**Załącznik nr 9 do SWZ**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

Przedmiotem zamówienia jest zakup i dostawa sprzętu i oprogramowania. Przedmiot zamówienia został podzielony na części:

Część I:

1. Serwer – 1 sztuka
2. Zasilacz awaryjny do serwera – 1 sztuka
3. Urządzenie do wykonywania kopii zapasowych – 1 sztuka

Część II:

1. Laptop – 2 sztuki
2. Komputer all-in-one – 8 sztuk
3. Microsoft Office Home & Business 2021 lub równoważny Pakiet biurowy - 10 sztuk

Część III:

1. Zapora UTM (firewall) – 1 sztuka

**CZĘŚĆ I**

1. **SERWER - 1 szt.**

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)**  |
| **Obudowa** | Obudowa 1UObudowa serwerowa do montażu w szafie RACK 19" wraz z wysuwanymi szynami dedykowanymi do tego urządzenia przez producenta serwera. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. Obudowa powinna posiadać możliwość instalacji interfejsu NFC do połączenia z aplikacją zarządzającą serwerem na telefonie. Aplikacja zarządzająca powinna być dostępna na Android i iOS, obudowa powinna posiadać dodatkowy przedni panel zamykany na klucz, chroniący dyski twarde przed nieuprawnionym wyjęciem z serwera. |
| **Płyta główna** | Płyta główna obsługująca co najmniej jeden procesor i co najmniej 4 sloty na pamięć taktowaną przynajmniej z częstotliwością 3200MT/s przy użyciu odpowiednich procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. Zintegrowany z płytą główną moduł TPM w wersji co najmniej 2.0. Płyta główna powinna obsługiwać do 128GB pamięci RAM. |
| **Chipset** | Dedykowany przez producenta procesora  |
| **Procesor** | Procesor typu skalowalnego posiadające co najmniej 8 rdzeni działający co najmniej z częstotliwością 2.9GHz lub równoważny osiągający w teście Passmark dostępnym na stronie<https://www.cpubenchmark.net/> wynik nie mniejszy niż 18 000 pkt. |
| **RAM** | Min. 64GB DDR4 LRDIMM 3200MT/s.  |
| **Zabezpieczenia pamięci RAM** | Memory Health Check, Memory Page Retire |
| **Gniazda PCIe** | minimum dwa sloty PCIe x16 generacji 4  |
| **Interfejsy sieciowe/FC/SAS** | Możliwość rozbudowy o dwa interfejsy sieciowe 10Gb Ethernet. Na płycie głównej powinna być zainstalowana dwuportowa karta sieciowa 1GB BT. Karta nie może zajmować slotu PCIe |
| **Dyski twarde** | Zainstalowane dyski min. 2x 600GB SAS 10k. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażonego w nośniki typu flash o pojemności min. 64GB, z możliwoscią konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmiejszenia ilości wnęk na dyski twarde. Możliwość instalacji dwóch dysków hot-swap z możliwością konfiguracji RAID 1.  |
| **Kontroler RAID** | Sprzętowy kontroler dyskowy PCI-E, możliwe konfiguracje poziomów RAID: 0,1,5,10.  |
| **Wbudowane porty** | min. port USB 2.0 oraz port USB 3.0, port VGA, |
| **Video** | Zintegrowana karta graficzna |
| **Wentylatory** | Redundantne Hot-Plug  |
| **Zasilacze** | Zasilacz Hot-Plug min 500W.  |
| **Bezpieczeństwo** | Możliwość wyłączenia w BIOS funkcji przycisku zasilania. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. Moduł TPM 2.0 v3. Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem |
| **Karta Zarządzania** | Możliwość zainstalowania niezależnej karty zarządzającej od zainstalowanego na serwerze systemu operacyjnego posiadającej dedykowany port RJ-45 Gigabit Ethernet umożliwiającej: * zdalny dostęp do graficznego interfejsu Web karty zarządzającej
* szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika
* możliwość podmontowania zdalnych wirtualnych napędów
* wirtualną konsolę z dostępem do myszy, klawiatury
* wsparcie dla IPv6
* wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH
* możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz.
* możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer
* integracja z Active Directory
* możliwość obsługi przez ośmiu administratorów jednocześnie
* Wsparcie dla automatycznej rejestracji DNS
* wsparcie dla LLDP
* wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej
* możliwość podłączenia lokalnego poprzez złącze RS-232.
* możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy.
* Monitorowanie zużycia dysków SSD
* możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi,
* Automatyczne zgłaszanie alertów do centrum serwisowego producenta
* Automatyczne update firmware dla wszystkich komponentów serwera
* Możliwość przywrócenia poprzednich wersji firmware
* Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON
* Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych
* Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram.
* Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera
* Serwer musi posiadać możliwość dostępu bezpośredniego poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE lub WIFI.
 |
| **Certyfikaty** | Serwer musi być wyprodukowany zgodnie z normą ISO-9001. Serwer musi posiadać deklaracja CE. Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 lub równoważny certyfikat producenta o stosowaniu w fabrykach polityki zarządzania energią, która jest zgodna z obowiązującymi przepisami na terenie Unii Europejskiej.Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2016, Microsoft Windows 2019 x64, Microsoft Windows 2022 x64 .  |
| **Warunki gwarancji** | 36 miesięcy gwarancji producenta z czterogodzinnym czasem reakcji od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta.Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji systemu.  |
| **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim.  |

1. **Zasilacz awaryjny do serwera – 1 szt.**

|  |
| --- |
| **Dane Ogólne** |
| Typ | Online |
| Moc | 3000VA / 2700W |
| Współczynnik Mocy | 0.90 |
| **Wejście** |
| Zakres Napięcia Wejściowego | 120-276 VAC Depends on Load Level |
| Max THDi | ≤5% |
| Input PF | ≥ 0.99 at full load |
| Zakres Częstotliwości | 45Hz - 55Hz or 54Hz - 66Hz |
| Częstotliwość (Synchronized Range) | 45Hz - 55Hz or 54Hz - 66Hz |
| **Wyjście** |
| Nominalne Napięcie Wyjściowe | 208/220/230/240 VAC |
| Napięcie Sinusoidalne | Tak |
| THDv | ≤2% Full Linear Load; ≤5% Non-Linear Load |
| Regulacja Napięcia (Tryb Bat.) | ±1% |
| Frequency (Battery Mode) | ±0,2Hz |
| **Dane Techniczne** |
| Load Crest Ratio | 3:1 |
| Transfer Time [AC to Battery] | 0ms |
| Transfer Time [Inverter to Bypass] | 0ms |
| Transfer Time [Inverter to ECO] | 1ms |
| Transfer Time [ECO to Inverter] | <10ms (7-8ms typical) |
| Bypass | Before UPS Power-on: Default “No” Change to “Yes” via display panelOverload und UPS Failure: Automatically transfer to bypassBy Setting: Voltage Rang: 120-276V ± 3% |
| Generator support | Tak |
| Overload Capacity | 12s @102%-130%; 1.5s @130%-150%; 100ms @ >150% |
| External Battery Connection | Tak |
| Charger | 1.5A |
| Fan Logic | Always on, automatic speed control |
| LCD Indicators | UPS status, Load level, Battery level, Input/Output voltage, AC mode, battery mode, Bypass mode, fault conditions; LCD Display colour : Blue, red, red flashing (depends on UPS status), direction swappable (rack/tower) |
| **Wydajność** |
| LINE mode full Load | 92.5% |
| BATTERY mode full Load | 87.0% |
| Energy Star compliance | Tak |
| **Baterie i czas podtrzymania** |
| Baterie | 6x 12V/9Ah |
| DC Voltage | 6 x 12V |
| Recharge Time | 3h to 90% |
| Full Load Backup Time | 3min |
| Half Load Backup Time | 11min |
| **Komunikacja i wyjścia** |
| IEC C13 Outlet | 8 |
| IEC C19 Outlet | 1 |
| Programmable Outlets | Tak |
| Wejście | C20 |
| Oprogramowanie | WinPower |
| USB port | Tak |
| Wsparcie dla HID | Tak |
| RS-232 Port | Tak |
| Port rozszerzeń | Tak, 1 |
| Dry Contacts | Tak |
| EPO Port | Tak |
| **Środowisko** |
| Poziom hałasu | < 45dB |
| Temperatura | 0°C – 40°C |
| Wilgotność | 0% - 95% RH (non-condensing) |
| **Logistyka** |
| Klasyfikacja IEC 62040-3 | VFI-SS-311 |
| Zawartość opakowanie | UPS, Manual, USB Cable, Input Power Cable, 2x IEC Cable, RS-232 Cable, Tower holder, Rack Ears, EPO Plug, Dry Contacts Plug |
| Języki instrukcji | EN/DE/FR/RU/PL |
| EAN | 4260074974423 |
| Szerokość | 438 mm |
| Wysokość | 86.5 mm |
| Głębokść | 608 mm |
| Waga | 28.6 kg |
| Karton - Szerokość | 590 mm |
| Karton - Wysokość | 236 mm |
| Karton - Głębokść | 790 mm |
| Karton - Waga | 31.2 kg |
| Pcs. per box | 1 |
| Pcs. per layer | 2 |
| Pcs. per pal | 16 |

1. **Urządzenie do wykonywania kopii bezpieczeństwa – 1 szt.**

|  |  |
| --- | --- |
| Procesor | AMD RyzenTM V1500B quad-core 2.2 GHz |
| Wbudowana pamięć RAM | 4 GB |
| Maks. wielkość pamięci | 32 GB |
| Rodzaj pamięci | DDR4 |
| Liczba obsadzonych gniazd pamięci | 1 |
| Liczba zainstalowanych dysków tw. | 2 ( 2 x 2 TB) |
| Maks. liczba dysków | 6 |
| Obsługa hot-swap dysków | Tak |
| RAID | Tak |
| Poziomy RAID | ● 0● 1● 10 (1+0)● 5● 6 |
| Architektura sieci | GigabitEthernet |
| Interfejs sieciowy | 4 x 10/100/1000 Mbit/s |
| Gniazda we/wy | ● 2 x eSATA● 4 x RJ-45 LAN● 1 x USB 3.1● 2 x USB 3.1 |
| Liczba wentylatorów | 2 |
| Wentylator | 9.2 cm |
| Obudowa | Tower |
| Waga | 5.1 kg |
| Wymiary | 166 x 282 x 243 mm |

**CZĘŚĆ II**

1. **Laptopy - 2 szt.**

|  |  |
| --- | --- |
| Ekran | 15.6” LED IPS FHD o rozdzielczości 1920x1080, z powłoką matową, nie dopuszcza się matryc typu "glare". Klapa komputera otwierana do 180 stopni. |
| Wydajność komputera | Oferowany komputer przenośny musi osiągać w teście wydajności SYSMARK 25 – wynik min. 1200 – **test z przeprowadzonej konfiguracji załączyć do oferty**. |
| Chipset | Zaprojektowany i wykonany do pracy w komputerach przenośnych rekomendowany przez producenta procesora. |
| Obudowa | Dopuszczalne kolory – czarny/srebrny. |
| Pamięć RAM | 8GB DDR4 (pamięć RAM rozszerzalna do 32GB – nie dopuszcza się wlutowanych pamięci w płytę główną). |
| Dysk twardy | Min. 256GB SSD  |
| Dysk twardy musi zawierać partycję recovery – na partycji musi znajdować się obraz zainstalowanych i skonfigurowanych elementów tj.:- systemu operacyjnego- oprogramowania antywirusowegoPartycja musi zapewniać przywrócenie systemu operacyjnego, zainstalowanego i skonfigurowanego w/w oprogramowania. Możliwość instalacji wewnątrz obudowy drugiego dysku 2.5. |
| Karta graficzna | Grafika zintegrowana z procesorem powinna umożliwiać pracę dwumonitorową ze wsparciem DirectX 12, OpenGL 4.5, pamięć współdzielona z pamięcią RAM, dynamicznie przydzielana. |
| Karta dźwiękowa | Karta dźwiękowa zgodna z HD Audio, wbudowane dwa głośniki stereo oraz dwa cyfrowe mikrofony |
| Wbudowane połączenia i karty sieciowe | Karta sieciowa LAN 10/100/1000 LANWLAN 802.11 ax wraz z Bluetooth 5.0 |
| Porty/złącza(wbudowane) | 1x Złącze RJ-45 (podłączenie sieci lokalnej)1x Czytnik Kart pamięci SD1x Thunderbolt 4 (z możliwością ładowania Baterii laptopa)3x USB 3.21x VGA1x Gniazdo mikrofonowe/Gniazdo słuchawkowe (Combo)1x HDMI ze wsparciem HDCP1x zasilanie DC-in |
| Klawiatura | Pełnowymiarowa klawiatura podświetlana z wydzielonymi pełnowymiarowymi klawiszami numerycznymi w prawej części klawiatury, w układzie US-QWERTY, polskie znaki zgodne z układem MS Windows "polski programistyczny", klawiatura podświetlana musi być wyposażona w 2 klawisze ALT (prawy i lewy). |
| Urządzenie wskazujące | Touch Pad (płytka dotykowa) wbudowana w obudowę notebooka.  |
| Kamera | Wbudowana, o parametrach: HD 1280x720, 720p HD audio/video nagrywanie. Wbudowane dwa kierunkowe mikrofony. Mechaniczna przesłona kamery. |
| Bateria | Litowo-jonowa 48Whr – czas pracy min. 14h wyników testów BAPCO MobileMark 25 – test załączyć do oferty. |
| Zasilacz | Zewnętrzny, pracujący w sieci elektrycznej 230V 50/60Hz. |
| Obudowa waga i wymiary | Obudowa wzmocniona, szkielet wykonany ze wzmocnionego aluminium. |
| Bezpieczeństwo | - Zabezpieczenie BIOS hasłem użytkownika.- Zabezpieczenie dysku twardego hasłem użytkownika.- Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego - Trusted Platform Module 2.0. |
| System operacyjny  | Zainstalowany system operacyjny Windows 11 Professional, klucz licencyjny musi umożliwiać instalację systemu operacyjnego zdalnie bez potrzeby ręcznego wpisywania klucza licencyjnego. |
| Certyfikaty i standardy | Certyfikat ISO 9001, 14001, 50001 dla producenta sprzętu **(należy załączyć do oferty).** |
| Oprogramowanie zabezpieczające  | System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance +. Silnik musi umożliwiać co najmniej:* wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji,
* wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych,
* wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear)

Szyfrowanie danych:* Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. Pełne szyfrowanie dysków działających m.in. na komputerach z systemem Windows.
* Zapobiegające utracie danych z powodu utraty / kradzieży punktu końcowego. Oprogramowanie szyfruje całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnia je tylko autoryzowanym użytkownikom.

Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej.Istnieje możliwość blokady zapisywanie plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach.Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną anyransomware.Zaawansowane monitorowanie krytycznych danych użytkownika zapewniające zapobiegające prze niezamierzonymi manipulacjami – ataki ransomware.Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej:* Tworzenie paczek instalacyjnych oprogramowania klienckiego, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi dla Windows oraz formatach dla systemów Linux
* Centralną dystrybucję na zarządzanych klientach uaktualnień definicji ochronnych, których źródłem będzie plik lub pliki wgrane na serwer konsoli przez administratora, bez dostępu do sieci Internet.
* Raportowanie dostępne przez dedykowany panel w konsoli, z prezentacją tabelaryczną i graficzną, z możliwością automatycznego czyszczenia starych raportów, z możliwością eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i dane/raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich
* Definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji

Zarządzanie przez Chmurę:1. Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach
2. Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury
3. Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur
4. Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy
5. Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach
6. Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń
7. Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej

 Centralna konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, dystrybucji szyfrowania, polityk i centralnie zarządzanie informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych w nagłych przypadkach.Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania.1. Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer
2. Oprogramowanie klienckie, zarządzane z poziomu serwera.

System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej:* różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie
* funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD
* funkcje regulowania połączeń WiFi i Bluetooth
* funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe
* funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi
* funkcje blokowania dostępu dowolnemu urządzeniu
* możliwość tymczasowego dodania dostępu do urządzenia przez administratora
* zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu
* możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka
* możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora
* możliwość używania tylko zaufanych urządzeń sieciowych, tym urządzeń wskazanych na końcówkach klienckich
* funkcję wirtualnej klawiatury
* możliwość blokowania każdej aplikacji
* możliwość zablokowania aplikacji w oparciu o kategorie
* możliwość dodania własnych aplikacji do listy zablokowanych
* zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach klientach poprzez konsole administracyjna na serwerze
* dodawanie innych aplikacji
* dodawanie aplikacji w formie portable
* możliwość wyboru pojedynczej aplikacji w konkretnej wersji
* dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB
* kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool
* możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki.
* możliwość zablokowania funkcji Printscreen
* funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows jak i Osx
* funkcje monitorowania i kontroli przepływu poufnych informacji
* możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików
* możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj
* możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe
* ochronę przed wyciekiem informacji na drukarki lokalne i sieciowe
* ochrona zawartości schowka systemu
* ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL
* możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych
* ochrona plików zamkniętych w archiwach
* Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem
* możliwość tworzenia profilu DLP dla każdej polityki
* wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania
* ochrona przez wyciekiem plików poprzez programy typu p2p

Monitorowanie zmian w plikach:* Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych.
* Funkcje monitorowania określonych rodzajów plików.
* Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania.
* Generator raportów do funkcjonalności monitora zmian w plikach.
* możliwość śledzenia zmian we wszystkich plikach
* możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach
* możliwość definiowana własnych typów plików

Optymalizacja systemu operacyjnego stacji klienckich:* usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku
* optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem
* możliwość zaplanowania optymalizacje na wskazanych stacjach klienckich
* instruktaż stanowiskowy pracowników Zamawiającego
* dokumentacja techniczna w języku polskim

 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:
	1. Microsoft Internet Explorer
	2. Microsoft Edge
	3. Mozilla Firefox
	4. Google Chrome
	5. 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:
	1. przegląd wybranych danych na podstawie konfigurowalnych widgetów
	2. zablokowania możliwości zmiany konfiguracji widgetów
	3. zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów.
	4. tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności
	5. eksport wszystkich skanów podatności do pliku CSV
 |
| Warunki gwarancjiWsparcie techniczne | Minimum 3-letnia gwarancja producenta, Czas reakcji serwisu - do końca następnego dnia roboczego. W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego. Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. |

1. **Komputer all-in-one 8 szt.**

|  |  |
| --- | --- |
| Typ | Komputer stacjonarny. Typu All in One, komputer fabrycznie wbudowany w obudowę monitora. W ofercie wymagane jest podanie modelu producenta komputera. |
| Wydajność obliczeniowa | Komputer w oferowanej konfiguracji musi osiągać w teście wydajnościowym BAPCO wyniki nie gorsze niż: SYSmark 25 Overall Rating – co najmniej wynik 1100 punktów**Dokumentem potwierdzającym spełnianie ww. wymagań będzie dołączony do oferty**. |
| Pamięć RAM | 16GB DDR4 możliwość rozbudowy do 32GB RAM.  |
| Pamięć masowa | 256GB SSDMożliwość instalacji dodatkowego dysku twardego M.2 lub 2.5 |
| Wydajność grafiki | Grafika zintegrowana z procesorem powinna umożliwiać pracę min. dwumonitorową, współdzielona i dynamicznie przydzielana pamięć z RAM,Karta osiągająca w teście PC Mark 10 Digital Content Creation wynik min. 2500 punktów – **wynik załączyć do oferty.** |
| Matryca | Rozmiar matrycy / plamki | min.23,8” / max. 0,275mm |
| Rozdzielczość | FHD (1920x1080) |
| Jasność typowa | min. 250 cd/m² |
| Kontrast typowy | 600:1 |
| Barwa koloru (typowa) | 72% NTSC |
| Kąty Horizontal/VerticalRodzaj matrycy | 178(+/- 89) / 178 (+/-89)Matowa IPS |
| Wyposażenie multimedialne | Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki min. 2W na kanał. Wbudowana w obudowę matrycy cyfrowa kamera 1.0 MP. Mechaniczna chowana w obudowie (nie dopuszcza się kamer przekręcanych)Wbudowane w obudowę dwa mikrofony |
| Obudowa | Typu All-in-One zintegrowana z monitorem min. 23.8 cali. Każdy komputer musi być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz wpisanym na stałe w BIOS.Podstawa jednostki typu All – in – One musi umożliwiać:Regulację pochyłu pionowego w zakresie od -5 do 20 stopni. |
| Certyfikaty i standardy | Certyfikat ISO9001, 50001, 45001 dla producenta sprzętu **(załączyć do oferty)** |
| System operacyjny  | Zainstalowany system operacyjny Windows 11 Professional, klucz licencyjny musi umożliwiać instalację systemu operacyjnego zdalnie bez potrzeby ręcznego wpisywania klucza licencyjnego. |
| Wymagania dodatkowe | Wbudowane porty:1x HDMI1x USB 3.2 Typ-C3x USB 3.2 Typ-AWymagane porty USB wbudowane, nie dopuszcza się stosowania rozgałęziaczy, hubów itp. Wszystkie porty dostępne dla użytkownika w najniższej możliwej regulacji wysokości1x Universal audio jack1x RJ-45 port 10/100/1000 MbpsKarta WiFi ax+ bluetooth 5.1Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona logo producenta oferowanej jednostki, dedykowana dla danego urządzenia; wyposażona w min. 2 złącza DIMM z obsługą do 32GB DDR4 pamięci RAM, min. 1 złącza M.2 2280 dla dysku twardego oraz 1 złącze M.2 karty WiFi.Klawiatura USB w układzie polski programistyMysz optyczna USB z dwoma przyciskami oraz rolką (scroll) |
| Dodatkowe oprogramowanie  | Oprogramowanie producenta komputera z nieograniczoną czasowo licencją na użytkowanie umożliwiające:* upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS’u z certyfikatem zgodności producenta do najnowszej dostępnej wersji,
* sprawdzenie przed zainstalowaniem wszystkich sterowników, aplikacji oraz BIOS bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem w celu uzyskania informacji o: poprawkach i usprawnieniach dotyczących aktualizacji, dacie wydania ostatniej aktualizacji, priorytecie aktualizacji, zgodności z systemami operacyjnymi
* dostęp do wykazu najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne
* włączenie/wyłączenie funkcji automatycznego restartu w przypadku, kiedy jest wymagany przy instalacji sterownika, aplikacji
* sprawdzenie historii aktualizacji z informacją, jakie sterowniki były instalowane z dokładną datą i wersją (rewizja wydania)
* dostęp do wykaz wymaganych sterowników, aplikacji, BIOS’u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu \*.xml
* dostęp do raportu uwzględniającego informacje o znalezionych, pobranych i zainstalowanych aktualizacjach z informacją, jakich komponentów dotyczyły, możliwość exportu takiego raportu do pliku \*.xml

Raport musi zawierać datę i godzinę podjętych i wykonanych akcji/zadań w przedziale czasowym min. 1 roku.System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance +. Silnik musi umożliwiać co najmniej:* wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji,
* wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych,
* stosowanie kwarantanny,
* wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear)
* skanowanie urządzeń USB natychmiast po podłączeniu,
* automatyczne odłączanie zainfekowanej końcówki od sieci,
* skanowanie plików w czasie rzeczywistym, na żądanie, w interwałach czasowych lub poprzez harmonogram, w sposób w pełni konfigurowalny w stosunku do podejmowanych akcji w przypadku wykrycia zagrożenia, z możliwością wykluczenia typu pliku lub lokalizacji.
* Zarządzanie „aktywami” stacji klienckiej, zbierające informacje co najmniej o nazwie komputera, producencie i modelu komputera, przynależności do grupy roboczej/domeny, szczegółach systemu operacyjnego, lokalnych kontach użytkowników, dacie i godzinie uruchomienia i ostatniego restartu komputera, parametrach sprzętowych (proc.,RAM, SN, storage), BIOS, interfejsach sieciowych, dołączonych peryferiach.
* Musi posiadać moduł ochrony IDS/IPS
* Musi posiadać mechanizm wykrywania skanowania portów
* Musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania skanowania portów
* Moduł wykrywania ataków DDoS musi posiadać kilka poziomów wrażliwości

Szyfrowanie danych:* Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. Pełne szyfrowanie dysków działających m.in. na komputerach z systemem Windows.
* Zapobiegające utracie danych z powodu utraty / kradzieży punktu końcowego. Oprogramowanie szyfruje całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnia je tylko autoryzowanym użytkownikom.

Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej.Istnieje możliwość blokady zapisywanie plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach.Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną any ransomware.Zaawansowane monitorowanie krytycznych danych użytkownika zapewniające zapobiegające prze niezamierzonymi manipulacjami – ataki ransomware Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej:* Przechowywanie danych w bazie typu SQL, z której korzysta funkcjonalność raportowania konsoli
* Zdalną instalację lub deinstalację oprogramowania ochronnego na stacjach klienckich, na pojedynczych punktach, zakresie adresów IP lub grupie z ActiveDirectory
* Tworzenie paczek instalacyjnych oprogramowania klienckiego, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi dla Windows oraz formatach dla systemów Linux
* Centralną dystrybucję na zarządzanych klientach uaktualnień definicji ochronnych, których źródłem będzie plik lub pliki wgrane na serwer konsoli przez administratora, bez dostępu do sieci Internet.
* Raportowanie dostępne przez dedykowany panel w konsoli, z prezentacją tabelaryczną i graficzną, z możliwością automatycznego czyszczenia starych raportów, z możliwością eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i dane/raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich
* Definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji

Zarządzanie przez Chmurę:1. Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach
2. Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury
3. Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur
4. Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy
5. Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach
6. Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń
7. Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej

Centralna konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, dystrybucji szyfrowania, polityk i centralnie zarządzanie informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych w nagłych przypadkach.Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania.1. Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer
2. Oprogramowanie klienckie, zarządzane z poziomu serwera.

System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej:* różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie
* funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD
* funkcje regulowania połączeń WiFi i Bluetooth
* funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe
* funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi
* funkcje blokowania dostępu dowolnemu urządzeniu
* możliwość tymczasowego dodania dostępu do urządzenia przez administratora
* zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu
* możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka
* możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora
* możliwość zarządzani urządzeniami podłączanymi do końcówki, takimi jak iPhone, iPad, iPod, Webcam, card reader, BlackBerry
* możliwość używania tylko zaufanych urządzeń sieciowych, w tym urządzeń wskazanych na końcówkach klienckich
* funkcję wirtualnej klawiatury
* możliwość blokowania każdej aplikacji
* możliwość zablokowania aplikacji w oparciu o kategorie
* możliwość dodania własnych aplikacji do listy zablokowanych
* zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach klientach poprzez konsole administracyjna na serwerze
* dodawanie innych aplikacji
* dodawanie aplikacji w formie portable
* możliwość wyboru pojedynczej aplikacji w konkretnej wersji
* dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB
* kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool
* możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki.
* możliwość zablokowania funkcji Printscreen
* funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows jak i Osx
* funkcje monitorowania i kontroli przepływu poufnych informacji
* możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików
* możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj
* możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe
* ochronę przed wyciekiem informacji na drukarki lokalne i sieciowe
* ochrona zawartości schowka systemu
* ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL
* możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych
* ochrona plików zamkniętych w archiwach
* Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem
* możliwość tworzenia profilu DLP dla każdej polityki
* wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania
* ochrona przez wyciekiem plików poprzez programy typu p2p

Monitorowanie zmian w plikach:* Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych.
* Funkcje monitorowania określonych rodzajów plików.
* Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania.
* Generator raportów do funkcjonalności monitora zmian w plikach.
* możliwość śledzenia zmian we wszystkich plikach
* możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach
* możliwość definiowana własnych typów plików

Optymalizacja systemu operacyjnego stacji klienckich:* usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku
* optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem
* możliwość zaplanowania optymalizacje na wskazanych stacjach klienckich
* instruktaż stanowiskowy pracowników Zamawiającego
* dokumentacja techniczna w języku polskim

Wspierane platformy i systemy operacyjne:1. Microsoft Windows XP/7/8/10/ Professional (32-bit/64-bit)
2. Microsoft Windows Server Web / Standard / Enterprise/ Datacenter (32-bit/64-bit)
3. Mac OS X, Mac OS 10
4. Linux 64-bit, Ubuntu, openSUSE, Fedora 14-25, RedHat

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:
	1. Microsoft Internet Explorer
	2. Microsoft Edge
	3. Mozilla Firefox
	4. Google Chrome
	5. 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. Nod skanujący w postaci aplikacji instalowanej lokalnie dostępny jest na poniższe systemy operacyjne:
	1. Windows 2008 R2
	2. Windows 2012
	3. Windows 2012 R2
	4. Windows 2016
7. Portal zarządzający musi umożliwiać:
	1. przegląd wybranych danych na podstawie konfigurowalnych widgetów
	2. zablokowania możliwości zmiany konfiguracji widgetów
	3. zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów.
	4. tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności
	5. eksport wszystkich skanów podatności do pliku CSV
 |
| Warunki gwarancjiWsparcie techniczne | Minimum 3-letnia gwarancja producenta, Czas reakcji serwisu - do końca następnego dnia roboczego. W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego.Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. |

1. **Microsoft Office Home & Business 2021 lub równoważny Pakiet biurowy - 10 szt.**

# **Pakiet biurowy musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:**

1. Dostępność pakietu w wersjach 32-bit oraz 64-bit umożliwiającej wykorzystanie ponad 2 GB przestrzeni adresowej.
2. Wymagania odnośnie interfejsu użytkownika:
	1. Pełna polska wersja językowa interfejsu użytkownika.
	2. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
3. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki:
	1. Posiada kompletny i publicznie dostępny opis formatu.
	2. Ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.
	3. Pozwala zapisywać dokumenty w formacie XML.
4. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb Zamawiającego.
5. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).
6. Do aplikacji pakietu musi być dostępna pełna dokumentacja w języku polskim.
7. Pakiet zintegrowanych aplikacji biurowych musi zawierać:
	1. Edytor tekstów.
	2. Arkusz kalkulacyjny.
	3. Narzędzie do przygotowywania i prowadzenia prezentacji.
	4. Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami).
8. Edytor tekstów musi umożliwiać:
	1. Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.
	2. Wstawianie oraz formatowanie tabel.
	3. Wstawianie oraz formatowanie obiektów graficznych.
	4. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).
	5. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.
	6. Automatyczne tworzenie spisów treści.
	7. Formatowanie nagłówków i stopek stron.
	8. Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.
	9. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
	10. Określenie układu strony (pionowa/pozioma), niezależnie dla każdej sekcji dokumentu.
	11. Wydruk dokumentów.
	12. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.
	13. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2007 lub Microsoft Word 2010, 2013, 2016 i 2019 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu.
	14. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
	15. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem.
	16. Wymagana jest dostępność mechanizmów umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.
9. Arkusz kalkulacyjny musi umożliwiać:
	1. Tworzenie raportów tabelarycznych.
	2. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych.
	3. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
	4. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML).
	5. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych.
	6. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych.
	7. Wyszukiwanie i zamianę danych.
	8. Wykonywanie analiz danych przy użyciu formatowania warunkowego.
	9. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie.
	10. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
	11. Formatowanie czasu, daty i wartości finansowych z polskim formatem.
	12. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
	13. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2007 oraz Microsoft Excel 2010, 2013, 2016 i 2019, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.
	14. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
10. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
	1. Przygotowywanie prezentacji multimedialnych, które będą:
	2. Prezentowanie przy użyciu projektora multimedialnego.
	3. Drukowanie w formacie umożliwiającym robienie notatek.
	4. Zapisanie jako prezentacja tylko do odczytu.
	5. Nagrywanie narracji i dołączanie jej do prezentacji.
	6. Opatrywanie slajdów notatkami dla prezentera.
	7. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo.
	8. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego.
	9. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym.
	10. Możliwość tworzenia animacji obiektów i całych slajdów.
	11. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera.
	12. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2007, MS PowerPoint 2010, 2013, 2016 i 2019.
11. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:
	1. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego.
	2. Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych.
	3. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców.
	4. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną.
	5. Automatyczne grupowanie wiadomości poczty o tym samym tytule.
	6. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy.
	7. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów.
	8. Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie.
	9. Zarządzanie kalendarzem.
	10. Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników.
	11. Przeglądanie kalendarza innych użytkowników.
	12. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach.
	13. Zarządzanie listą zadań.
	14. Zlecanie zadań innym użytkownikom.
	15. Zarządzanie listą kontaktów.
	16. Udostępnianie listy kontaktów innym użytkownikom.
	17. Przeglądanie listy kontaktów innych użytkowników.
	18. Możliwość przesyłania kontaktów innym użytkowników.
	19. Możliwość wykorzystania do komunikacji z serwerem pocztowym mechanizmu MAPI poprzez http.

**CZĘŚĆ III**

1. **Minimalne szczegółowe wymagania techniczne dla zapory UTM (firewall) – 1 szt.**

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 realizowane 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 3 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 20 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 1,8 Gbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 6,5 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 630 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. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego 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**

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 uprawniająca 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 dwuskładnikowego.
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 dwuskładnikowego 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 Firewall 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. W ramach logowania system pełniący funkcję Firewall 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 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: 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. 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.
2. Wykonawca musi zapewnić pierwszą linię wsparcia w języku polskim trybie 8x5. W celu realizacji wymogu wymagane jest posiadanie co najmniej dwóch inżynierów z aktualnym certyfikatem producenta oferowanego rozwiązania (jeżeli producent oferowanego rozwiązania stosuje stopniowy system certyfikacji to co najmniej jeden z inżynierów musi posiadać najwyższy stopień certyfikacji) oraz ISO 9001 w zakresie serwisowania urządzeń informatycznych. Wszystkie certyfikaty należy dołączyć do oferty. Zamawiający dopuszcza, aby usługę wsparcia świadczył autoryzowany dystrybutor oferowanego urządzenia, ale wtedy wraz z ofertą należy dostarczyć oświadczenie tego dystrybutora o gotowości świadczenia takiego wsparcia na rzecz Zamawiającego wraz z zakresem tego wsparcia.