**CZĘŚĆ I PRZETARGU**

1. Komputery stacjonarne (35 szt.)

|  |  |
| --- | --- |
| **Wykonawca oferuje sprzęt:** | *(model, symbol, producent)* |

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Wypełnia Wykonawca wpisując: parametry, rozwiązania techniczne dostarczanego sprzętu i oprogramowania lub określenie spełnia/nie spełnia 1** |
|  | Typ  i zastosowanie | Komputer stacjonarny wykorzystywany dla potrzeb aplikacji biurowych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego komputera. |  |
|  | Wydajność | Procesor wielordzeniowy zaprojektowany do pracy w komputerach stacjonarnych klasy x86. Poziom wydajności w PerformanceTest w teście CPU Mark nie mniejszy niż 9 000 punktów według wyników opublikowanych na <http://www.cpubenchmark.net/>. Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu. |  |
|  | Pamięć operacyjna | Min. 8GB DDR4 z możliwością rozszerzenia do 32 GB |  |
|  | Pamięć masowa | Min 512GB SSD M.2 PCIe NVMe zawierający RECOVERY umożliwiające odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. |  |
|  | Grafika | Zintegrowana z płytą główną lub dedykowana o wydajności w PassMark - G3D Mark w teście Average G3D Mark nie mniejszy niż 2700 punktów według wyników opublikowanych na http:// [www.videocardbenchmark.net](http://www.videocardbenchmark.net)  Min:  - 1 x HDMI  - 1 x Display Port |  |
|  | Komunikacja | |  |  | | --- | --- | | Karta sieciowa | 10/100/1000 | |  |
|  | Obudowa | Typu tower z obsługą kart PCI Express o wysokim (pełnym) profilu  Fabrycznie umożliwiająca montaż min. 2 kieszeni: 1 szt. zewnętrzna, 1 szt. 3,5”na standardowy dysk twardy, wewnętrzna zatoka do rozbudowy o dysk 3,5”  Wbudowany głośnik o mocy min. 2W  Zasilacz min. 500W o sprawności minimum 85%  Obudowa trwale oznaczona nazwą producenta, nazwą komputera i numerem seryjnym |  |
|  | Płyta główna | Zaprojektowana i wyprodukowana przez producenta komputera  Wyposażona w złącza min.:   * 1x PCI Express 3.0 x16, * 1x PCI Express 3.0 x1, * 2x M.2 (min. 1 przeznaczona dla dysku SSD PCIe NVMe) |  |
|  | Wymagania dodatkowe | Wbudowane porty/złącza (min):  1 x USB 3.2 Gen 2  1 x USB 3.2 Gen 2 (Typ-C)  6 x USB  Audio tylny panel  1 x USB 3.2 Gen 1 (Typ-C) z przodu obudowy  1 x USB 3.2 Gen 2 z przodu obudowy Złącze Audio z przodu obudowy  - port sieciowy RJ-45,  - porty słuchawek i mikrofonu na przednim lub tylnym panelu obudowy  Wymagana ilość i rozmieszczenie portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.  Klawiatura przewodowa w układzie US  Mysz przewodowa (scroll) |  |
|  | BIOS | BIOS zgodny ze specyfikacją UEFI   Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych informacji o:   - modelu komputera, PN  - numerze seryjnym,  - numerze inwentarzowym,  - MAC Adres karty sieciowej,  - wersja Biosu wraz z datą produkcji,  - zainstalowanym procesorze, jego taktowaniu i ilości rdzeni  - ilości pamięci RAM wraz z taktowaniem,  - stanie pracy wentylatora na procesorze  - napędach lub dyskach podłączonych do portów SATA oraz M.2 (model dysku i napędu optycznego)  Możliwość z poziomu Bios:  - wyłączania/włączania portów USB zarówno z przodu jak i z tyłu obudowy  - wyłączenia selektywnego (pojedynczego) portów SATA,  - wyłączenia karty sieciowej, karty audio, portu szeregowego,  - możliwość ustawienia portów USB w jednym z dwóch trybów:   1. użytkownik może kopiować dane z urządzenia pamięci masowej podłączonego do pamięci USB na komputer, ale nie może kopiować danych z komputera na urządzenia pamięci masowej podłączone do portu USB 2. użytkownik nie może kopiować danych z urządzenia pamięci masowej podłączonego do portu USB na komputer oraz nie może kopiować danych z komputera na urządzenia pamięci masowej   - ustawienia hasła: administratora, Power-On, HDD,  - blokady aktualizacji BIOS bez podania hasła administratora  - wglądu w system zbierania logów (min. Informacja o update Bios, błędzie wentylatora na procesorze, wyczyszczeniu logów) z możliwością czyszczenia logów  - alertowania zmiany konfiguracji sprzętowej komputera  - załadowania optymalnych ustawień Bios  - obsługa Bios za pomocą klawiatury i myszy |  |
|  | Zintegrowany System Diagnostyczny | Wizualny system diagnostyczny producenta działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera umożliwiający na wykonanie diagnostyki następujących podzespołów:   * wykonanie testu pamięci RAM * test dysku twardego lub SSD * test monitora * test magistrali PCI-e * test portów USB * test płyty głównej * test myszy i klawiatury * test procesora   Wizualna lub dźwiękowa sygnalizacja w przypadku błędów któregokolwiek z powyższych podzespołów komputera.  Ponadto system powinien umożliwiać identyfikacje testowanej jednostki i jej komponentów w następującym zakresie:   * PC: Producent, model * BIOS: Wersja oraz data wydania Bios * Procesor: Nazwa, taktowanie * Pamięć RAM: Ilość zainstalowanej pamięci RAM, producent oraz numer seryjny poszczególnych kości pamięci * Dysk: model, numer seryjny, wersja firmware, pojemność, temperatura pracy * Monitor: producent, model, rozdzielczość   System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera. |  |
|  | Certyfikaty | * ISO 9001 * ISO 14001 * deklaracja zgodności CE |  |
|  | Ergonomia i bezpieczeństwo | - Złącze typu Kensington Lock  - Układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania TPM 2.0 |  |
|  | Zainstalowane oprogramowanie | Microsoft Windows 10 Pro 64 bit lub system operacyjny klasy PC, który spełnia następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:  1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:  a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,  b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych  2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego  3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim  4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.  5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe  6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,  7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.  8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim  9. Wbudowany system pomocy w języku polskim.  10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).  11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.  12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.  13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.  14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.  15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze.  16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".  17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy.  18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.  19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.  20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.  21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.  22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.  23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)."  24. Wbudowany mechanizm wirtualizacji typu hypervisor."  25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.  26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.  27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.  28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).  29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi.  30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne.  31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.  32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM  33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych.  34. Możliwość tworzenia wirtualnych kart inteligentnych.  35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot)  36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.  37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.  38. Mechanizmy logowania w oparciu o:  a. Login i hasło,  b. Karty inteligentne i certyfikaty (smartcard),  c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),  d. Certyfikat/Klucz i PIN,  e. Certyfikat/Klucz i uwierzytelnienie biometryczne,  39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5  40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej.  41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach  42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń  43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń |  |
|  | Gwarancja | 2-letnia |  |

# Monitor LCD (40 szt.)

|  |  |
| --- | --- |
| **Wykonawca oferuje sprzęt:** | *(model, symbol, producent)* |

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Wypełnia Wykonawca wpisując: parametry, rozwiązania techniczne dostarczanego sprzętu i oprogramowania lub określenie spełnia/nie spełnia 1** |
|  | Proporcje obrazu | 16:9 |  |
|  | Przekątna ekranu | Min. 27" |  |
|  | Powierzchnia matrycy | Matowa |  |
|  | Technologia podświetlania | Diody LED |  |
|  | Rozdzielczość | Min. 1920 x 1080 (FHD 1080) |  |
|  | Kontrast statyczny | Min. 1 000:1 |  |
|  | Kontrast dynamiczny | Min. 3 000 000:1 |  |
|  | Gniazda we/wy | 1 x 3,5 mm minijack  1 x 15-pin D-Sub  1 x HDMI  1 x DisplayPort  5 x USB 3.0 |  |
|  | Pivot | Tak |  |
|  | Certyfikaty | * ISO 9001 * ISO 14001 * deklaracja zgodności CE |  |
|  | Standard VESA | 100 x 100 |  |
|  | Pobór mocy | Max. 23 W |  |
|  | Akcesoria w zestawie | Przewód zasilający  Kabel DP-DP  Kabel USB 3.0  Przewodnik szybkiej instalacji |  |
|  | Pozostałe parametry | Kąt nachylenia (przód / tył): -5° / 30°  Kąt obrotu (lewo / prawo): -45° / +45°  Podnoszenie (maksymalny zakres): 110 mm |  |
|  | Gwarancja | 2-letnia |  |

# NAS Backup (1 szt.)

|  |  |
| --- | --- |
| **Wykonawca oferuje sprzęt:** | *(model, symbol, producent)* |

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Wypełnia Wykonawca wpisując: parametry, rozwiązania techniczne dostarczanego sprzętu i oprogramowania lub określenie spełnia/nie spełnia 1** |
|  | Procesor | Min. Dwurdzeniowy o taktowaniu zegara min 2,00 GHz w trybie turbo do 2.90GHz  - pamięć podręczna min: 4 MB  - TDP max. 10 W |  |
|  | Wbudowana pamięć RAM | Min. 2 GB |  |
|  | Wielkość pamięci | Min. 6 GB |  |
|  | Rodzaj pamięci | DDR4 |  |
|  | Liczba wszystkich gniazd pamięci | 1 |  |
|  | Liczba zainstalowanych dysków tw. | 0 |  |
|  | Maks. liczba dysków | 2 |  |
|  | RAID | Tak |  |
|  | Poziomy RAID | - 0  - 1 |  |
|  | Architektura sieci | GigabitEthernet |  |
|  | Interfejs sieciowy | 2 x 10/100/1000 Mbit/s |  |
|  | Gniazda we/wy | 2 x RJ-45 LAN  2 x USB 3.0 |  |
|  | Liczba wentylatorów | Min. 1szt. |  |
|  | Obudowa | Desktop |  |
|  | Akcesoria w zestawie | Jednostka główna  Pakiet akcesoriów  Zasilacz sieciowy  Przewód zasilający AC  Kabel LAN RJ-45 X 2  Instrukcja szybkiej instalacji |  |
|  | Gwarancja | 2-letnia |  |

# Oprogramowanie antywirusowe (1 szt.)

|  |  |
| --- | --- |
| **Wykonawca oferuje:** | *(nazwa, producent)* |

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Wypełnia Wykonawca wpisując: parametry, rozwiązania techniczne dostarczanego sprzętu i oprogramowania lub określenie spełnia/nie spełnia 1** |
| 1 | Administracja zdalna | 1. Rozwiązanie musi wspierać instalację na systemach Windows Server (od 2012), Linux oraz w postaci maszyny wirtualnej w formacie OVA lub dysku wirtualnego w formacie VHD. 2. Rozwiązanie musi zapewniać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL. 3. Rozwiązanie musi zapewniać pobranie wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta. 4. Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania w języku polskim z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL. 5. Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów. 6. Rozwiązanie musi zapewniać utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi. 7. Rozwiązanie musi wspierać zarządzanie urządzeniami z systemem iOS i Android. 8. Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, które działają na stacjach roboczych w sieci. 9. Rozwiązanie musi zapewniać weryfikację podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe). 10. Rozwiązanie musi zapewniać instalowanie i odinstalowywanie oprogramowania firm trzecich dla systemów Windows oraz MacOS oraz odinstalowywanie oprogramowania zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT. 11. Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 12. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. 13. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. 14. Rozwiązanie musi zapewniać korzystanie z minimum 100 szablonów raportów, przygotowanych przez producenta oraz musi zapewniać tworzenie własnych raportów przez administratora. 15. Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog. 16. Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami. |  |
| 2 | Ochrona stacji roboczych | 1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 7/Windows 8/Windows 8.1/Windows 10/Windows 11). 2. Rozwiązanie musi wspierać architekturę ARM64. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. 5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych orazpodejrzanych aplikacji. 6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. 9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku. 10. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 11. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 12. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 13. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 14. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia. 15. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:  * tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, * tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, * tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, * tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, * tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.  1. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. 2. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. 3. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. 4. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 5. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 6. Rozwiązanie musi posiadać ochronę antyspamową dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail. 7. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:  * tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące, * tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie, * tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora, * tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.  1. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki. 2. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika. 3. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki. 4. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych. 5. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 100 kategorii i podkategorii. |  |
| 3 | Ochrona serwera | 1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7 i 8, CentOS 7 i 8, Ubuntu Server 16.04 LTS i nowsze, Debian 9, Debian 10, SUSE Linux Enterprise Server (SLES) 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux oraz Amazon Linux. 2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS. 5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji. 7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. 8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. |  |
| 4 | Dodatkowe wymagania dla ochrony serwerów Windows | 1. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. 2. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS). 3. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. 4. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 5. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 6. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 7. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 8. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. 9. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu. |  |
| 5 | Dodatkowe wymagania dla ochrony serwerów Linux | 1. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. 2. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. 3. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon. 4. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu. |  |
| 6 | Ochrona urządzeń mobilnych opartych o system Android | 1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. 2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne. 3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). 4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM. 5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi: 6. usunięcie zawartości urządzenia, 7. przywrócenie urządzenie do ustawień fabrycznych, 8. zablokowania urządzenia, 9. uruchomienie sygnału dźwiękowego, 10. lokalizację GPS. 11. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. 12. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: 13. nazwę aplikacji, 14. nazwę pakietu, 15. kategorię sklepu Google Play, 16. uprawnienia aplikacji, 17. pochodzenie aplikacji z nieznanego źródła. |  |

# Oprogramowanie biurowe, standard (50 szt.)

|  |  |
| --- | --- |
| **Wykonawca oferuje:** | *(nazwa, producent)* |

Pakiet standardowego oprogramowania biurowego pozwalający na edytowanie tekstów, tworzenie arkuszy kalkulacyjnych, prezentacji oraz klient poczty (wraz z nośnikiem). Licencja przenaszalna nie przypisana do konkretnej jednostki komputerowej. Pakiet zapakowany w zafoliowane, nieotwierane pudełko.

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Wypełnia Wykonawca wpisując: parametry, rozwiązania techniczne dostarczanego sprzętu i oprogramowania lub określenie spełnia/nie spełnia 1** |
| 1. | Oferowane funkcje | * + - 1. Tworzenie i edycja tekstu       2. Tworzenie i edycja arkuszy kalkulacyjnych       3. Tworzenie i edycja prezentacji       4. Klient poczty współpracujący w pełnym zakresie funkcjonalności z serwerem MS Exchange (e-mail, zadania, kalendarze)       5. Możliwość automatycznej instalacji komponentów (przy użyciu instalatora systemowego),       6. Możliwość zdalnej instalacji pakietu poprzez zasady grup (GPO),       7. Całkowicie zlokalizowany w języku polskim system komunikatów i podręcznej pomocy technicznej w pakiecie,       8. Możliwość prowadzenia dyskusji i subskrypcji dokumentów w sieci z automatycznym powiadomieniem o zmianach w dokumentach,       9. Możliwość delegacji uprawnień w systemach pocztowych do otwierania, drukowania, modyfikowania i czytania załączanych dokumentów i informacji,       10. Możliwość blokowania niebezpiecznej lub niechcianej poczty,       11. Współpraca z systemem MS Exchange, w tym odbiór poczty, możliwość udostępniania kalendarza dla innych użytkowników       12. Wsparcie dla formatu XML w podstawowych aplikacjach,       13. Możliwość nadawania uprawnień do modyfikacji i formatowania dokumentów lub ich fragmentów,       14. Automatyczne przesyłanie poczty na podstawie reguł, automatyczne odpowiedzi,       15. Możliwość automatycznego odświeżania danych pochodzących z Internetu w arkuszach kalkulacyjnych,       16. Możliwość dodawania do dokumentów i arkuszy kalkulacyjnych podpisów cyfrowych, pozwalających na stwierdzenie czy dany dokument/arkusz pochodzi z bezpiecznego źródła i nie został w żaden sposób zmieniony,       17. Możliwość zaszyfrowania danych w dokumentach i arkuszach kalkulacyjnych zgodnie ze standardem CryptoAPI,       18. Możliwość automatycznego odzyskiwania dokumentów i arkuszy kalkulacyjnych w wypadku odcięcia dopływu prądu.       19. Prawidłowe odczytywanie i zapisywanie danych w dokumentach w formatach: .DOC,.DOCX, XLS, XLSX, w tym obsługa formatowania makr, formuł, formularzy w plikach wytworzonych w MS Office 2010,2013, 2016, 2019 |  |

# Oprogramowanie biurowe, wersja PRO (1 szt.)

|  |  |
| --- | --- |
| **Wykonawca oferuje:** | *(nazwa, producent)* |

Pakiet standardowego oprogramowania biurowego pozwalający na edytowanie tekstów, tworzenie arkuszy kalkulacyjnych, prezentacji oraz klient poczty (wraz z nośnikiem). Licencja przenaszalna nie przypisana do konkretnej jednostki komputerowej. Pakiet zapakowany w zafoliowane, nieotwierane pudełko.

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Wypełnia Wykonawca wpisując: parametry, rozwiązania techniczne dostarczanego sprzętu i oprogramowania lub określenie spełnia/nie spełnia 1** |
| 1. | Oferowane funkcje | * + - 1. Tworzenie i edycja tekstu       2. Tworzenie i edycja arkuszy kalkulacyjnych       3. Tworzenie i edycja prezentacji       4. Klient poczty współpracujący w pełnym zakresie funkcjonalności z serwerem MS Exchange (e-mail, zadania, kalendarze)       5. Możliwość automatycznej instalacji komponentów (przy użyciu instalatora systemowego),       6. Możliwość zdalnej instalacji pakietu poprzez zasady grup (GPO),       7. Całkowicie zlokalizowany w języku polskim system komunikatów i podręcznej pomocy technicznej w pakiecie,       8. Możliwość prowadzenia dyskusji i subskrypcji dokumentów w sieci z automatycznym powiadomieniem o zmianach w dokumentach,       9. Możliwość delegacji uprawnień w systemach pocztowych do otwierania, drukowania, modyfikowania i czytania załączanych dokumentów i informacji,       10. Możliwość blokowania niebezpiecznej lub niechcianej poczty,       11. Współpraca z systemem MS Exchange, w tym odbiór poczty, możliwość udostępniania kalendarza dla innych użytkowników       12. Wsparcie dla formatu XML w podstawowych aplikacjach,       13. Możliwość nadawania uprawnień do modyfikacji i formatowania dokumentów lub ich fragmentów,       14. Automatyczne przesyłanie poczty na podstawie reguł, automatyczne odpowiedzi,       15. Możliwość automatycznego odświeżania danych pochodzących z Internetu w arkuszach kalkulacyjnych,       16. Możliwość dodawania do dokumentów i arkuszy kalkulacyjnych podpisów cyfrowych, pozwalających na stwierdzenie czy dany dokument/arkusz pochodzi z bezpiecznego źródła i nie został w żaden sposób zmieniony,       17. Możliwość zaszyfrowania danych w dokumentach i arkuszach kalkulacyjnych zgodnie ze standardem CryptoAPI,       18. Możliwość automatycznego odzyskiwania dokumentów i arkuszy kalkulacyjnych w wypadku odcięcia dopływu prądu.       19. Prawidłowe odczytywanie i zapisywanie danych w dokumentach w formatach: .DOC,.DOCX, XLS, XLSX, w tym obsługa formatowania makr, formuł, formularzy w plikach wytworzonych w MS Office 2010,2013, 2016, 2019       20. Możliwość projektowania, tworzenia, edycji, zarządzania relacyjnymi bazami danych,       21. Możliwość tworzenia publikacji graficznych, materiałów marketingowych, ulotek, plakatów. |  |

# Firewall (1 szt.)

|  |  |
| --- | --- |
| **Wykonawca oferuje:** | *(nazwa, producent)* |

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Wypełnia Wykonawca wpisując: parametry, rozwiązania techniczne dostarczanego sprzętu i oprogramowania lub określenie spełnia/nie spełnia 1** |
| 1 | Obsługa sieci | 1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP. |  |
| 2 | Zapora korporacyjna (Firewall) | 1. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. 2. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. 3. Urządzenie ma dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). 4. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. 5. Administrator musi mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola DSCP nagłówka pakietu, godziny oraz dnia nawiązywania połączenia. 6. Rozwiązanie musi umożliwiać między innymi filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. 7. Administrator ma możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall. 8. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów). 9. Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows 2k (Kerberos). |  |
| 3 | Intrusion prevention system (IPS) | 1. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalia w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. 2. Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy. 3. Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. 4. Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS. 5. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej. 6. Urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS. 7. Administrator urządzenia ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP. 8. Urządzenie ma mieć możliwość ochrony między innymi przed atakami typu SQL injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0. |  |
| 4 | Kształtowanie pasma (Traffic Shapping) | 1. Urządzenie ma mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. 2. Ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. 3. Rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring). 4. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch. |  |
| 5 | Ochrona antywirusowa | 1. Rozwiązanie ma zezwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania). 2. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji. 3. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. 4. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu odrzucenia. |  |
| 6 | Ochrona antyspam | 1. Producent ma udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). 2. Ochrona antyspam ma działać w oparciu o:    1. białe/czarne listy,    2. DNS RBL,    3. heurystyczny skaner. 3. W przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL. 4. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin. |  |
| 7 | Wirtualne sieci prywante (VPN) | 1. Urządzenie ma posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). 2. Odpowiednio kanały VPN można budować w oparciu o:    1. PPTP VPN,    2. IPSec VPN,    3. SSL VPN. 3. SSL VPN musi działać w trybach Tunel i Portal. 4. W ramach funkcji SSL VPN producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. 5. Urządzenie ma posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). 6. Urządzenie ma posiadać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf. 7. Urządzenie ma umożliwiać tworzenie tuneli w oparciu o technologię Route Based. |  |
| 8 | Filtr dostępu do stron WWW | 1. Urządzenie ma posiadać wbudowany filtr URL. 2. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych. 3. Administrator musi mieć możliwość dodawania własnych kategorii URL. 4. Urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora. 5. Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST. 6. Administrator posiada możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji: 7. blokowanie dostępu do adresu URL, 8. zezwolenie na dostęp do adresu URL, 9. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. 10. Administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. 11. Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych. 12. Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS. 13. Urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. 14. Urządzenie posiada możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane. |  |
| 9 | Uwierzytelnianie | 1. Urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o:    1. lokalną bazę użytkowników (wewnętrzny LDAP),    2. zewnętrzną bazę użytkowników (zewnętrzny LDAP),    3. usługę katalogową Microsoft Active Directory. 2. Rozwiązanie musi pozwalać na równoczesne użycie co najmniej 5 różnych baz LDAP. 3. Rozwiązanie ma zezwalać na uruchomienie specjalnego portalu, który umożliwia autoryzacje w oparciu o protokoły:    1. SSL,    2. Radius,    3. Kerberos. 4. Urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory. 5. Co najmniej jedna z metod transparentnej autoryzacji nie wymaga instalacji dedykowanego agenta. 6. Autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu domeny. |  |
| 10 | Administracja łączami do internetu (ISP) | 1. Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). 2. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:    1. równoważenie względem adresu źródłowego,    2. równoważenie względem połączenia. 3. Mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. 4. Urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 5. Urządzenie ma posiadać mechanizm statycznego trasowania pakietów. 6. Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 7. Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. 8. Rozwiązanie powinno zapewniać obsługę routingu dynamicznego w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP. |  |
| 11 | Pozostałe usługi i funkcje rozwiązania | 1. Urządzenie musi posiadać wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci. 2. Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay. 3. Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6. 4. Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS. 5. Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3. 6. Urządzenie musi posiadać usługę DNS Proxy. |  |
| 12 | Administracja urządzeniem | 1. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego. 2. Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. 3. Komunikacja może odbywać się na porcie innym niż https (443 TCP). 4. Urządzenie ma być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. 5. Rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana. 6. Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. 7. Urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów powinno być możliwe za pomocą transmisji szyfrowanej (TLS). 8. Rozwiązanie ma mieć możliwość eksportowania logów za pomocą protokołu IPFIX. 9. Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora. 10. Urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora. 11. Urządzenie musi posiadać funkcjonalność anonimizacji logów. 12. Urządzenie ma mieć możliwość bezpośredniego podłączenia karty pamięci typu SD w celu zbierania logów. |  |
| 13 | Raportowanie | 1. Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. 2. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. 3. System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego. 4. System raportujący musi umożliwiać wygenerowanie co najmniej 5 różnych raportów. 5. System raportujący ma dawać możliwość edycji konfiguracji z poziomu raportu. 6. W ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny. 7. Dodatkowy system umożliwia tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy. |  |
| 14 | Parametry sprzętowe | 1. Urządzenie musi być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać z wbudowanej pamięci flash. 2. Liczba portów Ethernet 10/100/1000Mbps – min. 8. 3. Urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G pochodzącego od dowolnego producenta. 4. Przepustowość Firewall – min. 4 Gbps. 5. Przepustowość Firewall wraz z włączonym systemem IPS – min. 2,4 Gbps. 6. Przepustowość filtrowania Antywirusowego – min. 495 Mbps. 7. Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 600 Mbps. 8. Maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż 100. 9. Maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 20. 10. Obsługa min. VLAN 64. 11. Liczba równoczesnych sesji - min. 300 000 i nie mniej niż 18 000 nowych sesji/sekundę. 12. Urządzenie musi dawać możliwość budowania klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive. 13. Urządzenie jest nielimitowane na użytkowników. |  |
| 15 | Ochrona przed wyciekiem danych (DLP) | * + - 1. Pełne wsparcie dla stacji roboczych z systemami Windows 7/Windows 8.1/Windows 10/Windows 11.       2. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2012 i nowszych.       3. Pomoc w programie (help) i dokumentacja do programu dostępna w języku angielskim.       4. Konsola administracyjna oraz komunikaty klienta muszą być w języku polskim.       5. Serwer administracyjny musi wspierać instalację w oparciu o bazę MS SQL.       6. Serwer administracyjny musi działać w architekturze serwer-klient, gdzie komunikacja serwera zarządzającego z klientem odbywa się przy pomocy agenta.       7. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.       8. Serwer administracyjny musi umożliwiać wykonanie instalacji/dezinstalacji zdalnej klienta na stacjach roboczych.       9. Reguły DLP muszą być egzekwowane również w przypadku braku połączenia między klientem, a serwerem zarządzającym.       10. W przypadku braku połączenia klienta z serwerem zarządzającym, klient musi mieć możliwość lokalnego przechowywania informacji oraz zebranych danych do czasu ponownego połączenia z serwerem administracyjnym.       11. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsol.       12. Administrator musi posiadać możliwość zarządzania bazą danych poprzez określone zadania: kopia bazy danych, kopia oraz wyczyszczenie bazy danych, wyczyszczenie bazy danych.  Administrator musi posiadać możliwość określenia wykonywania czasu związanego z wykonywaniem zadań na bazie danych. Zadania powinny być wykonywane co najmniej z interwałem: raz na tydzień, raz na dwa tygodnie, raz w miesiącu, raz na trzy miesiące.       13. Administrator musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych. Jeżeli rozmiar bazy danych osiągnie skonfigurowany rozmiar, najstarsze informacje muszą być usunięte z bazy danych, w celu nie przekroczenia skonfigurowanego rozmiaru bazy.       14. Serwer administracyjny programu musi mieć możliwość automatycznego pobierania aktualizacji definicji kategoryzowania stron internetowych, aplikacji oraz rozszerzeń plików. Musi być możliwość wyłączenia automatycznego pobierania.       15. Administrator musi mieć możliwość tworzenia nowych kont administratorów w konsoli programu jak i ich usuwania oraz klonowania.       16. Administrator musi mieć możliwość przypisywania jak i odbierania uprawnień do wybranych modułów programu. Uprawnienia muszą być podzielone na:  1. Ustawienia, które określają możliwość wykonania konfiguracji na poszczególnym module, 2. Logi, które określają możliwość wyświetlenia logów poszczególnego modułu.    * + 1. Serwer musi posiadać możliwość synchronizacji użytkowników oraz stacji roboczych z domeną Active Directory.        2. System musi posiadać możliwość logowania zdarzeń aktywności stacji roboczej, w oparciu o co najmniej: 3. logowanie oraz wylogowanie użytkownika, 4. włączenie oraz wyłączenie stacji roboczej, 5. blokada oraz odblokowanie stacji roboczej, 6. przejście w stan bezczynności stacji roboczej.    * + 1. Administrator musi mieć możliwość, wymuszenia synchronizacji ustawień oraz logów, pomiędzy stacją roboczą, a serwerem, w czasie rzeczywistym.        2. Serwer administracyjny musi mieć możliwość ustawienia powiadomień dla użytkownika końcowego, w przypadku złamania reguł ustawionych w modułach związanymi z ochroną DLP. W powiadomieniu administrator musi posiadać możliwość określenia własnej grafiki, kontaktowego adresu e-mail oraz odnośnika do polityki bezpieczeństwa organizacji.        3. Oprogramowanie musi posiadać możliwości audytu stacji roboczych/użytkowników w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, ruch sieciowy, wysyłane oraz odebrane wiadomości e-mail oraz wykonane czynności na plikach.        4. Administrator musi posiadać możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji oraz typów plików.        5. Administrator musi posiadać możliwość filtrowania oraz sortowania zebranych danych. Tak odfiltrowane dane, administrator może zapisać w postaci plików PDF bądź XLS.        6. Konsola musi posiadać możliwość wysyłania powiadomień, jeśli dany użytkownik przekroczy określoną dopuszczalną ilość wysyłanych maili oraz w przypadku przekroczenia dopuszczalnej ilości wysyłanych danych do sieci w danym dniu lub tygodniu.        7. Serwer musi posiadać możliwość wysłania alertów, co najmniej za pośrednictwem wiadomości email.        8. Serwer administracyjny musi posiadać możliwość konfiguracji raportów w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, drukowane dokumenty, ruch sieciowy, wysyłane wiadomości e-mail oraz wykonywane czynności na plikach.        9. Raporty muszą być generowane w oparciu o wskazane stacje robocze, użytkowników bądź grupy w określonym przedziale czasu.        10. Raporty muszą być generowane do pliku PDF i/lub XLS, po podaniu lokalizacji zapisywanego pliku lub na wskazany adres(y) e-mail.        11. Serwer administracyjny musi posiadać wbudowany serwer SMTP udostępniony przez producenta oprogramowania.        12. Serwer administracyjny musi umożliwiać kategoryzację (tagowanie) plików na poziomie systemu plików lub na poziomie metadanych pliku.        13. Serwer administracyjny musi umożliwiać wykonanie zadania kategoryzacji (tagowania) plików, które już znajdują się na stacjach roboczych i zasobach sieciowych, ale również nowych plików, które powstaną na bazie już skategoryzowanych (otagowanych) plików.        14. Serwer administracyjny musi mieć możliwość kategoryzacji (tagowania) plików wrażliwych w oparciu o: 7. aplikacje, z której zostały utworzone, 8. lokalizację, 9. adres URL, 10. format pliku, 11. zawartość pliku.     * + 1. Administrator musi mieć możliwość wyszukiwania danych osobowych na zasobach zarówno lokalnych jak i sieciowych.         2. Dla plików skategoryzowanych (otagowanych), musi być możliwe utworzenie następujących reguł: 12. blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików, do lokalizacji na określonych dyskach lokalnych, 13. blokowanie oraz zezwalanie na zapisywanie, przenoszenie do lokalizacji na dyskach zewnętrznych z możliwością określenia białej oraz czarnej listy tych urządzeń, 14. blokowanie oraz zezwalanie na drukowanie na określonych drukarkach, 15. blokowanie oraz zezwalanie na zapisywanie i przenoszenie do lokalizacji sieciowej, 16. blokowanie oraz zezwalanie na wysyłanie za pośrednictwem klientów pocztowych z możliwością określenia białej i czarnej listy adresów i domen, 17. blokowanie oraz zezwalanie na wysyłanie do poczty webowej, 18. blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików do chmury, zarówno za pomocą przeglądarki internetowej jak i aplikacji, w oparciu o co najmniej poniższe usługi:   • Dropbox,  • Google Drive,  • SharePoint,  • OneDrive Business,  • OneDrive Personal.   1. blokowanie oraz zezwalanie na przesyłanie za pomocą komunikatorów, 2. blokowanie oraz zezwalanie na zapisywanie i przenoszenie danych poprzez usługę pulpitu zdalnego, 3. blokowanie oraz zezwalanie na wykonywanie zrzutów ekranowych, skopiowania zawartości oraz wirtualnego drukowania, 4. uruchomienie wybranego formatu pliku przez wskazaną przez administratora aplikacje,    * + 1. Serwer administracyjny musi umożliwiać możliwość zabezpieczenia korzystania z niezaufanych repozytoriów GIT.        2. Każda z polityk musi posiadać możliwość ustawienia jej w trybie powiadomienia dla użytkownika.        3. Serwer administracyjny musi dawać możliwość klasyfikacji pliku (tagowania) użytkownikowi na stacji roboczej. Klasyfikacja musi odbywać się poprzez integrację z menu kontekstowym.        4. Klasyfikacja użytkownika musi posiadać opcję, która uniemożliwi użytkownikowi zmianę klasyfikacji na niższą.        5. Serwer administracyjny musi umożliwiać określenie białych i czarnych list zawierających urządzenia pamięci masowej, drukarki fizycznych i sieciowych, lokalizacji sieciowych, adresów e-mail oraz domen, urządzeń przenośnych, firewire oraz bluetooth, które mogą być wykorzystywane do określenia reguł dostępu.        6. Serwer administracyjny musi posiadać funkcjonalność globalnego zablokowania lub zezwolenia na korzystanie z określonych folderów lokalnych, sieciowych, dysków o określonych literach oraz folderów synchronizacji z usługami chmury.        7. Serwer musi posiadać funkcjonalność skonfigurowania reguł dostępu dla urządzeń podłączanych do portu USB, urządzeń przenośnych, nośników optycznych CD/DVD, urządzeń Firewire, urządzeń podczerwieni, urządzeń Bluetooth, portów COM oraz LPT.        8. Serwer administracyjny musi posiadać możliwość zaszyfrowania całej powierzchni dysku w oparciu o funkcjonalność BitLocker z użyciem hasła lub modułu TPM.        9. Serwer administracyjny musi posiadać możliwość szyfrowania dysków zewnętrznych w oparciu o funkcjonalność BitLocker. Szyfrowanie oraz autoryzacja dla zaszyfrowanych nośników wymiennych musi być w pełni niezauważalna dla użytkownika.        10. Serwer administracyjny musi posiadać możliwość wyświetlenia i eksportu klucza odzyskiwania do zaszyfrowanych dysków oraz dysków wymiennych.        11. Serwer administracyjny musi posiadać możliwość wyszukiwania i ochrony plików w oparciu o ich zawartość, co najmniej o: 5. numery kart kredytowych, 6. numer PESEL, 7. numer polskiego dowodu osobistego, 8. polski numer paszportu, 9. wyrażenia regularne, 10. określone ciągi znaków, 11. numer IBAN.     * + 1. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.         2. Weryfikacja zawartości pliku w czasie rzeczywistym musi posiadać funkcjonalność OCR (Optical Character Recognition).         3. System musi posiadać możliwość importu własnych słowników do wyszukiwania danych.         4. W przypadku incydentu bezpieczeństwa, system musi wykonać duplikat pliku lub wiadomości e-mail, w którym znajdują się dane wrażliwe (tzw. funkcjonalność „Shadow-copy”).         5. Serwer administracyjny musi posiadać możliwość wyznaczenia progu ilości wystąpień danych wrażliwych, od jakich zostanie uruchomione zadanie klasyfikacji (tagowania).         6. Serwer administracyjny musi posiadać możliwość integracji klasyfikacji danych, z modułem DLP dostępnym na rozwiązaniu FortiGate.         7. Serwer administracyjny musi umożliwiać eksport logów do rozwiązania FortiSIEM.         8. Serwer administracyjny musi umożliwiać eksport identyfikatorów oznaczonych plików do rozwiązania FortiMail, które będzie w stanie kontrolować przesyłanie tak oznaczonych plików.         9. Serwer administracyjny musi umożliwiać integrację z Office365. Integracja musi pozwalać na: 12. audyt i logowanie wiadomości e-mail, 13. audyt i logowanie operacji na plikach, 14. wprowadzanie polityk zabezpieczeń do wiadomości e-mail.     * + 1. System musi umożliwiać integrację z narzędziami analitycznymi tj. Power BI, Tabeau).         2. Serwer administracyjny musi posiadać konsolę dostępną z poziomu przeglądarki internetowej, służącą do raportowania i zarządzania stacjami roboczymi i urządzeniami mobilnymi.         3. Konsola musi wyświetlać informacje na temat bezpieczeństwa danych, produktywności pracowników oraz utylizacji sprzętu które są podzielone na: 15. Bezpieczeństwo danych:  * Przegląd informacji o incydentach bezpieczeństwa. * Przegląd danych przychodzących. * Przegląd danych wychodzących. * Przegląd informacji z Office365 które dotyczą m.in. pobierania, współdzielenia oraz lokalnego dostępu do plików. * Podłączane/odłączane urządzenia przenośne.  1. Produktywność:  * Przegląd informacji na temat produktywności użytkowników. * Aktywność użytkowników podczas przeglądania stron WWW oraz korzystania z aplikacji. * Trendy.  1. Eksploatacja sprzętu:  * Przegląd informacji na temat eksploatacji sprzętu komputerowego. * Eksploatacja sprzętu komputerowego, najbardziej nieaktywne komputery. * Eksploatacja drukarek. * Eksploatacji sieci.   + - 1. Konsola webowa musi posiadać możliwość konfiguracji/zmiany domyślnego serwera SMTP.       2. Konsola webowa musi umożliwiać weryfikację wersji zainstalowanego oprogramowania klienta wraz z możliwością aktualizacji do nowej wersji lub dezaktywacji tego oprogramowania.       3. Konsola webowa musi umożliwiać wygenerowanie raportu w postaci pliku DOCX, który zawiera informacje nt: * plików przenoszonych na nośniki USB i inne urządzenia przenośne, * plików przesłanych za pomocą wiadomości e-mail, * plików przesłanych za pomocą poczty webowej, * plików przesłanych do Internetu, * plików wysłanych za pomocą komunikatorów, * plików przesłanych na dyski chmurowe, * analiza sposobu korzystania z aplikacji, * analiza korzystania z Internetu, * analiza wykorzystania porali do poszukiwania pracy. |  |

…………………………………………….

*(podpis)*

**1 Prawą stronę tabeli, należy wypełnić stosując słowa „spełnia” lub „nie spełnia” w przypadku zapisów ogólnych, w przypadku gdy wymagania są opisane przy pomocy parametrów technicznych lub dopuszczone jest zastosowanie różnych materiałów oraz terminów w tabeli, należy wpisać oprócz powyższych słów oferowane wartości techniczno-użytkowe.**

**W przypadku, gdy Wykonawca w którejkolwiek z pozycji wpisze słowa „nie spełnia” lub zaoferuje niższe wartości oferta zostanie odrzucona, gdyż jej treść jest niezgodna z warunkami zamówienia (art. 226 ust. 1 pkt. 5) ustawy Prawo zamówień publicznych )**