1. Komputer przenośny - 5 szt.

Nazwa	Parametry minimalne
Zastosowanie	Komputer przenośny będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do internetu oraz poczty elektronicznej, jako lokalna baza danych
Matryca	Komputer przenośny z ekranem 15” o rozdzielczości: FullHD (1920 x 1080) z podświetleniem LED, jasność matrycy min. 250 cd/m2
Wydajność	Procesor osiągający w teście PassMark Performance Test, co najmniej 10 000punktów w kategorii Average CPU Mark. Wynik dostępny na stronie: https://www.cpubenchmark.net/cpu_list.php na dzień 18.02.2022 r.
Pamięć RAM	Min. 16 GB DDR4 możliwością rozbudowy do 32GB, Jeden wolny slot pamięci.
Pamięć masowa	Min. 500 GB SSD
Karta graficzna	Zintegrowana
Multimedia	• karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, • wbudowane głośniki stereo, • mikrofon wbudowany w obudowę matrycy, • klapka zasłaniająca kamerę
Bateria i zasilanie	Bateria 4-cell o pojemności min. 47 WHR. Zasilacz min 45 W
Waga i wymiary	Waga komputera z baterią nie większa niż 1.9 kg.
Obudowa	Wykonana z trwałych materiałów.
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 dla poszczególnych komponentów systemu).
BIOS	– BIOS zgodny ze specyfikacją UEFI, pełna obsługa za pomocą klawiatury i samego urządzenia wskazującego (touchpad/mysz). oraz samego urządzenia wskazującego (touchpad/mysz). Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: wersji BIOS, numerze seryjnym i dacie produkcji komputera, wielkości, prędkości i sposobie obsadzenia zainstalowanej pamięci RAM w slotach, typie, ilości rdzeni, min. i maks. prędkości zainstalowanego procesora oraz wielkości pamięci cache L2 i L3 zainstalowanego procesora, zainstalowanym dysku twardym (a w szczególności o jego pojemności), MAC adresie wbudowanej w płytę główną karty sieciowej, kontrolerze video, kontrolerze audio, przekątnej i natywnej rozdzielczości zainstalowanej matrycy, zainstalowanej karcie sieci bezprzewodowej, poziomie naładowania baterii wraz z informacją o mocy podłączonego zasilacza. – Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z USB.

	– Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych, ustawienia haseł na poziomie użytkownika, administratora (oddzielne hasła) – możliwość włączenia/wyłączenia zintegrowanego kontrolera USB, kontrolera audio, kamery, mikrofonu, głośników. – Oferowany BIOS musi posiadać poza swoją wewnętrzną strukturą menu szybkiego boot'owania, które umożliwia min.: uruchamianie systemu z zainstalowanego HDD, uruchamianie systemu z urządzeń zewnętrznych typu HDD-USB, USB Pendrive, uruchamianie systemu z serwera za pośrednictwem zintegrowanej karty sieciowej,
Bezpieczeństwo	• Układ szyfrowania TPM (Trusted Platform Module) lub analogiczny, • klawiatura odporna na zachlapanie lub zalanie • możliwość montażu na lince zabezpieczającej.
Certyfikaty	– Deklaracja zgodności CE
System operacyjny	a) System operacyjny klasy PC musi spełniać poniższe wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji. b) Możliwość dokonywania aktualizacji i poprawek systemu przez Internet oraz dodatkowo z możliwością wyboru instalowanych poprawek (możliwość scentralizowanego wyboru instalowanych poprawek dzięki dodatkowemu oprogramowaniu producenta). c) Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu. d) Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie w ofercie nazwy strony serwera WWW. e) System musi umożliwiać pracę w domenie. f) Wymagane jest aby dostarczona licencja systemu operacyjnego dopuszczała instalację systemu operacyjnego producenta, którego wsparcie dodatkowe wygasa nie wcześniej niż 1 października 2025 r. g) Internetowa aktualizacja zapewniona w języku polskim. h) Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IPv4 i IPv6. i) Wbudowane narzędzie do szyfrowania dysków w oparciu o TPM komputera. j) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe. k) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi). l) Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer. m) 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. n) Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu.

o) Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
p) 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.
q) Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych.
r) Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.
s) Wbudowany system pomocy w języku polskim.
t) Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).
u) Zarządzanie stacją roboczą poprzez polityki rozumiane jako zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji.
v) Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.
w) Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
x) Wsparcie dla logowania przy pomocy smartcard.
   - Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji.
   - Posiadanie narzędzi służących 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, 4.0, 5.0 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
   - Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń.
   - Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.
   - Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową.
   - Rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację.
   - Graficzne środowisko instalacji i konfiguracji.
   - Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.
   - Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.

	- 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 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). - System musi posiadać możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).
Wymagania pozostałe	Wbudowane porty i złącza: a) 1xHDMI, b) 1x RJ-45 (10/100/1000), c) min. 3x USB 3.2 Gen 1 d) 1 x DisplayPort over USB-C e) 1x Thunderbolt™ 4 over USB-C f) czytnik kart multimedialnych w formacie co najmniej SD, g) port audio combo (słuchawki oraz mikrofon), h) gniazdo ładowania, i) gniazdo linki zabezpieczającej, j) zintegrowana w postaci wewnętrznego modułu mini-PCI Express karta sieci WLAN 802.11AC z modułem bluetooth.
Warunki gwarancji	– gwarancja producenta na laptop) - min. 24 miesiące

2. Komputer stacjonarny - 10 szt.

Nazwa	Parametry minimalne
1. Typ komputera	Komputer stacjonarny

2. Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do zasobów lokalnej sieci komputerowej oraz usług sieci Internet, aplikacji graficznych wektorowych oraz rastrowych, a także danych multimedialnych.
3. Procesor	Wydajność obliczeniowa: Procesor, który powinien osiągać w teście wydajności PassMark PerformanceTest (wynik dostępny: http://www.passmark.com/products/pt.htm) co najmniej wynik 17500 punktów Passmark CPU Mark.
4. Płyta główna	– chipset dostosowany do oferowanego procesora lub równoważny – minimum 2 sloty pamięci lub więcej, obsługującej częstotliwość minimum 2999 MHz lub więcej – minimum 1 x PCI Express 3.0 x 16 – minimum 1 x PCI Express 3.0 x 4 (mechanicznie x16) – minimum 4x złącza SATA 6.0 Gb/s – minimum 1x M.2 dla dysku SSD o parametrach co najmniej PCIe 3.0 x4
5. Pamięć operacyjna RAM	– minimum 16 GB DDR4 – minimum 1 wolny slot pamięci na płycie głównej, – minimalny rozmiar możliwego rozszerzenia obsługiwanej pamięci, zapewniony i potwierdzony przez producenta komputera: 64 GB
6. Porty w tylnej części komputera	Komputer musi posiadać: – minimum 2 x Display Port 1.4 z obsługą funkcji Multi-Stream, – minimum 4 x USB, w tym co najmniej 2x USB 3.2 Gen 1, 2x USB 2.0 – minimum 1 port sieciowy RJ-45, – osobne porty audio line-in i line-out Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB oraz VIDEO nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.
6. Porty w przedniej części komputera	Komputer musi posiadać: - minumum 5 x USB, w tym min. 2 porty USB 3.2 Gen 1, 3 porty USB 2.0 oraz 1 port USB 3.2 Gen 1 Typ C (ładownie do 15W) – port audio do podłączenia słuchawek z mikrofonem

7. Dysk twardy	- Minimum 512GB SSD z interfejsem M.2 NVMe, zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego zainstalowanego na komputerze przez producenta, po awarii, do stanu fabrycznego (tryb OOBE dla systemu MS Windows) - Możliwość zamontowania w obudowie dwóch dysków 3,5 cala lub 2,5 cala.
8. Napęd optyczny	Nagrywarka DVD +/-RW
9. Karta dźwiękowa	Karta dźwiękowa zintegrowana z płytą główną, zgodna ze standardem High Definition 5.1
10. Karta graficzna	Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki. Pełna obsługa funkcji i standardów DX12, OpenGL 4.5, OpenCL 2.1. Możliwość fabrycznego zainstalowania dodatkowej, dedykowanej karty graficznej z pamięcią własną min. 4 GB. Grafika zintegrowana w procesorze musi umożliwiać jednoczesną obsługę co najmniej dwóch monitorów. Na potrzeby obsługi większej liczby monitorów oferowany komputer musi umożliwiać jednoczesną obsługę monitorów podłączonych do grafiki zintegrowanej w procesorze oraz zainstalowanej osobnej karty graficznej (jeśli jest ona wymagana).
11. Karta sieciowa	Karta sieciowa 10/100/1000 Ethernet RJ-45, zintegrowana z płytą główną wspierająca obsługę technologii WoL oraz PXE. Zintegrowana karta sieciowa musi być wyposażona w diodę statusu informującą a aktywności połączenia oraz diodę informującą o prędkości połączenia.
12. BIOS	BIOS UEFI w wersji 2.6 lub wyższej. Możliwość odczytania z BIOS informacji o: - modelu komputera, - numerze seryjnym, - AssetTag/IDTag - MAC Adres karty sieciowej, - wersja Biosu wraz z datą jego produkcji, - zainstalowanym procesorze, jego taktowaniu - ilości pamięci RAM wraz z taktowaniem i obłożeniem slotów Możliwość z poziomu BIOS: - wyłączenia selektywnego portów USB, minimum wyłączanie portów z przodu oraz wyłączanie portów z tyłu jako grup

	- wyłączenia selektywnego (pojedynczego) portów SATA, - zmiany pracy wentylatorów między trybem optymalizacji głośności lub temperatury, - ustawienia hasła: administratora, Power-On, HDD, - możliwość zbierania i przeglądania logów zdarzeń z informacją odnośnie godziny, daty i kodu błędu zdarzenia - ustawienie automatycznej aktualizacji BIOS z serwera producenta komputera
13. Klawiatura	Klawiatura USB w układzie polskim programisty (105 klawisze) z kablem o długości min. 1,8 m.
14. Mysz	Mysz optyczna USB z klawiszami oraz rolką (scroll) z kablem o długości min. 1,8 m.
15. Obudowa	– Typu Microtower przystosowana do pracy w pionie, z obsługą kart PCI Express; – Wbudowany głośnik do odtwarzania plików multimedialnych. – Suma wymiarów obudowy, nie może przekroczyć: 860 mm, najkrótszy z wymiarów nie większy niż: 180 mm – Obudowa jednostki centralnej beznarzędziowa, pozwalająca na demontaż komponentów i kart rozszerzeń (PCIe) oraz napędu optycznego i dysków twardych (co najmniej 3,5 cala) bez użycia narzędzi, z obiegiem powietrza tylko przód-tył - brak perforacji na bokach obudowy . –
16. Zasilanie	Zasilacz o mocy nie mniejszej niż 280 W i nie większej niż 300 W, o sprawności 94% przy obciążeniu 50%. Roczny pobór mocy jednostki centralnej, nie większy, niż w specyfikacji energetycznej dla Energy Star w wersji 8.0. Zasilacz spełniający kryteria 80Plus PLATINUM według informacji podanej na stronie: https://www.clearesult.com/80plus/
17. Bezpieczeństwo i funkcje zarządzania	1. Możliwość zastosowania mechanicznego zabezpieczenia przed kradzieżą komputera. 2. Zamek zatrzaskowy z kluczem, nie wystający poza obrys obudowy zabezpieczający przed niepowołanym dostępem do wnętrza obudowy. 3. Funkcjonalność TPM 2.0.

	4. Certyfikowane oprogramowanie umożliwiające – bez względu na stan czy obecność systemu operacyjnego w bezpieczny (bezpowrotny) sposób usunięcie danych z dysku twardego - w ofercie należy podać nazwę i producenta oprogramowania. 5. System diagnostyczny działający bez udziału systemu operacyjnego, czy też jakichkolwiek dołączonych urządzeń na zewnątrz czy też wewnątrz komputera, umożliwiający otrzymanie informacji o: - modelu, oznaczeniu i numerze seryjnym komputera, pojemności zainstalowanej pamięci RAM Oprogramowanie diagnostyczne musi umożliwiać: - wykonanie testu pamięci RAM, - wykonanie podstawowego testu prawidłowej pracy CPU - wykonanie testu dysku twardego. System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera (Zaimplementowany w sprzętowym mikro kodzie płyty głównej)
18. Sterowniki i oprogramowanie	Zapewnienie na dedykowanej stronie internetowej producenta dostępu do najnowszych sterowników i uaktualnień, realizowane poprzez podanie numeru seryjnego/modelu urządzenia, podać link strony www. Oprogramowanie producenta komputera posiadające funkcje zarządzania sterownikami (wykrywanie i instalowanie aktualizacji). Oprogramowanie umożliwiające – bez względu na stan czy obecność systemu operacyjnego oraz bez podłączania żadnych urządzeń czy nośników zewnętrznych - w bezpieczny (bezpowrotny) sposób usunięcie danych z dysku twardego. Usuwanie danych z dysku twardego musi odbywać się przy wykorzystaniu certyfikowanych algorytmów a wynikiem pracy oprogramowania musi być protokół zawierający dane kasowanego dysku oraz informacje o zastosowanym algorytmie kasowania. W ofercie należy podać nazwę i producenta oprogramowania.
19. Certyfikaty i oświadczenia (Załączyć do oferty)	1. **Oferowane komputery stacjonarne muszą posiadać europejską deklarację zgodności CE.**

	2. Certyfikat poprawnej współpracy z zaoferowanym systemem operacyjnym - do oferty dołączyć wydruk ze strony producenta oprogramowania systemowego. **3. Oferowane komputery stacjonarne muszą posiadać certyfikat TCO 9.0 – obecność modelu na stronie https://tcocertified.com/product-finder/** **4. Oferowane komputery stacjonarne muszą posiadać certyfikat EPEAT dla standardu IEEE 1680.1 - 2018 – obecność modelu na stronie https://www.epeat.net/?category=pcsdisplays**
20. Zainstalowane oprogramowanie systemowe	Zainstalowany system operacyjny co najmniej Windows 10 Pro 64-bitowy w polskiej wersji językowej lub system równoważny wraz z nośnikiem instalacyjnym. Klucz licencyjny systemu musi być zapisany trwale w BIOS i umożliwiać jego instalację bez potrzeby ręcznego wpisywania klucza licencyjnego. *Zamawiający nie dopuszcza zaoferowania systemu operacyjnego pochodzącego z rynku wtórnego, reaktywowanego systemu.* System równoważny 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. Interfejsy użytkownika dostępne w wielu językach do wyboru – w tym polskim i angielskim. 3. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe. 4. Wbudowany system pomocy w języku polskim. 5. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim. 6. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego. 7. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika.

	8. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne. 9. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 10. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 11. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 12. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 13. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi). 14. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer. 15. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji. 16. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji. 17. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe. 18. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 19. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu.

	20. 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. 21. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. 22. Obsługa standardu NFC (near field communication). 23. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 24. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 25. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. 26. Mechanizmy logowania do domeny w oparciu o: a. Login i hasło, b. Karty z certyfikatami (smartcard), c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM). 27. Mechanizmy wieloelementowego uwierzytelniania. 28. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5. 29. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu. 30. Wsparcie dla algorytmów Suite B (RFC 4869). 31. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec. 32. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk. 33. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 34. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń.

	35. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem, 36. 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. 37. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację. 38. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 39. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe. 40. Udostępnianie modemu. 41. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 42. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 43. 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.). 44. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu). 45. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych. 46. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika.

	47. Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB. 48. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych. 49. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych. 50. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.
21. Gwarancja	Gwarancji jakości producenta: Na okres co najmniej 24 miesięcy - świadczonej w siedzibie Zamawiającego, chyba że niezbędne będzie naprawa sprzętu w siedzibie producenta ,lub autoryzowanym przez niego punkcie serwisowym - wówczas koszt transportu do i z naprawy pokrywa Wykonawca, Czas reakcji na zgłoszoną reklamację gwarancyjną - do końca następnego dnia roboczego W przypadku naprawy trwającej dłużej niż 48 godzin, zamawiającemu musi zostać dostarczony komputer zastępczy Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta, Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela

3. Monitor - 10 szt.

Nazwa	Parametry minimalne
Ekran	23,8 cala o rozdzielczości natywnej minimum 1920x1080 pikseli, maksymalny rozmiar piksela 0.275 mm, matryca matowa, pokryta powłoką 3H, technologia matrycy IPS
Parametry obrazu	Odwzorowanie 16.7 miliona kolorów, kontrast typowy 1000:1, jasność min. 250 cd/m^2, czas reakcji matrycy max. 5ms, kąty widzenia pionowe/poziome minimum 178/178 stopni
Wejścia wideo i inne	1x DP, 1x DVI-D, 1x D-SUB, wejście/wyjście audio
Obudowa i regulacja monitora	Pochylenie ekranu w zakresie -5° / +22°(tzw. Tilt), zintegrowany zasilacz i głośniki stereo o mocy minimum 2W każdy, możliwość regulacji głośności z

	menu OSD monitora, złącze Kensington Lock, złącze montażu na ścianie w standardzie VESA
Funkcje zarządzana energią i parametrami wyświetlania obrazu	Technologia zapewniająca zużycie energii przez monitor w trybie power save na poziomie 0.2W pozwalająca na redukcję ogólnego zużycia energii przez monitor (bez konieczności manualnego wyłączania monitora przez użytkownika), zgodność z normą Energy Star 8.0, zużycie energii przy ustawieniach EPA max. 14W
Menu monitora	Regulacja głośności Regulacja jasności Regulacja kontrastu Regulacja koloru (sRGB, 5000K, 6500K, 7500K, Użytkownika (R,G,B) Menu w języku polskim oraz angielskim.
Kable	kabel sygnałowy cyfrowy o długości minimum 1.8m, kabel zasilający o długości minimum 1,8m, kabel audio
Gwarancja	Gwarancja 24 miesiące

4. Oprogramowanie Antywirusowe- 40 szt.

Minimalne wymagania

Ochrona antywirusowa niżej wymienionego systemu monitorowana i zarządzana z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową.

Od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, do prawidłowego działania wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli znajdującej się na serwerach producenta.

Rozwiązanie dla ochrony antywirusowej stacji roboczych wspiera następujące systemy operacyjne:

- Microsoft Windows 7 z dodatkiem SP1
- Microsoft Windows 8.1
- Microsoft Windows 10
- Microsoft Windows 11
- macOS 11 "Big Sur"
- macOS 10.15 "Catalina"
- macOS 10.14 "Mojave"

Rozwiązanie dla ochrony antywirusowej systemów serwerowych wspiera następujące systemy operacyjne:

- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Microsoft Windows Server 2022

Wspierane przeglądarki internetowe do obsługi konsoli zarządzającej:

- Microsoft Internet Explorer
- Microsoft Edge
- Mozilla Firefox

- Google Chrome
- Safari

Zarówno konsola jak i oprogramowanie antywirusowe do ochrony stacji roboczych oraz serwerów posiada Polski interfejs użytkownika.
Ten sam agent zainstalowany na systemach Windows umożliwia rozbudowę funkcjonalności o system EDR i mechanizm zarządzania podatnościami – aktywacja dodatkowych funkcji uzależniona jest tylko od posiadanej licencji, automatycznie aktywowana w momencie jej dodania i nie wymaga reinstalacji agenta w środowisku oraz posiadania osobnej konsoli zarządzającej.
Funkcjonalności systemu mogą różnić się w zależności od platformy na jakiej zainstalowany jest agent ze względu na ich ograniczenia, jednak chronione platformy są zarządzane z tej samej konsoli zarządzającej

Opis technologii

1. Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanowania heurystycznego, modułu skanującego nośniki wymienne, monitora ruchu http oraz modułu wykrywającego rootkity.
2. Rozwiązanie posiada wbudowany mechanizm ochrony przed zagrożeniami typu ransonmware.
3. Rozwiązanie wspiera technologię Antimalware Scan Interface (AMSI)
4. Rozwiązanie umożliwia wybór plików do skanowania – wszystkich plików lub tylko plików o określonych rozszerzeniach.
5. W momencie wykrycia infekcji rozwiązanie automatycznie stara się wyleczyć plik a jeśli nie jest to możliwe przenosi go do bezpiecznego folderu kwarantanny.
6. Rozwiązanie posiada możliwość ręcznej reakcji na wykryte zagrożenie, w takim przypadku pozwala na: wyleczenie pliku, usunięcie, przeniesienie do kwarantanny, zmiany nazwy, zablokowania.
7. Rozwiązanie chroni plik systemowy HOSTS przed nieautoryzowanymi zmianami.
8. Rozwiązanie posiada mechanizmy skanujące dyski sieciowe.
9. Skanowanie dysków sieciowych jest możliwe dla dowolnych operacji na takich zasobach lub tylko przy wykonywaniu znajdujących się tam plików.
10. Rozwiązanie posiada możliwość tworzenia wykluczeń dla mechanizmów ochrony w czasie rzeczywistym, w tym co najmniej dla: plików, folderów, procesów.
11. Rozwiązanie posiada mechanizm ochrony ruchu http chroniący użytkownika przed malware oraz phishingiem.
12. Istnieje możliwość stworzenia wykluczenia dla wskazanej aplikacji, tak aby nie skanowała ona ruchu http.
13. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie przez wywołanie funkcji w interfejsie lokalnym oprogramowania.
14. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
15. Rozwiązanie posiada możliwość dystrybuowania aktualizacji baz definicji wirusów oraz aktualizacji oprogramowania zainstalowanego na stacji końcowej, za pomocą serwera pośredniczącego.
16. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej do nowej wersji, następuje w sposób automatyczny, niewidoczny dla użytkownika końcowego.
17. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej nie wymaga dodatkowych czynności konfiguracyjnych ze strony administratora systemu i następuje automatycznie w momencie udostępnienia takiej aktualizacji przez producenta.

18. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli zarządzania.
19. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej w określone dni i godziny tygodnia i miesiąca.
20. Rozwiązanie posiada możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli lub lokalnie przez określonego klienta.
21. Rozwiązanie posiada możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.
22. Rozwiązanie posiada możliwość wywołania procesu skanowania z niskim priorytetem, co pozwala na skanowanie z użyciem mniejszej ilości zasobów systemowych.
23. Rozwiązanie posiada możliwość wywołania skanowania uwzględnionych rozszerzeń a także ich wykluczanie.
24. Rozwiązanie posiada możliwość skanowania urządzeń przenośnych takich jak pendrive, dyski zewnętrzne itp.
25. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie.
26. Rozwiązanie posiada funkcję skanowania na żądanie pojedynczych plików, katalogów, napędów przy pomocy skrótu w menu kontekstowym
27. Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).
28. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
29. Rozwiązanie posiada heurystyczną technologię do wykrywania nowych, nieznanych wirusów.
30. Umożliwia wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan", „rootkit".
31. Posiada mechanizm wykrywania nowych i nieznanych zagrożeń (0-day), bazujący na technologii chmurowej, analizującej podejrzane pliki wykonywalne (przez pliki wykonywalne rozumie się co najmniej: aplikacje, interpretowalną zawartość Flash, Sliverlight, skrypty oraz makra dokumentów pakietu Office).
32. Rozwiązanie posiada technologię wykrywania nowych i nieznanych zagrożeń typu 0-day, technologia ta powinna w głównej mierze bazować na metadanych na temat analizowanego pliku. Pliki sklasyfikowane jako bezpieczne, nie są wysyłane do analizy w infrastrukturze producenta.
33. Rozwiązanie posiada technologię wykrywania nowych i nieznanych zagrożeń, która w przypadku podejrzanych plików umożliwia automatyczne ładowanie ich do systemu sandbox, utrzymywanego w infrastrukturze dostawcy oprogramowania antywirusowego w celu przeprowadzenia dodatkowej strukturalnej i behawioralnej analizy podejrzanego pliku.
34. Rozwiązanie posiada możliwość wyłączenia mechanizmu automatycznego przesyłania podejrzanych plików do dodatkowej analizy przez producenta.
35. Rozwiązanie posiada możliwość umieszczenia oprogramowania typu „spyware", „adware", „keylogger", „dialer", „trojan" w kwarantannie.
36. Rozwiązanie posiada możliwość obsługi plików skompresowanych obejmującego najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX.
37. Rozwiązanie posiada możliwość logowania historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów jest możliwy z poziomu GUI aplikacji jak i konsoli centralnego zarządzania.
38. Rozwiązanie automatycznie powiadamia użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona.

39. Rozwiązanie posiada możliwość wyłączenia powiadomień dla użytkowników stacji końcowej o wykrytych zagrożeniach.
40. Rozwiązanie posiada możliwość wyłączenia interfejsu użytkownika oprogramowania zainstalowanego na stacji końcowej.
41. Rozwiązanie umożliwia blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.
42. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez system reputacyjny producenta.
43. Rozwiązanie posiada możliwość instalacji dodatku do przeglądarki internetowej (Google Chrome, Mozilla Firefox, MS Edge) pozwalającego na wyświetleniu graficznej informacji o reputacji witryny, która pojawia się w wynikach wyszukiwania w wyszukiwarkach internetowych.
44. Rozwiązanie jest wyposażone w mechanizm ochrony przeglądarki internetowej, w tym analizujący uruchamiane skrypty ActiveX i pobierane pliki.
45. Rozwiązanie posiada możliwość ochrony podczas przeglądania sieci Internet na podstawie badania reputacji witryn.
46. Rozwiązanie umożliwia blokowanie dostępu do kategorii witryn WWW skatalogowanych przez systemy producenta.
47. Oprogramowanie zapewnia co najmniej 30 kategorii klasyfikacji witryn WWW.
48. Użytkownik podczas próby przejścia na witrynę znajdująca się w zablokowanej przez Administratora kategorii, jest powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej.
49. Rozwiązanie umożliwia blokowanie witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS.
50. Rozwiązanie posiada wbudowany mechanizm zabezpieczenia połączenia do witryn skategoryzowanych przez producenta jako „bankowość elektroniczna” poprzez uniemożliwienie nawiązania nowych sesji do niezaufanych hostów na czas połączenia z bankiem.
51. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie blokuje możliwość uruchamiania od strony chronionego hosta poleceń cmd oraz skryptów.
52. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie automatycznie blokuje zdalny dostęp do hosta za pomocą takich narzędzi jak pulpit zdalny, TeamViewer, LogMein, VNC itp.
53. Kontrola połączenia umożliwia zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora – administrator ma możliwość tworzenia własnej listy takich witryn.
54. Rozwiązanie posiada wbudowaną funkcję, która po zakończeniu sesji z witrynami sklasyfikowanymi jako „bankowość elektroniczna” czyści zawartość schowka systemowego.
55. Rozwiązanie posiada funkcję zarządzania zaporą ogniową (tzw. personal firewall) wbudowaną w system Windows, z opcją definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup.
56. Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.
57. Rozwiązanie pozwala na tworzenie własnych reguł w oparciu co najmniej o: kierunek komunikacji sieciowej, protokół sieciowy, oraz możliwość wyboru akcji zezwolenia lub zablokowania wskazanej komunikacji.
58. Rozwiązanie posiada możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej).
59. Rozwiązanie umożliwia stworzenie zestawów reguł do natychmiastowego zastosowania, które zablokują komunikację sieciową w celu izolacji hosta na żądanie administratora.

60. Rozwiązanie jest wyposażone w mechanizm aktualizacji aplikacji (patch managment), umożliwiający instalację dostępnych poprawek dla systemu operacyjnego oraz aplikacji na nim zainstalowanych.
61. Mechanizm aktualizacji aplikacji (patch managment) nie wymaga instalowania dodatkowych agentów oprócz agenta AV.
62. Moduł aktualizacji aplikacji, okresowo skanuje aplikacje zainstalowane na stacji roboczej i umożliwia ich aktualizację do najnowszych wersji.
63. Moduł aktualizacji aplikacji pełni role mechanizmu łatającego podatności i instalującego aktualizacje oprogramowania, a nie jedynie pasywnego skanera luk w bezpieczeństwie aplikacji.
64. Administrator posiada możliwość określenia, kiedy i jakie aktualizacje mają zostać zainstalowane automatycznie.
65. Administrator posiada możliwość uruchomienia aktualizacji dla systemu operacyjnego jak i aplikacji znajdujących się na nim na żądanie dla wybranych lub wszystkich hostów.
66. Mechanizm aktualizacji aplikacji umożliwia automatyczne wyświetlenie komunikatu użytkownikowi od strony hosta o konieczności zamknięcia danej aplikacji, tak aby proces aktualizacji mógł się zakończyć.
67. W przypadku gdy instalacja aktualizacji dla systemu operacyjnego lub innej aplikacji wymaga restartu hosta w celu jej zastosowania, administrator posiada możliwość wymuszenia automatycznego restartu, wymuszenia restartu po określonej liczbie godzin, lub wyświetlenia komunikatu użytkownikowi o konieczności restartu.
68. Administrator konsoli zarządzającej ma możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji.
69. Mechanizm aktualizacji aplikacji (patch managment) nie wymaga uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces.
70. Administrator ma możliwość zdefiniowania aplikacji, które nie podlegają aktualizacji, poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej.
71. Rozwiązanie umożliwia wyświetlenie w GUI od strony chronionego hosta informacji o brakujących poprawkach dla systemu lub aplikacji i umożliwienie, ich instalacji przez użytkownika końcowego.
72. System centralnego zarządzania prezentuje niezaktualizowane aplikacje występujące na wszystkich chronionych hostach lub listę nieaktualizowanego oprogramowania dla pojedynczej stacji końcowej.
73. Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.
74. Mechanizm kontroli urządzeń zewnętrznych wspiera m.in. urządzenia takie jak: pamięci masowe, napędy CD/DVD, modemy, porty COM i LTP, drukarki, czytniki kart pamięci, kamery, urządzenia bluetooth.
75. Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączania do stacji końcowej.
76. Lista urządzeń zaufanych jest tworzona co najmniej w oparciu o nazwę urządzenia i identyfikator sprzętowy.
77. Rozwiązanie posiada możliwość blokady zapisywania plików na zewnętrznych dyskach USB urządzenia takie są wówczas dostępne w trybie tylko do odczytu.
78. Mechanizm kontroli urządzeń umożliwia blokadę uruchamiania plików wykonywalnych z nośników pamięci. Blokada ta pozwala na korzystanie z pozostałych danych zapisanych na takich nośnikach.
79. Rozwiązanie posiada możliwość zabezpieczenia zmian w konfiguracji przez użytkownika końcowego przy wykorzystaniu hasła.
80. Zmiany w konfiguracji mogą być dokonywane przez użytkownika końcowego tylko dla poszczególnych funkcji aplikacji wskazanych przez administratora w profilu.
81. Rozwiązanie jest wyposażone w dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware niezależnie od pozostałych modułów ochrony. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.

82. Moduł posiada możliwość pracy w trybie monitorowania (bez blokowania) przekazując administratorowi informacje dotyczące prób modyfikacji plików w chronionych folderach.
83. Administrator posiada możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.
84. Istnieje możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną antyransomware.
85. Rozwiązanie potrafi automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz daje możliwość wskazania zaufanych aplikacji przez administratora.
86. Rozwiązanie posiada funkcjonalność kontroli uruchamianych aplikacji.
87. Tryb kontroli aplikacji umożliwia uruchomienie wszystkich aplikacji, uruchomienie i monitorowanie wszystkich aplikacji, blokowanie niezaufanych aplikacji.
88. Istnieje możliwości blokowania, zezwolenia lub monitorowania aplikacji w oparciu, co najmniej o docelowy identyfikator SHA1,SHA256, lokalizację pliku, wersję pliku, nazwę aplikacji, wielkość pliku, wydawcę, ważność podpisu cyfrowego aplikacji.
89. Tworzone reguły dotyczyć mogą czynności: uruchomienia aplikacji, ładowania modułu, uruchomienia instalatora, dostępu do pliku.

Centralna administracja

1. Portal zarządzający jest dostępny w języku polskim.
2. Komunikacja pomiędzy portalem centralnego zarządzania a stacjami roboczymi odbywa się w formie zaszyfrowanej.
3. W celu korzystania z centralnej administracji, od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli zarządzającej znajdującej się na serwerach producenta.
4. Interfejs zarządzania posiada funkcję wyświetlania monitów o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.
5. Interfejs jest wyposażony w panel kontrolny zawierający podsumowanie stanu bezpieczeństwa organizacji w postaci graficznych wykresów.
6. Wykresy są interaktywne, tzn. że po wybraniu interesującego elementu, następuje przekierowanie do zawierającego bardziej szczegółowe dane menu.
7. Rozwiązanie posiada dedykowaną zakładkę zawierającą informację o wszystkich hostach posiadających zainstalowane oprogramowanie do ochrony, w tym: ich nazwy, status ochrony, przypisany profil bezpieczeństwa.
8. Istnieje możliwość eksportu listy wszystkich hostów do pliku CSV.
9. Administrator ma możliwość wglądu w szczegóły zgłaszającego się hosta, w których zawarte są informacje dotyczące: ostatniego podłączenia do konsoli zarządzającej, wersji zainstalowanego produktu, systemu operacyjnego, stanu ochrony, akcji związanych z wykrytymi zagrożeniami i skanowaniami.
10. Administrator ma możliwość z poziomu szczegółów klienta, uruchomienia skanowania antywirusowego, instalacji aktualizacji dla aplikacji i systemu operacyjnego, przypisania profilu, usunięcia urządzenia, zmiany klucza subskrypcji, odizolowania hosta od sieci i pobrania pliku diagnostycznego.
11. Komputery nie nawiązujące komunikacji z konsolą zarządzającą mogą być automatycznie usuwane z listy po określonym przez administratora czasie - co najmniej 60 dni.
12. Rozwiązanie posiada dodatkową zakładkę zawierającą informacje dotyczącą brakujących aktualizacji dla zainstalowanych aplikacji i systemu operacyjnego.
13. Istnieje możliwość posortowania i filtrowania brakujących poprawek pod względem ich poziomu krytyczności.

14. Informacje dotyczące brakujących poprawek dla aplikacji i systemu operacyjnego zawierają liczbę i typ hostów na których został wykryty brak danej poprawki.
15. Po wskazaniu danej poprawki administrator posiada możliwość jej instalacji na wskazanych komputerach lub na wszystkich komputerach i serwerach, dla których dana poprawka została wydana.
16. Administrator ma możliwość wglądu w historię instalowanych poprawek na chronionych hostach.
17. Rozwiązanie posiada moduł raportujący w którym wyświetlane są informacje dotyczące stanu ochrony, infekcji malware, instalowanych aplikacji.
18. Raporty mogą być tworzone zgodnie z harmonogramem i wysyłane na wskazane adresy email.
19. Rozwiązanie posiada wbudowany mechanizm zarządzania subskrypcjami, z możliwością dodawania nowych kluczy licencyjnych.
20. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.
21. Portal zarządzający umożliwia dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu EDR, mechanizmów zarządzania podatnościami, ochrony usług Microsoft 365.
22. Dodanie klucza licencyjnego skutkuje pojawieniem się dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym.
23. Rozwiązanie ma możliwość definiowania różnych profili ustawień dla chronionych urządzeń z poziomu portalu zarządzającego.
24. Profile mogą być przypisane do pojedynczych hostów lub do grup.
25. Rozwiązanie pozwala administratorowi podczas tworzenia profili wskazanie funkcjonalności, które mogą być zmieniane przez użytkownika od strony chronionego hosta – możliwość wprowadzanych zmian jest do określenia dla poszczególnych funkcji programu oraz całości konfiguracji.
26. Z poziomu portalu zarządzającego isnieje możliwość pobrania plików instalacyjnych, wykorzystywanych do instalacji agenta na objętych licencją hostach.
27. Pliki instalacyjne mają posiadać plików .EXE, .MSI, .MPKG, .DEB, .RPM w zależności od platformy i typu systemu na jakich ma zostać zainstalowany agent.
28. Tworzone profile muszą dają administratorowi możliwość blokowania ustawień konfiguracyjnych aplikacji zainstalowanych od strony stacji roboczych w celu uniemożliwienia ich modyfikacji przez lokalnego użytkownika.
29. Portal zarządzający pozwala na zarządzanie oprogramowaniem instalowanym na urządzeniach mobilnych (smartphony) w przypadku posiadania odpowiedniej licencji.
30. Konsola posiada możliwość definiowania wielu kont administratorów o różnych poziomach dostępu.
31. W ramach posiadanych licencji istnieje możliwość przenoszenia oprogramowania w ramach danego klucza subskrypcji z jednej stacji roboczej na inną.
32. możliwość blokowania każdej aplikacji
33. możliwość zablokowania aplikacji w oparciu o kategorie
34. możliwość dodania własnych aplikacji do listy zablokowanych
35. zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach klientach poprzez konsole administracyjna na serwerze
36. dodawanie innych aplikacji
37. dodawanie aplikacji w formie portable
38. możliwość wyboru pojedynczej aplikacji w konkretnej wersji
39. dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB
40. kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool
41. możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki.
42. możliwość zablokowania funkcji Printscreen

43. funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows jak i OSx
44. funkcje monitorowania i kontroli przepływu poufnych informacji
45. możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików
46. możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj
47. możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe
48. ochronę przed wyciekiem informacji na drukarki lokalne i sieciowe
49. ochrona zawartości schowka systemu
50. ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL
51. możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych
52. ochrona plików zamkniętych w archiwach
53. Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem
54. możliwość tworzenia profilu DLP dla każdej polityki
55. wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania
56. ochrona przez wyciekiem plików poprzez programy typu p2p
57. Monitorowanie zmian w plikach:
58. Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych.
59. Funkcje monitorowania określonych rodzajów plików.
60. Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania.
61. Generator raportów do funkcjonalności monitora zmian w plikach.
62. możliwość śledzenia zmian we wszystkich plikach
63. możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach
64. możliwość definiowana własnych typów plików
65. Optymalizacja systemu operacyjnego stacji klienckich:
66. usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku
67. optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem
68. możliwość zaplanowania optymalizacje na wskazanych stacjach klienckich
69. instruktaż stanowiskowy pracowników Zamawiającego
70. dokumentacja techniczna w języku polskim

Platforma do zarządzania dla Android i iOS:

- Musi zapewnić kompleksowy system ochrony i zarządzania urządzeniami mobilnymi z systemami Android oraz iOS a także ich ochronę
- Funkcjonalność musi być realizowana za pomocą platformy w chmurze bez infrastruktury wewnątrz sieci firmowej.
- Zarządzanie użytkownikiem
- Musi umożliwiać zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email
- Musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, Nazwisko, adres email, Departament, numer telefonu stacjonarnego, numer telefonu komórkowego, typ użytkownika
- Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi
- Musi posiadać możliwość eksportu danych użytkownika

Zarządzanie urządzeniem:

- Musi umożliwiać wdrożenie przez Email, SMS, kod QR oraz ADO
- Musi umożliwiać import listy urządzeń z pliku CSV
- Musi umożliwiać dodanie urządzeń prywatnych oraz firmowych

- Musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: Data wdrożenia, typ wdrożenia, status wdrożenia, status urządzenia, numer telefonu, właściciel, typ właściciela, grupa, reguły, konfiguracja geolokacji, wersja agenta
- Musi umożliwiać podgląd co najmniej następujących informacji sprzętowych: model, producent, system, IMEI, ID SIM, dostawca SIM, adres MAC, bluetooth, Sieć, wolna przestrzeń na dysku, całkowita przeszłość na dysku, bateria, zużycie procesora, sygnał
- Musi umożliwiać podgląd lokacji w zakresach czasu: dzisiaj, wczoraj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres
- Musi zawierać podgląd aktualnie zainstalowanych aplikacji
- Musi zawierać informacje o zużyciu łącza danych, a w tym: Ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych,
- Musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł
- Moduł raportowania musi umożliwiać podgląd w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres.

Oprogramowanie pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa:
Wymagania dotyczące technologii:

1. Dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową
2. Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta.
3. Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych:

- Microsoft Internet Explorer
- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari

4. Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących
5. Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie
6. Portal zarządzający musi umożliwiać:

a) przegląd wybranych danych na podstawie konfigurowalnych widgetów
b) zablokowania możliwości zmiany konfiguracji widgetów
c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów.
d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności
e) eksport wszystkich skanów podatności do pliku CSV

Licencja udzielona na okres min 24 mc

5. Serwer - 1 szt.

Nazwa	Parametry minimalne
Obudowa	• Typu RACK, wysokość nie więcej niż 2U; • Szyny umożliwiające wysunięcie serwera z szafy stelażowej; • Ramię porządkujące ułożenie przewodów z tyłu serwera; • Obudowa gotowa do zainstalowania 16 dysków twardych hot plug 2,5”;

	• Możliwość zainstalowania fizycznego zabezpieczenia (np. na klucz lub elektrozamek) uniemożliwiającego fizyczny dostęp do dysków twardych; • Zainstalowane 2 szt. dyski SSD SATA 1,92 TB Read-Intensive; • Zainstalowane 4 szt. dysków SAS 10k 2,4TB ; • Możliwość zainstalowania dedykowanego wewnętrznego napędu blu-ray

Płyta główna	• Dwuprocesorowa;
	• Wyprodukowana i zaprojektowana przez producenta serwera
	• Możliwość instalacji procesorów 38-rdzeniowych;
	• Zainstalowany modułu TPM 2.0 współpracujący z Windows Serwer 2022;
	• 6 złącz PCI Express generacji 4 w tym
	  ○ 3 fizyczne złącza o prędkości x16;
	  ○ 3 fizyczne złącza o prędkości x8;
	• 32 gniazda pamięci RAM;
	• Obsługa minimum 4TB pamięci RAM DDR4;
	• Obsługa minimum 12TB pamięci RAM DDR4 + pamięć nieulotna
	• Wsparcie dla technologii:
	  ○ Memory Scrubbing
	  ○ SDDC
	  ○ ECC
	  ○ Memory Mirroring
	  ○ ADDDC;
	• Obsługa pamięci nieulotnej instalowanej w gniazdach pamięci RAM (przez pamięć nieulotną rozumie się moduły pamięci zachowujące swój stan np. w przypadku nagłej awarii zasilania, nie dopuszcza się podtrzymania bateryjnego stanu pamięci)
	• Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) nie zajmujące klatek dla dysków hot-plug;

Procesory	• 1 procesor 8-rdzeniowy • Taktowanie 3,2GHz • architektura x86_64 osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017_fp_base minimum 154 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów w oferowanym serwerze). Wynik musi być opublikowany na stronie https://www.spec.org/cpu2017/results/cpu2017.html
Pamięć RAM	• 128 GB pamięci RAM • DDR4 Registered • 3200Mhz
Kontrolery LAN	• Karta LAN, nie zajmująca żadnego z dostępnych slotów PCI Express, wyposażona minimum w interfejsy: 2x 10Gbit SFP+, dostarczona wraz z wkładkami 10GB SFP+ MM, możliwość wymiany zainstalowanych interfejsów na 2x 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe;

	• Zainstalowana karta 4x1GB RJ-45, umieszczona w slocie PCI-E;
Kontrolery I/O	• Możliwość zainstalowania dwóch nośników flash o pojemności 64GB w konfiguracji RAID-1, rozwiązanie dedykowane dla hypervisora oraz niezajmujące zatok dla dysków hot-plug; • Zainstalowany kontroler SAS 3.0 RAID 0,1,5,6,50,60, 2GB pamięci podręcznej cache oraz podtrzymaniem pamięci;
Porty	• Zintegrowana karta graficzna ze złączem VGA z tyłu; • 2 port USB 3.0 wewnętrzne; • 2 porty USB 3.0 na panelu przednim • 2 porty USB 3.0 dostępne z tyłu serwera; • Możliwość wyposażenia w port serial, 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 94% (tzw. klasa Platinum) o mocy minimalnej 900W; • Należy dostarczyć kable zasilające C13-C14 o długości min 2,5 metra. • Redundantne wentylatory hotplug;

Zarządzanie	• Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii
	  ○ informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:
	  ▪ karty rozszerzeń zainstalowane w dowolnym slocie PCI Express
	  ▪ procesory CPU
	  ▪ pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM
	  ▪ wbudowany na płycie głównej nośnik pamięci M.2 SSD
	  ▪ status karty zrządzającej serwera
	  ▪ wentylatory
	  ▪ bateria podtrzymująca ustawienia BIOS płyty główne
	  ▪ zasilacze
	• system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym)–
	Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:
	• Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;
	  ○ Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z

	możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; ○ Dostęp poprzez przeglądarkę Web, SSH; ○ Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii; ○ Zarządzanie alarmami (zdarzenia poprzez SNMP) ○ Możliwość przejęcia konsoli tekstowej ○ Możliwość zarządzania przez 6 administratorów jednocześnie ○ Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM) ○ Obsługa serwerów proxy (autentykacja) ○ Obsługa VLAN ○ Synchronizacja czasu poprzez protokół NTP ○ Możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej • Możliwość pobrania oprogramowanie zarządzającego i diagnostyczne wyprodukowanego przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna); • Dedykowana, do wbudowania w kartę zarządzającą (lub zainstalowana) pamięć flash o pojemności minimum 16 GB; • Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN; • Serwer posiada 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. • BIOS UEFI w specyfikacji 2.7;
System Operacyjny	• Serwer ma być dostarczony wraz z systemem operacyjnym opisanym w pkt „Serwerowy system operacyjny + Cale dostępowe”
Gwarancja	• Min 2 lat gwarancji producenta serwera w trybie on-site z czasem reakcji najpóźniej w ciągu następnego dnia roboczego od zgłoszenia awarii. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. • 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	• **Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta; -załączyć do oferty** • Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; • **Zgodność z normami: CB, RoHS, WEEE, GS oraz CE; załączyć do oferty**

Serwerowy system operacyjny+ cale dostępowe użytkownika.

Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze.
Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

1) Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
2) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
3) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
4) 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.
5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
9) Wbudowane wsparcie instalacji i pracy na wolumenach, które:

a) pozwalają na zmianę rozmiaru w czasie pracy systemu,
b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
d) umożliwiają zdefiniowanie list kontroli dostępu (ACL).

10) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
13) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15) Dostępne dwa rodzaje graficznego interfejsu użytkownika:
    a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
    b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
16) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
17) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
18) Mechanizmy logowania w oparciu o:
    a) Login i hasło,
    b) Karty z certyfikatami (smartcard),
    c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
19) 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..
20) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
21) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
22) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
23) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
24) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
25) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
    b) 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:
        i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,

ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.

c) Zdalna dystrybucja oprogramowania na stacje robocze.
d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
   i. Dystrybucję certyfikatów poprzez http
   ii. Konsolidację CA dla wielu lasów domeny,
   iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
   iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
f) Szyfrowanie plików i folderów.
g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
i) Serwis udostępniania stron WWW.
j) Wsparcie dla protokołu IP w wersji 6 (IPv6),
k) Wsparcie dla algorytmów Suite B (RFC 4869),
l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
m) 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:
   i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
   ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
   iii. Obsługi 4-KB sektorów dysków
   iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
   v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
   vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

26) 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.
27) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
28) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
29) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
30) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
31) Zorganizowany system szkoleń i materiały edukacyjne w języku polskim
32) Serwerowy system operacyjny w najnowszej wersji producenta oprogramowania dostępnej na rynku.
33) Dostawca wraz z systemem operacyjnym dostarczy 40 licencji User Cal w najnowszej wersji producenta oprogramowania dostępnej na rynku.

6. Oprogramowanie wirtualizacji - 1 szt.

Minimalne wymagania:

Wraz z serwerem należy dostarczyć oprogramowanie do wirtualizacji. Dostarczane oprogramowanie musi być w najnowszej wersji obecnie dostępnej na rynku. Licencja dla 1 serwerów fizycznych posiadających 2 procesory ze wsparciem technicznym 9x5 z 4h-czasem zdalnej reakcji oraz gwarancją utrzymania aktualnej wersji przez okres min. 3 lat. Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych.

- Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
- Pojedynczy klaster może się skalować do 3 fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji.
- Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafi obsłużyć

i wykorzystać procesory fizyczne wyposażone w 768 logicznych wątków oraz do 12TB pamięci fizycznej RAM.

- Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-256 procesorowych.
- Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB.
- Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych

z możliwością przydzielenia do 6 TB pamięci operacyjnej RAM.

- Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych.
- Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe.
- Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
- Rozwiązanie musi wspierać następujące systemy operacyjne: Windows XP, Windows Vista, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2012,

Windows Server 2016, Windows Server 2019, Windows 7, Windows 8, Windows 10, SLES 11, SLES 12, SLES 15, RHEL 8, RHEL 7, RHEL 6, RHEL 5, RHEL 4, Solaris 11 ,Solaris 10, Debian, CentOS, FreeBSD, Asianux, Ubuntu 20, Ubuntu 18, Ubuntu 10, SCO OpenServer, SCO Unixware, Mac OS X, Amazon Linux 2, Oracle Linux.

- Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
- Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy. .
- Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku.
- Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
- Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
- Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory.
- Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (hosta, maszyny wirtualnej) bez potrzeby wyłączania wirtualnych maszyn.
- System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów.
- Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.
- Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN).

7. NAS do backup'u danych - 1 szt.

Nazwa	Parametry minimalne
Procesor	Min 4-rdzeniowy procesor 1,7 GHz
Pamięć systemowa	8 GB pamięci SODIMM DDR3 (1 x 8 GB)
Maksymalna ilość pamięci	8 GB
Obudowa	RACK 1U
Pamięć Flash	512 MB (ochrona przed podwójnym rozruchem systemu operacyjnego)
Wnęka na dyski	4 x 3,5-calowy SATA 6 Gb/s, 3 Gb/s
Zgodność z dyskami	3,5-calowe kieszenie: 3,5-calowe dyski twarde SATA 2,5-calowe dyski twarde SATA 2,5-calowe dyski półprzewodnikowe SATA
Możliwość wymiany podczas pracy	tak

Obsługa akceleracji pamięci podręcznej SSD	tak
Port Gigabit Ethernet (RJ45)	2
Port 10 Gigabit Ethernet	1 x 10GbE SFP+
Port USB 3.2 Gen 1	4
Przyciski	Zasilanie, Reset
Ostrzeżenie systemowe	brzęczyk
Gniazdo zabezpieczające Kensington	Tak
Sumaryczna pojemność dyskowa	4 x 8000 GB (32 TB)
Parametry zainstalowanych dysków	Interfejs: Serial ATA III Pojemność HDD: 8000GB Szybkość HDD: 7200 RPM Rozmiar HDD: 3.5" Rozmiar bufora dysku pamięci: 256MB MTBF (Średni okres międzyawaryjny): 2000000 h Szybkość transmisji interfejsu HDD: 6GB/s Kompatybilność: dyski powinny znajdować się na liście kompatybilności serwera NAS z bieżącego zamówienia. Gwarancja: 24 miesiące
Gwarancja na serwera NAS	24 miesiące

8. Oprogramowanie backupowe - 1 szt.

Minimalne wymagania:

- Kompletne rozwiązanie backupowe do wszelkich zastosowań ochrony danych serwerów i stacji roboczych
- Rozwiązanie musi zapewnić wsparcie back-upowe dla systemów operacyjnych:

- Windows 7, Windows 8, Windows 10, Windows 11
- Windows Server 2008, Server 2012, Server 2016, Server 2019, Server 2022

- Licencja oprogramowania wieczysta z co najmniej rocznym wsparciem serwisowym (supportem)

Rozwiązanie musi umożliwiać:

- Tworzenie obrazów dysków-odtwarzanie awaryjne w systemach Windows Vista, 7, 8, 10, 2008, 2012, 2016)
- Klonowanie dysku twardego (na SSD)
- P2V: fizyczny na wirtualny
- Tworzenie dysku odzyskiwania (z preinstalowanymi sterownikami)

- Tworzenie kopii zapasowych w chmurze (Google Drive, Amazon S3, Azure Storage, OneDrive, Dropbox)
- Zdalne tworzenie kopii zapasowych z wykorzystaniem protokołu FTP/SFTP
- Kopie zapasowa przyrostowa (RCT), kopia zapasowa z sieci i przywracanie maszyn wirtualnych Hyper-V
- Przyrostowe kopie zapasowe, przyrostowa replikacja i przywracanie maszyn wirtualnych VMware ESXi / vCenter / ESXi Free
- Kopie zapasowe i przywracanie baz danych SQL Server/Oracle/MySQL/MariaDB/PostgreSQL
- Tworzenie kopii zapasowych i przywracanie Microsoft Exchange 2010 (SP1), 2013, 2016
- Tworzenie kopii zapasowych i przywracanie Exchange Online (Office 365)
- Szybkie kopiowanie na dyski, serwery NAS, urządzenia pamięci masowej USB, RDX, sieć itd.
- Kopie zapasowa na taśmie (DAT, LTO, USB, SAS itd.)
- Funkcja przywracanie pojedynczych plików
- Możliwość przywracania do innego sprzętu
- Możliwość połączenia z konsolą odzyskiwania oprogramowania

Wymagane funkcjonalności oprogramowania:

- Przyrostowe tworzenie kopii zapasowych i synchronizacja (z usuwaniem starych plików)
- Ochrona kopii zapasowych przed wirusami Ransomware (CryptoLocker, Locky, WannaCry, Cerber, Petya, Bad-Rabbit, Osiris, ...)
- 256-bitowe bezpieczne szyfrowanie AES
- Kompresja Zip
- Kopiowanie i kompresja zip ścieżek powyżej 255 znaków
- Planowanie automatycznego tworzenia kopii zapasowych
- Powiadomienia e-mailowe
- Nieograniczone zadania tworzenia kopii zapasowych
- Nieograniczone miejsca docelowe i elementy źródłowe
- Uruchamianie zewnętrznych skryptów
- Pliki dziennika – logi
- Obsługa wielu języków
- Zaawansowane filtry i zmienne niestandardowe
- Automatyczne uwierzytelnianie w udziałach sieciowych
- Ochrona konfiguracji
- Kopia uprawnień NTFS (ACL)
- Możliwość instalowania oprogramowania jako usługi
- Kopiowanie plików otwartych lub zablokowanych (VSS)
- Przesyłanie i pobieranie witryn internetowych
- Utrzymywanie wielu wyników tworzenia kopii zapasowych
- Rozwiązanie niewymagające angażowania dużych zasobów i przenośne
- Automatyczna aktualizacja
- Włączone wsparcie i aktualizacje

9. Zasilacz awaryjny UPS do stacji roboczych - 20 szt.

Minimalne wymagania:

- Typ: wolnostojący (tower)
- Wbudowany moduł regulacji napięcia AVR
- Moc wyjściowa pozorna: co najmniej 750 VA
- Moc wyjściowa skuteczna (czynna):co najmniej 410 W
- Napięcie wejściowe:230 V
- Kształt napięcia wyjściowego: schodkowa aproksymacja sinusoidy
- Napięcie wyjściowe akumulatora: 12 V
- Czas podtrzymania przy obciążeniu 100% : minimum 1 min
- Czas podtrzymania przy obciążeniu 50% : minimum 8,5 min
- Czas przełączania na UPS: maksymalnie 6 ms
- Czas ładowania: maksymalnie 8 godz.
- Zabezpieczenia przeciwprzepięciowe
- Interfejs USB (typ B)
- Co najmniej 3 zewnętrzne gniazdka wyjściowe francuskie CEE7
- Co najmniej 1 gniazdo RJ-45 (in/out)
- Sygnalizacja optyczno-akustyczna: np. diody LED + dźwięk

Wymagania środowiskowe:

- Środowisko pracy: 0 - 40 °C.
- Wilgotność względna podczas pracy: 0 - 95%
- Wysokość robocza: 0-3000 metrów.
- Temperatura przechowywania: 15 - 40 °C.
- Wilgotność względna przechowywania: 0-95%

10. Zapora sieciowa UTM - 1 szt.

Minimalne wymagania:

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy 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 musi wspierać 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 – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:
   - 10 portami Gigabit Ethernet RJ-45.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 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 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 1.4 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.

Funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być 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 – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
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. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone 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. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.

12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system

Polityki, Firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać 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 musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
5. Element systemu realizujący funkcję Firewall musi integrować 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
   - Google Cloud Platform (GCP).
   - OpenStack.
   - VMware NSX.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19 i 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
   - 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.
   - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   - Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać 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 musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
   - Routingu statycznego.
   - Policy Based Routingu.
   - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Funkcje SD-WAN

1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać 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) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać 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. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
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 powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.

5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres [36] miesięcy.

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres min 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
   - **Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych.**
   - **Certyfikat ISO 9001 podmiotu serwisującego.**

11.Zasilacz awaryjny UPS serwerowy - 1 szt.

Nazwa elementu, parametru lub cechy	Opis wymagań minimalnych
Moc pozorna	3000 VA
Moc rzeczywista	3000 W

Topologia (klasyfikacja IEC 62040-3)	Line-interactive z AVR
Współczynnik mocy	1
Czas przełączenia na baterię	<4 ms
Liczba, typ gniazd wyjściowych	8 x IEC C13 (2 grupy gniazd sterowalnych za pomocą oprogramowania oraz z poziomu wyświetlacza 2x2 IEC C13 10A), 1 x IEC C19 16A
Typ gniazda wejściowego	IEC C20 16A
Czas podtrzymania dla 2500W obciążenia	4 min
Czas podtrzymania przy 1200W obciążenia	13 min
Czas podtrzymania przy 3000W obciążenia z dodatkowym modułem bateryjnym	17 min
Dodatkowe baterie	Możliwość dodania do 4 dodatkowych modułow baterii w celu wydłużenia czasu podtrzymania do 84 minut dla 2500W obciążenia przy pf=1,0
Napięcie znamionowe	200/208/220/230/240/250 V
Tolerancja napięci prostownika	160 V – 294 V (regulacja programowa 150-294 V)
Częstotliwość znamionowa	50/60 Hz autodetekcja
Tolerancja częstotliwości	47– 70 Hz
Kształt napięcia	Sinusoidalny
Napięcie znamionowe wyjściowe	200/208/220/230/240 V do wyboru przez użytkownika
Zakres zmian napięcia	+6/-10% napięcia nominalnego
Częstotliwość wyjściowa	50/60 Hz
Współczynnik szczytu	3:1
Baterie wymieniane przez użytkownika "na gorąco"	Tak
Ochrona przed przeładowaniem	Tak (ograniczenie prądu ładowarki, wyłączenie ładowarki / alarm)
Ochrona przed głębokim rozładowaniem	Tak
Okresowy automatyczny test baterii	Tak
System zarządzania pracą baterii	System nieciągłego ładowania baterii. **Do oferty dołączyć należy opis algorytmu ładowania nieciągłego baterii.** W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym

	cyklu nie może być krótszy niż 14 dni. Opis powinien być materiałem firmowym producenta lub musi być przez niego potwierdzony.
Możliwość uruchomienia bez napięcia w sieci "zimny start"	Tak
Baterie wewnętrzne o pojemności nie mniejszej niż	9Ah 12V, minimum 6 szt.
Czas ładowania baterii do poziomu 90%	< 3 godz. do 90% pojemności użytkowej
Interfejs komunikacyjny	• USB
	• RS232 DB-9 żeński (HID)
	• styki przekaźnikowe
	• miniport wyłącznik ON/OFF
	• SNMP/Ethernet
Panel sterowania z wyświetlaczem LCD	• Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPSa). Dostarcza informacji o : stanie pracy urządzenia, stanie obciążenia, pomiarach i ustawieniach. Funkcje ustawień i odczytów: lokalne, wyjścia (napięcie wyjściowe , częstotliwość wyjściowa), baterii (test baterii), pomiary i dane (numer seryjny,napięcie i częstotliwość wejściowa i wyjściowa, poziom obciążenia, pozostały czas podtrzymania, wydajność, zużycie energii w kWh).
	• Poziomy rząd przycisków sterowania
	• Poziomy rząd wskaźników stanu : zasialanie z siec(zielony), trybu bateryjnego (żółty), usterki (czerwony)
	• Sygnalizator akustyczny
Sygnały akustyczne	• Awaria
	• Niski stan naładowania baterii
	• Przeciążenie
	• Serwis
Przyciski sterujące i wskaźniki diodowe LED	• Przycisk Escape (anulowanie)
	• Przyciski funkcyjne (przewijanie w górę i w dół)
	• Przycisk Enter (potwierdzający)
	• Przycisk ON/OFF załączenia i wyłączenia
	• LED trybu zasilania z siec i(kolor zielony)
	• LED trybu baterii (kolor żółty)
	• LED usterki (kolor czerwony)
Typ obudowy	Uniwersalna Tower/Rack 2U
Dane techniczne karty SNMP	Network Support: Ethernet /10Mbps - Half duplex - 10Mbps - Full duplex - 100Mbps - Half duplex - 100Mbps - Full duplex - 1.0 Gbps - Full duplex / HTTP 1.1, SNMP V1, SNMP V3/ NTP, SMTP, DHCP/
	Tymczasowe hasła: Nadawanie użytkownikowi dostępu za pomocą konta. Konto może wygasać po odpowiedniej, wprowadzonej liczbie dni (hasło przestaje być aktywne). Blokowanie konta: Po określonej liczbie nieudanych prób wpisania hasła lub określonej liczbie dni.
	Protokoły: MQTT/RNDIS/LDAP/NVD/SSH/PKI
	Kamptybilność: SNMP v1/v3 i IP v4/v6

	Interfejs: HTML5
	Adresowanie IP: DHCP/BootP/Manualne
	Szyfrowanie: pakiet szyfrów TLS 1.2 z minimum SHA256
	Dostępny port USB (microUSB - port serwisowy)
	Certyfikaty: UL 2900-1, 2900-2-2
Dołączone oprogramowanie	Tak, monitorujące i zarządzające UPS, umożliwiające automatyczne zamykanie serwerów zasilanych z systemu i pracujących pod kontrolą systemów operacyjnych: - Windows: 7 / 8 / 2008 / Vista / 2003 / XP - Microsoft SCVMM 2012 - Linux: Debian GNU Linux: Lenny, SUSE/Novell: SLES 11, OpenSUSE 11.2, Redhat Enterprise Linux: RHEL 5.3, 5.4, 5.5, Fedora core 12 Ubuntu: 10.04 - VMWare: vCenter / ESXi 5.1 - Citrix XEN 6.0
Zgodność ze standardem Energy Star	Tak
Maksymalna szerokość	438 mm
Maksymalna wysokość całkowita	172 mm (4U)
Maksymalna głębokość	603 mm
Maksymalny ciężar całkowity	71 kg
Poziom hałasu w odl. 1m	do 40 dBA dla pracy normalnej
Znaki bezpieczeństwa	CE, Energy Star, IEC/EN 62040-1-1, IEC/EN 62040-2 class B, IEC/EN 62040-3
Gwarancja producenta	24 miesiące dla elektroniki, 24 miesiące dla baterii (3 lata pełnej gwarancji po rejestracji produktu)
Możliwość montażu ręcznego bypassu serwisowego	Tak

12.Szkolenie z Cyberbezpieczeństwa - 1 szt.

W ramach zadania wykonawca przeprowadzi szkolenia w zakresie cyberbezpieczeństwa dla pracowników Urzędu Gminy Wojaszówka. Szkolenia powinny odbywać się w 2 grupach nie większych niż 15 osób i trwać nie dłużej niż 2h/grupa. Szkolenia przeprowadzone będą w siedzibie zamawiającego: Wojaszówka 115, 38-471 Wojaszówka– budynek Urzędu Gminy.

Wykonawca przekaże harmonogram szkolenia nie później niż 7 dni przed rozpoczęciem szkolenia.

Program szkolenia:

1. **System cyberbezpieczeństwa**

- Podstawowe narzędzia cyberbezpieczeństwa
- Z czego powinien składać się skuteczny system cyberbezpieczeństwa
- Jak go zbudować?

2. **Podejrzane urządzenia elektroniczne**

- Przykłady zagrożeń laptopy, pendrive, smartfony
- Jak się przed tym chronić?

3. **Ransomware**

- Ransomware jako najczęstszy rodzaj ataków na firmy i instytucje
- Jak się chronić i na co zwracać uwagę aby nie paść ofiarą cyberprzestępców

4. **Phishing jak działa i na co zwracać uwagę**

- Phishing – czym jest, jak działa?
- Przykłady zagrożeń związanych z Phishingem

5. **Typowe zagrożenia występujące w internecie**

• Prezentacja z wykorzystanie symulatora zagrożeń internetowych

Wykonawca podczas szkoleń zapewni dostęp do nowoczesnej platformy w formie strony www dostępnej w standardzie WCAG 2.1 – symulator zagrożeń internetowych. Szkolenia obędą się z wykorzystaniem dostarczonych komputerów przenośnych- laptop dostarczonych w ramach projektu. Symulator musi być narzędziem umożliwiającym użytkownikowi w bezpieczny sposób sprawdzenie oraz poznanie typowych zagrożeń czyhających na użytkowników w Internecie. Korzystanie z symulatora musi być całkowicie bezpieczne dla użytkownika końcowego (żadne z wpisywanych danych nie mogą być zapisywane i archiwizowane). W symulatorze konieczne jest zaimplementowanie min. 8 scenariuszy (zagrożeń) popularnych przestępstw internetowych, z którymi użytkownicy mogą się spotkać podczas codziennego korzystania z Internetu. Pierwsze cztery dotyczące tzw. Phishing'u w różnych odsłonach, ((Phishing Clone, Phishing Spear, Phishing Spear Chat, Phishing
Whaling) następny dotyczy oszustwa typu Pharming, dwa kolejne mają przedstawiać zasadę działania zagrożenia typu Malware, (Malware Post, Malware Email,) natomiast ostatni dotyczący certyfikatów SSL (Certificate Fraud Chat) . Wykonawca zobowiązany jest przekazać zamawiającemu dostępy do platformy na min 30 dni od daty szkolenia, wraz z instrukcją obsługi.

Wymagania szczegółowe dla platformy Symulującej zagrożenia internetowe:

a) **Moduł podstron (fałszywych witryn)** – moduł ten będzie umożliwiał tworzenie różnego rodzaju fałszywych witryn nakłaniających użytkowników do pobierania

zainfekowanych załączników, podawania danych wrażliwych i/lub dokonywania płatności internetowych.

b) **Moduł czatu –** w module tym zaimplementowany zostanie czat z botami, namawiającymi do zakupów różnych produktów powodując wyłudzenie danych osobowych, numerów kart kredytowych itp. ltd. W module tym zostaną zaimplementowane opracowane scenariusze

c) **Moduł e-mail** – w module tym użytkownik będzie miał do przeglądnięcia kilka wiadomości email przesłanych z różnych źródeł, wiadomości te będą zawierały linki bądź załączniki po kliknięciu których, zostanie uruchomiona akcja symulująca zachowanie się malware, np. blokada komputera (przeglądarki) na jakiś określony czas. Po kliknięciu załącznika „zainfekowanego" na ekranie powinna pojawić się informacja na temat, że twój komputer został zainfekowany, wykradliśmy twoje dane osobowe itd. Itp. W tym module należy również pokazać działanie tzw. szyfrującego wirusa, który po kliknięciu w załącznik szyfruje wszystkie pliki tekstowe, w tym przypadku symulator powinien pokazać przykład

d) **Moduł edukacyjny –** moduł zawierający szczegółowe informacje na temat występujących cyberprzestępstw. W szczególności powinien się skupić na phishingu, pharmingu oraz malware.

- Moduł ten powinien zawierać informacje na temat występowania oraz identyfikacji danego zagrożenia, sposobów zapobiegania, oraz informacji na temat, co użytkownik powinien w pierwszej kolejności zrobić, gdy zostanie już oszukany – czyli gdzie się zgłosić najpierw, jakie dane zabezpieczyć, zmienić hasła, czy zablokować karty płatnicze.
- Materiały edukacyjne powinny być przedstawione w formie plików PDF przedstawiających, na co zwrócić szczególną uwagę podczas korzystania z portali społecznościowych, różnego rodzaju czatów, różnego rodzaju serwisów internetowych oraz odbierania wiadomości e-mail.
- Moduł edukacyjny powinien być ściśle zintegrowany z pozostałymi modułami tj. Po przejściu każdego z opracowanych i zaimplementowanych w symulatorze scenariuszy powinna pojawić się informacja o tym jak i dlaczego użytkownik dał się oszukać i jakie to może mieć konsekwencje w późniejszym czasie.

e) **Moduł postów społecznościowych,** zawierający możliwe ataki phishingowe lub pharmingowe, w module postów społecznościowych będą znajdować się zarówno „rzeczywiste” posty nie stanowiące zagrożenia jaki i posty z potencjalnym zagrożeniem.