwiązanie ochrony w punkcie styku typu UTM na potrzeby wdrażanego Oprogramowania.
2. Dostawę powiązanych z wdrażanym ZSI urządzeń peryferyjnych tj. komputerów oraz komputerów przenośnych.
3. Instalacja, wdrożenie, konfiguracja i uruchomienie sprzętu oraz niezbędnego oprogramowania w ramach zamówienia na sprzęcie wskazanym przez Zamawiającego (zbieranie i analiza logów, systemu ochrony i akceleracji sieciowych, UTM).

2. Etapy dostaw i wdrożenia sprzętu wraz z oprogramowaniem

Zamawiający oczekuje, że Wykonawca przedstawi Szczegółowy Harmonogram Dostaw i Wdrożenia sprzętu wraz z oprogramowaniem. Zostanie on opracowany zgodnie ze szczegółową strukturą zadań oraz produktów poszczególnych etapów projektu z uwzględnieniem spodziewanych przez Zamawiającego dat uruchomienia poszczególnych elementów infrastruktury teleinformatycznej, jednak nie mniej niż w podziale na:

1. Prace przygotowawcze, lista sprzętu i niezbędnego oprogramowania,
2. Dostawa licencji, instalacja oprogramowania i sprzętu na infrastrukturze Zamawiającego,
3. Wdrożenie poszczególnych rozwiązań teleinformatycznych w kolejności pozwalającej na optymalne obciążenie pracą zespołu Zamawiającego i Wykonawcy, obejmujące podział na: prace konfiguracyjne, szkolenia personelu (administratorów),
4. Terminy i zakresy dostaw jak i terminy instalacji oraz wdrożenia. Zamawiający oczekuje, że Wykonawca określi przewidywane:
    - Terminy dostaw;
    - Terminy instalacji i konfiguracji;
    - Terminy wdrożenia wraz ze niezbędnymi szkoleniami.

Wszystkie wymienione produkty projektu (etapów) wym. w harmonogramie podlegają odbiorowi przez Zamawiającego.

3. Wymagania ogólne

Elementy sprzętu i oprogramowania musu być wdrożony zgodnie z obowiązującymi przepisami prawa (w szczególności ustawy o systemie informacji w ochronie zdrowia oraz ustawą o działalności leczniczej oraz ustawą o finansach publicznych), zgodnie ze strukturą organizacyjną i regulaminami Zamawiającego, rozporządzeniami oraz dobrymi praktykami.

Zamawiający wymaga, by dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej na dzień jego instalacji (tzn. powinno być dostosowane do zmieniających się powszechnie obowiązujących przepisów prawa lub regulacji wewnętrznych Zamawiającego).

Dostarczany w ramach postępowania sprzęt i oprogramowanie nie może być przeznaczony do wycofania z produkcji, sprzedaży lub wsparcia technicznego.

Dostarczone elementy sprzętu i oprogramowania muszą umożliwiać działanie w architekturze wysokiej dostępności (HA).

Sprzęt i oprogramowanie muszą gwarantować integralność danych, bieżącą kontrolę poprawności wprowadzanych danych, spójność danych.

Sprzęt i oprogramowanie musi posiadać mechanizmy ochrony danych przed niepowołanym dostępem, nadawania uprawnień dla użytkowników do korzystania jak również do korzystania z wybranych funkcji. W miarę możliwości elementy systemu muszą być integrowane z systemem domenowym na poziomie użytkownika.

Dla dostarczonego oprogramowania należy dostarczyć: licencje, nośniki instalacyjne, instrukcje użytkownika i administratora (w formie elektronicznej).

4. Dostawa sprzętu i oprogramowania systemowego

Poniżej przedstawiono parametry minimalne jaki dostarczany sprzęt musi spełniać. W przypadku gdy do realizacji Przedmiotu Zamówienia wymagany jest sprzęt/oprogramowanie/licencje nieujęte w poniższym zestawieniu Wykonawca musi go dostarczyć i wykazać w wykazie asortymentowo-cenowym.

4.1 Stacje robocze wraz z monitorem – 35 szt.

Zamawiający wymaga dostarczenia łącznie 35 szt. stacji roboczych spełniających poniższe parametry minimalne.

Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
Komputer	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji.
Obudowa	Typu Mini Tower (stalowa lub aluminiowa) zamknięta skrzynka w formie prostopadłościanu z elementami plastikowymi, umożliwiająca umieszczenie i zamocowanie najważniejszych elementów komputera. Postawione wymagania dla obudowy: • wewnątrz - 8.9 cm (3.5") • 1 wewnątrz - 6.4 cm (2.5") • z przodu dostępne - 13.3 cm (5.25") • 1 z przodu dostępny - 8.9 cm (3.5") • na froncie dostępne porty 2x USB 3.2, 2x 3.5mm Jack (Audio + Mic);
Chipset	Dostosowany do zaoferowanego procesora
Płyta główna	Zaprojektowana i wyprodukowana przez producenta komputera, trwale oznaczona nazwą producenta komputera (na etapie produkcji). Płyta główna wyposażona w min. 2 złącza 1 x PCI Express 4.0 x16 oraz 2x PCI Express x 1. Wbudowana karta sieciowa 1 Gbit z obsługą WOL.
Procesor	Procesor o min. 6 rdzeni, 12 wątków. Częstotliwość procesora min. 3,9 GHz, w trybie turbo 4,4 GHz, 16MB cache, bazowe TDP – 65W, ze zintegrowaną kartą graficzną, osiągający wynik minimum 19850 punktów na podstawie Performance Test w teście CPU Mark według wyników opublikowanych na https://www.cpubenchmark.net/cpu_list.php
Pamięć operacyjna	Min. 8 GB, 3200MHz DDR4, 4 sloty na pamięć, z czego min. 2 wolne. Możliwość pracy pamięci w trybie dual channel z możliwością rozbudowy do 128 GB.
Dysk twardy	1 Dysk: min 500 GB SSD PCIe/NVMe, prędkość odczytu min. 3500MB/s, zapisu min. 2300MB/s
Napęd optyczny	Nagrywarka DVD +/-RW
Karta graficzna	Zintegrowana karta graficzna z procesorem.
Audio	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition.
Sieć	Karta sieciowa LAN obsługująca prędkości 10/100/1000
Porty/złącza	Wbudowane porty: - 1 x HDMI,

	- 2 x DP, - 6 x USB w tym min.: 4x USB 3.2 oraz 2 x USB-C; - port sieciowy RJ-45, - port szeregowy RS-232 - porty słuchawek i mikrofonu na przednim lub tylnym panelu obudowy Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.
Klawiatura/mysz	Kolor: czarny Gwarancja: 36 miesięcy
Zasilacz	O mocy minimum 400W; wentylator zasilacza o wymiarach 120x120mm. MTBF na poziomie minimum 100000h Wtyczki: 1 x 20+4pin / 1 x 4pin / 3 x SATA / 2 x MOLEX 4pin / 1 x FDD 4pin Dodatkowe informacje: Certyfikat 80 Plus BRONZE / Ochrona OVP, OCP i SCP / Aktywne PFC Pobór mocy w trybie czuwaniaØ 1.4 Watt (S3 Mode, Suspend to RAM, WOL aktywowany) 0,30 Watt Soft off (S5 Mode) Moc nominalna 63 kWh na rok (ETEC Typical Energy Consumption)
System operacyjny	System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 13. Możliwość sterowania czasem dostarczania nowych wersji systemu

	operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)." 24. Wbudowany mechanizm wirtualizacji typu hypervisor." 25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.

	32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 34. Możliwość tworzenia wirtualnych kart inteligentnych. 35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38. Mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty inteligentne i certyfikaty (smartcard), c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN e. Certyfikat/Klucz i uwierzytelnienie biometryczne 39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń system operacyjny zapewniający logowanie za pomocą poświadczeń Active Directory zgodny z oprogramowaniem HIS
BIOS	~~Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy.~~ ~~Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o:~~ ~~- modelu komputera, PN~~ ~~- numerze seryjnym,~~ ~~- numerze inwentarzowym (AssetTag),~~ ~~- MAC Adres karty sieciowej,~~ ~~- wersja Biosu wraz z datą produkcji,~~ ~~- zainstalowanym procesorze, jego taktowaniu i ilości rdzeni~~ ~~- ilości pamięci RAM wraz z taktowaniem,~~ ~~- stanie pracy wentylatora na procesorze~~ ~~- stanie pracy wentylatora w obudowie komputera~~ ~~- napędach lub dyskach podłączonych do portów SATA (model dysku twardego i napędu optycznego)~~ ~~Możliwość z poziomu Bios:~~ ~~- wyłączenia/włączenia selektywnego (pojedynczo) portów USB zarówno z przodu jak i z tyłu obudowy~~ ~~- wyłączenia selektywnego (pojedynczego) portów SATA,~~ ~~- wyłączenia karty sieciowej, karty audio, portu szeregowego,~~ ~~- możliwość ustawienia portów USB w jednym z dwóch trybów:~~ ~~1. użytkownik może kopiować dane z urządzenia pamięci masowej~~

	~~podłączonego do pamięci USB na komputer ale nie może kopiować danych z komputera na urządzenia pamięci masowej podłączone do portu USB~~ ~~2. użytkownik nie może kopiować danych z urządzenia pamięci masowej podłączonego do portu USB na komputer oraz nie może kopiować danych z komputera na urządzenia pamięci masowej~~ ~~- ustawienia hasła: administratora, Power-On, HDD,~~ ~~- blokady aktualizacji BIOS bez podania hasła administratora~~ ~~- wglądu w system zbierania logów (min. Informacja o update Bios, błędzie wentylatora na procesorze, wyczyszczeniu logów) - z możliwością czyszczenia logów~~ ~~- alertowania zmiany konfiguracji sprzętowej komputera~~ ~~- wyboru trybu uruchomienia komputera po utracie zasilania (włącz, wyłącz, poprzedni stan)~~ ~~- ustawienia trybu wyłączenia komputera w stan niskiego poboru energii~~ ~~- zdefiniowania trzech sekwencji bootujących (podstawowa, WOL, po awarii)~~ ~~- kontrola otwarcia i zamknięcia obudowy komputera za pomocą zamka elektromagnetycznego~~ ~~- załadowania optymalnych ustawień Bios~~ ~~bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.~~ Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: - modelu komputera, PN - numerze seryjnym, - numerze inwentarzowym (AssetTag), - MAC Adres karty sieciowej, - wersja Biosu wraz z datą produkcji, - zainstalowanym procesorze, jego taktowaniu i ilości rdzeni - ilości pamięci RAM wraz z taktowaniem, - stanie pracy wentylatora na procesorze - stanie pracy wentylatora w obudowie komputera - napędach lub dyskach podłączonych do portów SATA (model dysku twardego i napędu optycznego) Możliwość z poziomu Bios: - wyłączenia/włączenia selektywnego (pojedynczo) portów USB zarówno z przodu jak i z tyłu obudowy - wyłączenia selektywnego (pojedynczego) portów SATA, - wyłączenia karty sieciowej, karty audio, portu szeregowego, - możliwość ustawienia portów USB w jednym z dwóch trybów: 1. użytkownik może kopiować dane z urządzenia pamięci masowej podłączonego do pamięci USB na komputer ale nie może kopiować danych z komputera na urządzenia pamięci masowej podłączone do portu USB 2. użytkownik nie może kopiować danych z urządzenia pamięci masowej podłączonego do portu USB na komputer oraz nie może kopiować danych z komputera na urządzenia pamięci masowej

	- ustawienia hasła: administratora, Power-On, HDD, - blokady aktualizacji BIOS bez podania hasła administratora - wglądu w system zbierania logów (min. Informacja o update Bios, błędzie wentylatora na procesorze, wyczyszczeniu logów) z możliwością czyszczenia logów - alertowania zmiany konfiguracji sprzętowej komputera - wyboru trybu uruchomienia komputera po utracie zasilania (włącz, wyłącz, poprzedni stan) - ustawienia trybu wyłączenia komputera w stan niskiego poboru energii - zdefiniowania trzech sekwencji bootujących (podstawowa, WOL, po awarii) - załadowania optymalnych ustawień Bios bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych
Zintegrowany System Diagnostyczny	Wizualny system diagnostyczny producenta działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera umożliwiający na wykonanie diagnostyki następujących podzespołów: • wykonanie testu pamięci RAM • test dysku twardego • test monitora • test magistrali PCI-e • test portów USB • test płyty głównej Wizualna lub dźwiękowa sygnalizacja w przypadku uszkodzenia bądź błędów któregokolwiek z powyższych podzespołów komputera. Ponadto system powinien umożliwiać identyfikacje testowanej jednostki i jej komponentów w następującym zakresie: • PC: Producent, model • BIOS: Wersja oraz data wydania Bios • Procesor : Nazwa, taktowanie • Pamięć RAM : Ilość zainstalowanej pamięci RAM, producent oraz numer seryjny poszczególnych kości pamięci • Dysk twardy: model, numer seryjny, wersja firmware, pojemność, temperatura pracy • Monitor: producent, model, rozdzielczość System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera.
Certyfikaty i standardy	- Certyfikat ISO9001:2000 dla producenta sprzętu (należy załączyć do oferty) - ENERGY STAR - 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 - Komputer posiadający certyfikację EPEAT, na poziomie GOLD, znajdujący się na liście GEC pod adresem: https://www.epeat.net/search-computers-and-displays (wymaganie nieobligatoryjne - dodatkowo punktowane)

Waga/rozmiary urządzenia	Wysokość urządzenia nie większa niż 42 cm
Bezpieczeństwo	- Złącze typu Kensington Lock - ~~Możliwość wyposażenia obudowy komputera w zamek elektromagnetyczny sterowany z poziomu BIOS, chroniącym przed nieautoryzowanym dostępem do komputera (wymaganie nieobligatoryjne – dodatkowo punktowane~~)
Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji.
Oprogramowanie	Dedykowane oprogramowanie producenta sprzętu umożliwiające automatyczna weryfikacje i instalację sterowników oraz oprogramowania użytkowego producenta w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralna bazą sterowników i oprogramowania użytkowego producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika. Oprogramowanie musi być wyposażone w moduł rejestru zdarzeń, w którym znajdują się informacje o tym kiedy i jakie sterowniki zostały zainstalowane na danej maszynie. Oprogramowanie musi zapewniać również ustawienie automatycznego uaktualnienia wszystkich sterowników we wskazanym dniu miesiąca.
Oprogramowanie biurowe	Office 2021 Standard lub 2021 Pro Plus lub równoważne zapewniające poprawną wymianę dokumentów biurowych w jednostce oraz zapewniający klienta poczty wspierającego integrację z pakietem biurowym oraz wbudowanym kalendarzem pozwalającym na przesyłanie drogą elektroniczną planowanych spotkań.
Gwarancja	Min. 24 miesiące door-to-door Gwarancja musi być realizowana przez producenta lub autoryzowanego serwis partnera producenta.
Wsparcie techniczne producenta	- możliwość weryfikacji u producenta konfiguracji fabrycznej i oferowanej zakupionego sprzętu - możliwość weryfikacji na stronie producenta posiadanej/wykupionej gwarancji - możliwość weryfikacji statusu naprawy urządzenia po podaniu unikalnego numeru seryjnego - Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.
Aspekty środowiskowe	Zaoferowanie jednostki z zastosowaniem w produkcie tworzyw sztucznych pochodzących z recyklingu w ilości przekraczającej 30% (parametr musi być weryfikowalny na podstawie oficjalnej dokumentacji producenta). – Wymaganie nieobligatoryjne – dodatkowo punktowane.
Monitor	Ilość równa ilości komputerów
Przekątna	Min. 23.8"
Panel	IPS LED, wykończenie matowe
Rozdzielczość	1920 x 1080
Jasność	Min. 250 cd/m2

Plamka	Maks 0.28mm
Kontrast statyczny	Min. 1000:1
Czas reakcji	~~maks. 4ms~~ maks. 5 ms.
Kąty widzenia	Min. Poziomo – 178 stopni, Pionowo – 178 stopni
Wbudowane złącza	Min. 1x VGA, 1x HDMI, 1x DISPLAY PORT, 2x USB, wyjście słuchawkowe, Kensington Lock
Głośniki	Wbudowane min. 2x2W
Funkcje	Redukcja światła niebieskiego, Flicker free,
Regulacja	Regulacja wysokości min. 130 mm, rotacja w Pivot min. 90 stopni, obrót stopy min. 90 stopni, kąty pochylenia min. 22 stopni w górę oraz 5 stopni w dół
Certyfikaty	Min. TCO, CE, REACH (do oferty załączyć oświadczenie producenta sprzętu)
Wymagania dodatkowe:	Sprzęt fabrycznie nowy, oryginalnie zapakowany, bez śladów użytkowania, oznaczony logo producenta. Możliwość pobrania sterowników oraz obrazu systemu ze strony producenta po podaniu numeru seryjnego. Sprzęt wyprodukowany w Europie, nie wcześniej niż w 2023 roku. Na sprzęcie powinien być umieszczony symbol legalności systemu operacyjnego w formie naklejki/hologramu potwierdzający jego autentyczność W ramach dostawy sprzętu Wykonawca zapewni również: - Instalację sprzętu w miejscu wskazanym przez Zamawiającego. - Uruchomienie, przetestowanie i wstępną konfigurację zgodnie z wytycznymi Zamawiającego. Stacja robocza i monitor muszą być tego samego producenta

4.2 Komputery przenośne – 15 szt.

Zamawiający wymaga dostarczenia łącznie 15 szt. komputerów przenośnych spełniających poniższe parametry minimalne.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Komputer	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji.
Typ	Przenośny laptop/notebook itp.
Ekran	Przekątna 15,6" o rozdzielczości FHD (min. 1920x1080 przy 60Hz) z powłoką przeciwodblaskową

Procesor	Min. 6 rdzeni, 12 wątków, ze zintegrowaną grafiką, taktowanie bazowe 2,1GHz, w trybie turbo 4,0GHz, 8MB cache, osiągający w teście PassMark CPU Mark wynik min. 13100 punktów (należy dołączyć wydruk ze strony https://www.cpubenchmark.net z wynikiem testu dla oferowanego procesora). Pobór mocy TDP Typical nie większy niż 15W.
Płyta główna:	Wyposażona przez producenta w dedykowany chipset dla oferowanego procesora.
Pamięć operacyjna	min. DDR4 16GB o taktowaniu nie niższym niż 3200MHz, 1 slot wolny, możliwość rozbudowy pamięci do 32GB
Parametry pamięci masowej:	Dysk SSD M2 o pojemności min. 512GB, prędkość odczytu/zapisu minimum: 3100/1800 MB/s, możliwość instalacji drugiego dysku 2.5cala w obudowie
Karta graficzna:	Zintegrowana z procesorem z dynamicznie przydzielaną pamięcią współdzieloną.
Wyposażenie multimedialne:	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wbudowane głośniki
Komunikacja:	Wbudowana karta sieci bezprzewodowej 802.11 a/b/g/n/ac, moduł Bluetooth w wersji min. 5.0, karta sieciowa 10/100/1000 ze złączem RJ-45, możliwość instalacji modemu LTE wewnątrz obudowy (nie dopuszcza się modemu podłączanego do portu USB)
Klawiatura:	Układ klawiszy US, klawiatura podświetlana z możliwością czterostopniowej regulacji podświetlenia oraz zmiany koloru podświetlenia, wydzielony blok klawiszy numerycznych
Bateria i zasilanie:	Komputer wyposażony w baterię o pojemności min. 36Wh umożliwiającą pracę przez min. 360 minut (wg. danych producenta) oraz zasilacz.
Certyfikaty:	Certyfikat CE, ISO14001, ISO9001 lub równoważne
System operacyjny:	W pełni będzie integrował się z istniejącą usługą Active Directory, w tym GPO (m.in. automatyzacja procesów instalacji oprogramowania). Wykonawca ma obowiązek dostarczyć sprzęt z systemem operacyjnym Windows 11 Pro PL (wersja 64 – bitowa). Klucz systemu musi być zapisany trwale w BIOS i umożliwiać instalację systemu operacyjnego z nośnika lub napędu lub zdalnie bez potrzeby ręcznego wpisywania klucza licencyjnego.
Oprogramowanie:	Office 2021 Standard lub 2021 Pro Plus lub równoważne zapewniające poprawną wymianę dokumentów biurowych w jednostce oraz zapewniający klienta poczty wspierającego integrację z pakietem biurowym oraz wbudowanym kalendarzem pozwalającym na przesyłanie drogą elektroniczną planowanych spotkań.
Gwarancja:	Min. 24 miesiące door-to-door Gwarancja musi być realizowana przez producenta lub autoryzowanego serwis partnera producenta.
Wymagania dodatkowe:	Wbudowana kamera internetowa trwale zainstalowana w obudowie matrycy, wejście audio, wbudowany mikrofon, wbudowane głośniki, czytnik kart pamięci, złącza USB – min. 4 szt. w tym 1x USB 3.1 Type-C i 1x USB 3.1 Type-A, wyjście HDMI, Touchpad, TPM 2.0, gniazdo Kensington Lock, waga max 1,6 kg, sprzęt fabrycznie nowy, oryginalnie zapakowany, bez śladów użytkowania. Możliwość pobrania sterowników oraz obrazu systemu operacyjnego ze strony producenta po podaniu numeru seryjnego.

	Sprzęt wyprodukowany w Europie, nie wcześniej niż w 2023 roku. Laptop trwale oznaczony logo producenta. Na sprzęcie powinien być umieszczony symbol legalności systemu operacyjnego w formie naklejki/hologramu potwierdzający jego autentyczność W ramach dostawy sprzętu Wykonawca zapewni również: - Instalację sprzętu w miejscu wskazanym przez Zamawiającego. - Uruchomienie, przetestowanie i wstępną konfigurację zgodnie z wytycznymi Zamawiającego.

4.3 Stacje zbierania i analizy logów – 1 szt.

Zamawiający wymaga dostarczenia łącznie 1 szt. sprzętu lub oprogramowania do zbierania i analizy logów sieci i systemów informatycznych, które są zgodne z poniższym opisem wymagań lub/i parametrami technicznymi.

Wymaganie	Opis oraz parametry techniczne
Ogólne	Narzędzia do monitorowania sieci i systemów informatycznych, które umożliwia w czasie rzeczywistym zbieranie i analizowanie danych z różnych źródeł. Oprogramowanie to pozwala na monitorowanie wydajności systemów, zasobów sieciowych oraz aplikacji, gdzie zostaną zapisane logi systemowe celem zapewnienia niezbędnego bezpieczeństwa.
Monitorowanie aktywności sieci	Umożliwia monitorowanie aktywności sieci, w tym przepływu danych, obciążenia interfejsów sieciowych i wykorzystania pasma.
Monitorowanie stanu urządzeń	Pozwala na monitorowanie stanu urządzeń, takich jak serwery, routery, przełączniki i inne urządzenia sieciowe, w celu wykrywania i eliminowania problemów z nimi związanych.
Monitorowanie usług	Umożliwia monitorowanie usług, takich jak serwery WWW, bazy danych i inne aplikacje, w celu zapewnienia ich niezawodności i wykrywania problemów.
Alarmowanie	Pozwala na konfigurowanie alarmów i powiadomień w przypadku wykrycia problemów w systemie.
Automatyzacja	Umożliwia automatyzację niektórych procesów, takich jak restartowanie usług w przypadku awarii, wykonywanie skryptów, generowanie raportów i wiele innych.
Raportowanie	Posiada funkcjonalność raportowania, która umożliwia generowanie raportów dotyczących wydajności systemu oraz trendów i statystyk.
Wizualizacja	Zapewnia wiele narzędzi wizualizacji danych, w tym wykresy, diagramy, tabele i wiele innych
Analityka	Umożliwia analizę danych zebranych przez system, co umożliwia wykrywanie trendów i ustalanie korelacji między różnymi parametrami.
Dostępność	Kompatybilny z następującymi interfejsami: 1. Interfejs www – główny interfejs użytkownika, który pozwala na konfigurację i zarządzanie systemem monitorowania, w tym dodawanie hostów, monitorowanie usług, tworzenie raportów, przeglądanie logów i wiele więcej. 2. Interfejs konsolowy – alternatywny interfejs użytkownika, który pozwala na wykonywanie poleceń wiersza poleceń. 3. Interfejs API – umożliwiający automatyzację i integrację z innymi systemami. API powinno dostarczać RESTful API, JSON-RPC API oraz XML-RPC API, które można wykorzystać do integracji z innymi narzędziami i aplikacjami.

Zarządzanie	1. Możliwość tworzenia hostów 2. Tworzenie szablonów 3. Konserwacja i aktualizacja 4. Tworzenie triggerów i alarmów
Dodatkowe wymagania	Możliwość zintegrowania z wieloma systemami operacyjnymi i aplikacjami, takimi jak Linux, Windows, VMware, Docker, MySQL i PostgreSQL.

4.4 System ochrony i akceleracji aplikacji sieciowych – 2 szt.

Zamawiający wymaga dostarczenia łącznie 2 szt. sprzętowego rozwiązania, które ma wesprzeć system ochrony i akceleracji aplikacji sieciowych według poniższych minimalnych wymagań:

Nazwa komponentu	Wymagane minimalne parametry techniczne/funkcjonalne
Obudowa	• Typu RACK, wysokość nie więcej niż 1U; • Szyny umożliwiające wysunięcie serwera z szafy stelażowej bez odłączania urządzania • Ramię porządkujące ułożenie przewodów z tyłu serwera; • Możliwość zainstalowania 8 dysków twardych hot plug, 8 dysków SFF 2,5'' typu Hot Swap, SAS/SATA/SSD. • Zainstalowane 2 dyski SSD o pojemności minimum 240GB każdy, bez konieczności zajmowania slotów dyskowych hot-plug, z zabezpieczeniem minimum RAID1 • Możliwość zainstalowania dedykowanego wewnętrznego napędu blue-ray
Płyta główna	• Dwuprocesorowa; • Wyprodukowana i zaprojektowana przez producenta serwera • Możliwość instalacji procesorów 40-rdzeniowych; • Zainstalowany moduł TPM 2.0 • Sloty rozszerzeń o Wymagane dwa sloty OCP V3 z możliwością instalacji dwóch kart jednocześnie o trzy aktywne gniazda PCI-Express Generacji 3 lub 4 • 32 gniazda pamięci DIMM; • Obsługa minimum 4TB pamięci RAM; • Wsparcie dla technologii: o obsługi zabezpieczeń: min. ECC i SDDC o obsługi mechanizmu Memory Mirroring, Memory Scrubbing o obsługę modułów pamięcii DCPMM
Procesory	• Procesor maksymalnie 8-rdzeniowy klasy x86 - 64 bity, osiągający w testach SPECint_rate_base2017 wynik nie gorszy niż 134 punkty w konfiguracji dwuprocesorowej dla oferowanego modelu serwera. Wymagana publikacja na stronach spec.org raportu potwierdzającego uzyskanie wymaganego wyniku wydajności przez oferowany model serwera wyposażonego w oferowane procesory. • Liczba procesorów : 2 szt
Pamięć RAM	• 384GB RDIMM DDR4 2933MT/s DDR4 Registered
Kontrolery LAN	• Minimum 4 porty Ethernet 10Gbps z interfejsami SFP+ obsadzonymi

lub inne karty rozszerzeń	adapterami światłowodowymi pracującymi w trybie MultiMode. • Porty wyprowadzone z karty LAN nie mogą zajmować wolnego slotu rozszerzenia PCIe • Możliwość instalacji w serwerze drugiej karty LAN jw. • Serwer musi posiadać zainstalowana co najmniej 2-portową kartę HBA PCIe FC16Gbps, wyposażoną we wkładki optyczne dla podłączenia okablowania typu MultiMode
Kontrolery I/O	• Kontroler sprzętowy obsługujący poziom zabezpieczenia minimum RAID1 dla zainstalowanych dysków i zapewniający uruchomienie systemu operacyjnego Vmware.
Porty	• Zintegrowana karta graficzna ze złączem VGA z tyłu serwera; • 5 portów USB 3.0 • port szeregowy (RS232), możliwość wykorzystania portu serial do zarządzania serwerem; • Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera;
Zasilanie, chłodzenie	• Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy minimalnej 900W; • Redundantne wentylatory hotplug (min 8)
Karta/moduł zarządzający	Niezależna od system operacyjnego, zintegrowana z płytą główną serwera bez konieczności jej instalacji jako dodatkowej karty w slocie PCI Express. Karta zarządzająca musi zapewniać co najmniej poniższe funkcjonalności: • monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski (fizyczne i logiczne), karty sieciowe • dostęp do karty zarządzającej poprzez a) dedykowany port RJ45 do komunikacji wyłącznie z kontrolerem zarządzania, • dostęp do karty możliwy: a) z poziomu przeglądarki webowej (GUI), b) poprzez IPMI 2.0 (Intelligent Platform Management Interface), • wbudowane narzędzia diagnostyczne, • zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego, • obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie, • wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników, • przesyłanie alertów poprzez e-mail, • obsługa zdalnego serwera logowania (remote syslog), • Przywracanie funkcjonalności BIOS (tzw. BIOS RECOVERY) bez lokalnej interwencji serwisu lub pracownika. Bez konieczności otwierania

	serwera. • wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów CD/DVD, • monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji, • konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping), • Możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej (w szczególności bez pendrive, dysków twardych wewn. i zewn., itp.) – możliwość manualnego wykonania aktualizacji jak również możliwość automatyzacji. • możliwość równoczesnej obsługi GUI (otwarte sesje) przez minimum 16 użytkowników. • wsparcie dla Microsoft Active Directory • obsługa SSL i SSH, • wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 • Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną, posiadające dedykowany port RJ45. • moduł zarządzający musi wspierać protokół SSDP • rozszerzenie standardowych możliwości zdalnego zarządzania serwerem o funkcje bezpośredniego - z dedykowanego nośnika SD zainstalowanego w samym serwerze – wykonywania m.in.: aktualizacji sterowników i firmware'u, zaawansowanej diagnostyki stanu pracy serwera, konfiguracji i instalacji serwera bez użycia nośników USB czy DVD, zbierania logów i raportów o stanie serwera, zarządzania certyfikatami bezpieczeństwa dla użytkowników uprawnionych do zarządzania serwerem. Wszystkie te operacje mogą być obsługiwane w trybie Out-Of-band, tzn. bez względu na stan zainstalowanego systemu operacyjnego.
Wspierane OS	• Microsoft Windows Server 2016, 2019, Windows 2022 • Red Hat Enterprise Linux (RHEL) 8 • SUSE Linux Enterprise Server (SLES) 15 • VMware ESXi 6.x, 7.x, 8.x
Gwarancja	• 3 lata gwarancji producenta serwera w trybie on-site (na miejscu) z gwarantowanym przez producenta czasem naprawy do końca następnego dnia roboczego. Czas reakcji do 4h od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. • Aktywna funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu; • Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych;

	• Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie; • Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty);
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 – wymaganie oświadczenie wykonawcy lub producenta; • Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – na żądanie Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta • Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki; • W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej 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; • Oferowane Urządzenie musi posiadać certyfikację producenta serwera do poprawnej pracy ciągłej urządzenia w temperaturze otoczenia 35 stopni Celsiusa

4.5 System ochrony w punkcie styku typu UTM – 2 szt.

Zamawiający wymaga dostarczenia łącznie 2 szt. urządzeń UTM (z ang. Unified Threat Management) czyli rozwiązanie, które łączy w sobie kilka funkcjonalności związanych z bezpieczeństwem oraz zarządzaniem sieci komputerowych w jednym urządzeniu. W zależności od konkretnego modelu i producenta UTM powinien spełnić poniższe minimalne wymagania w oparciu o opis i ewentualne parametry techniczne.

Wymaganie	Opis oraz parametry techniczne
Ogólne	System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy

	sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System wspiera protokoły IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych. 5. System ma pracować w postaci redundantnego klastra.
Interfejsy, dysk oraz zasilanie	1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: • 10 portami Gigabit Ethernet RJ-45. 2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System jest wyposażony w zasilanie AC.
Wydajność	1. W zakresie Firewall'a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.3 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 750 Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla

	ruchu http – minimum 650 Mbps.
Funkcje systemu bezpieczeństwa	W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. 13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
Polityki, firewall	1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. 5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich

	przy budowaniu polityk kontroli dostępu. • Amazon Web Services (AWS). • Microsoft Azure. • Cisco ACI. • Google Cloud Platform (GCP). • OpenStack. • VMware NSX. • Kubernetes.
Zestawienia VPN	1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: • Wsparcie dla IKE v1 oraz v2. • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19, 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. • Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. • Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. • Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling" dla połączeń Client-to-Site. 2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta. • Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie zapewnia obsługę: 1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w

	nagłówkach IP). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
SD-WAN	1. 1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
Zarządzanie pasmem	1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System daje możliwość określania pasma dla poszczególnych aplikacji. 3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości. 4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze. 8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

	9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
Ochrona przed atakami	1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. 8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. 9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
Kontrola aplikacji	1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. 6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
Kontrola www	1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.

	2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. 4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. 3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. 4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. 3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.

	5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). 9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
Logowanie	1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 4. Możliwość włączenia logowania per reguła w polityce firewall. 5. System zapewnia możliwość logowania do serwera SYSLOG. 6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
Serwisy i licencje	Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: - Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.
Gwarancja oraz wsparcie	Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

5. Wdrożenie sprzętu i oprogramowania systemowego

Instalacja i konfiguracja platformy sprzętowej (serwerowej) obejmujące minimum:

A. Wypakowanie i utylizacja opakowań.
B. Montaż w miejscu przeznaczenia używania (odpowiednie szafy RACK).

C. Podłączenie do istniejącej infrastruktury sieci LAN i zasilania.
D. Aktualizacja oprogramowania wewnętrznego.

W zakresie komputerów PC i komputerów przenośny Zamawiający nie wymaga instalacji urządzeń na stanowiskach docelowych, komputery PC i komputery przenośne muszą jednak mieć zainstalowane oprogramowanie systemowe i skonfigurowane partycje odtwarzania systemu.

Konfiguracja i uruchomienie sprzętu oraz oprogramowania systemowego

Do zadań Wykonawcy w każdym z poniższych punktów należy: wypakowanie i utylizacja opakowań oraz montaż w miejscu przeznaczenia używania, ponad to co jest opisane poniżej.

Systemy ochrony i akceleracji sieciowych

Na sprzęcie należy zainstalować stacje (mogą być wirtualne) do analizy i gromadzenia logów i skonfigurować go do korzystania z w infrastrukturze w trybie HA. Wykonawca zaprojektuje schemat rozmieszczeń, ilości i przydział zasobów dla serwerów (wirtualnych) typu SIEM wymaganych do realizacji Przedmiotu Zamówienia zgodnie z zalecanymi wymaganiami instalowanych Systemów.

6. Przygotowanie i dostarczenie dokumentacji wstępnej oraz końcowej technicznej

W ramach zamówienia Wykonawca zobowiązuje się do gromadzenia i przechowywania wstępnej dokumentacji technicznej realizacji każdego Zadania. Dokumentacja projektowa będzie przechowywana przez cały okres realizacji projektu.

6.1 Wymagania dot. zakresu dokumentacji

Zamawiający wymaga, aby Wykonawca dostarczył do każdego przekazanego elementu sprzętu i oprogramowania dokumentację powykonawczą, którą należy traktować jako dokumentację techniczną. Dokumentacja musi zawierać wszystkie niezbędne loginy, hasła, kody dostępu, itp. pozwalające na odtworzenie pełnego zakresu systemu po awarii, zarządzanie w pełnym zakresem dostarczonym rozwiązaniem oraz pełnienie usługi serwisu przez inny podmiot po okresie trwałości projektu. Hasła muszą zostać dostarczone w zamkniętej kopercie i przekazane muszą być protokolarnie wyznaczonemu przedstawicielowi Zamawiającego.

W ramach zamówienia Dostawca przygotuje dokumentację wstępna, która zostanie zaakceptowana przez Zamawiającego.

Po wdrożeniu zostanie sporządzona dokumentacja powykonawcza związana z zagadnieniami powyżej oraz zostaną przeprowadzone instruktaże dla administratorów systemów (maksymalnie 2-dniowe).

Zamawiający wymaga aby Wykonawca we współpracy z Zamawiającym stworzył Politykę backupu i archiwizacji zgodnie z obowiązującymi przepisami prawa oraz wymaganiami dostarczonych systemów.

Dokumentacja musi być sporządzona w języku polskim.

7. Gwarancja i serwis

Wykonawca będzie świadczył na rzecz Zamawiającego usługi serwisu w zakresie przedmiotu zamówienia (umowy) w zaoferowanym okresie (licząc od daty podpisania protokołu odbioru) zapewniając jednocześnie odpowiednie wsparcie merytoryczne.

W ramach usługi Wykonawca zobowiązany jest do nieodpłatnego usuwania dysfunkcji:

- z przyczyn zawinionych przez Wykonawcę będących konsekwencją wystąpienia: błędu lub wady fizycznej pakietu aktualizacyjnego lub instalacyjnego, błędu w dokumentacji technicznej, błędu w wykonaniu usług przez Wykonawcę (wdrożenie lub konfiguracje);
- spowodowanych aktualizacjami sprzętu lub oprogramowania.

Zgłoszenia będą klasyfikowane zgodne ze słownikiem pojęć, zawarte w załącznikach do Umowy, przez Zamawiającego w uzgodnieniu z Wykonawcą w kwestii dotyczącej sprzętu.

W każdym przypadku Zgłaszający i Wykonawca mogą uzgodnić inny czas dostarczenia rozwiązania niż określono w warunkach. W takim przypadku niezbędne jest potwierdzenie ustalonego terminu w formie pisemnej.

Terminy wymienione w załącznikach do Umowy obowiązują w przypadku dostarczonego sprzętu.