Załącznik nr 1 do SWZ. Szczegółowy opis przedmiotu zamówienia

Dotyczy zamówienia publicznego pn. Dostawa rozwiązań z zakresu cyberbezpieczeństwa, w tym specjalistycznego sprzętu komputerowego i oprogramowania dla Gminy Zamość w ramach projektu „Cyberbezpieczna Gmina Zamość”

# Część 2. Dostawa sprzętu i oprogramowania z usługami wdrożenia dla Gminnego Ośrodka Pomocy Społecznej w Zamościu

Ogólne warunki realizacji zamówienia

1. Przedmiot zamówienia obejmuje dostawy do siedziby jednostki podległej Zamawiającemu – Gminnego Ośrodka Pomocy Społecznej w Zamościu w zakresie i ilościach wskazanych w zestawieniach rzeczowo – ilościowych odpowiednio dla każdej części.
2. Dostarczany sprzęt i oprogramowanie muszą być fabrycznie nowe, nieużywane, nieuszkodzone i nieobciążone prawami osób trzecich.
3. Dostarczany sprzęt i oprogramowanie muszą pochodzić z oficjalnego kanału dystrybucyjnego w UE.
4. Wykonawca zapewni takie opakowanie sprzętu jakie jest wymagane, żeby nie dopuścić do jego uszkodzenia lub pogorszenia jego jakości w trakcie transportu do miejsca dostawy.
5. Sprzęt będzie oznaczony zgodnie z obowiązującymi przepisami, a w szczególności znakami bezpieczeństwa.
6. Urządzenia przeznaczone do montażu w szafie rack Wykonawca zainstaluje w szafach wskazanych przez Zamawiającego, uruchomi je i skonfiguruje w porozumieniu z Zamawiającym. Wykonawca musi dostarczyć wszelkie akcesoria montażowe umożliwiające instalację urządzeń w szafach i ich uruchomienie.
7. Wykonawca wyda Zamawiającemu instrukcje obsługi sprzętu lub – jeśli są one udostępniane przez producenta w formie elektronicznej – przekaże adresy WWW, pod którymi można je pobrać.
8. Dla oprogramowania Wykonawca zobowiązany jest do udzielenia niewyłącznej licencji Zamawiającemu lub przeniesienia na Zamawiającego niewyłącznego uprawnienia licencyjnego zgodnego z zasadami licencjonowania określonymi przez producenta.

Kody CPV

* 48820000-2 Serwery
* 30233000-1 Urządzenie do przechowywania i odczytu danych
* 35120000-1 Systemy i urządzenia nadzoru i bezpieczeństwa
* 32420000-3 Urządzenie sieciowe
* 31682530-4 Awaryjne urządzenia energetyczne
* 48000000-8 Pakiety oprogramowania i systemy informatyczne
* 48422000-2 Zestawy pakietów oprogramowania
* 48600000-4 Pakiety oprogramowania dla baz danych i operacyjne
* 48900000-7 Różne pakiety oprogramowania i systemy komputerowe
* 72263000-6 Usługi wdrażania oprogramowania

# Część 2. Dostawa sprzętu i oprogramowania z usługami wdrożenia dla Gminnego Ośrodka Pomocy Społecznej w Zamościu

## Zestawienie rzeczowo - ilościowe

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | Przedmiot dostawy | Ilość | Miejsce dostawy |
|  | Zakup urządzenia UTM z licencją na 1 rok | 1 | Gminny Ośrodek Pomocy Społecznej w Zamościu |
|  | Przedłużenie licencji na UTM | 1 | Gminny Ośrodek Pomocy Społecznej w Zamościu |
|  | Zakup redundantnego switcha zarządzalnego | 1 | Gminny Ośrodek Pomocy Społecznej w Zamościu |
|  | Zakup redundantnego serwera fizycznego z systemem operacyjnym | 1 | Gminny Ośrodek Pomocy Społecznej w Zamościu |
|  | Licencja dostępu klienta usług pulpitu zdalnego | 5 | Gminny Ośrodek Pomocy Społecznej w Zamościu |
|  | Licencja na serwerowy system operacyjny | 1 | Gminny Ośrodek Pomocy Społecznej w Zamościu |
|  | Licencje dostępowe do serwerowego systemu operacyjnego | 32 | Gminny Ośrodek Pomocy Społecznej w Zamościu |
|  | Zakup licencji oprogramowania do kompleksowej ochrony antywirusowej stacji roboczych i serwera | 33 | Gminny Ośrodek Pomocy Społecznej w Zamościu |
|  | Zakup oprogramowania do monitorowania sieci LAN i inwentaryzacji zasobów | 32 | Gminny Ośrodek Pomocy Społecznej w Zamościu |
|  | Zakup UPS typu rack | 1 | Gminny Ośrodek Pomocy Społecznej w Zamościu |
|  | Usługi konfiguracji i wdrożenia zabezpieczeń | 1 | Gminny Ośrodek Pomocy Społecznej w Zamościu |
|  | Zakup redundantnego serwera NAS typu rack, 8 dysków | 2 | Gminny Ośrodek Pomocy Społecznej w Zamościu |
|  | Zakup dysków USB na potrzeby backupu | 5 | Gminny Ośrodek Pomocy Społecznej w Zamościu |
|  | Zakup UPS stanowiskowych | 20 | Gminny Ośrodek Pomocy Społecznej w Zamościu |

## Zakup urządzenia UTM z licencją na 1 rok

|  |  |
| --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** |
| Wymagania ogólne | Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza.  System realizujący funkcję firewall musi dawać możliwość pracy w jednym z trzech trybów: routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.  System musi wspierać IPv4 oraz IPv6 w zakresie:  • Firewall.  • Ochrony w warstwie aplikacji.  • Protokołów routingu dynamicznego. |
| Redundancja, monitoring i wykrywanie awarii | * + - 1. Dla funkcji: 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.  1. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 2. Monitoring stanu realizowanych połączeń VPN. |
| Interfejsy, przestrzeń dyskowa | * + - 1. System realizujący funkcję firewall musi dysponować minimum 7 portami Gigabit Ethernet RJ-45.       2. System firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.       3. W ramach systemu firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q. |
| Wydajność | 1. W zakresie frewall’a obsługa nie mniej niż 1,4 mln jednoczesnych połączeń oraz 30 tys. nowych połączeń na sekundę. 2. Przepustowość stateful firewall: nie mniej niż 10 Gbps dla pakietów 512 B. 3. Przepustowość firewall z włączoną funkcją kontroli aplikacji: nie mniej niż 1.7 Gbps. 4. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.3 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, kontrola aplikacji, antywirus - minimum 750 Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps. |
| Funkcje systemu bezpieczeństwa | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:  Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.  Kontrola Aplikacji.  Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.  Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.  Ochrona przed atakami - Intrusion Prevention System.  Kontrola stron WWW.  Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.  Zarządzanie pasmem (QoS, Traffic shaping).  Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).  Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.  Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.  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 | Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.  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.   W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.  Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP, nazwy domenowe, hashe złośliwych plików. |
| 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.  1. 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 upoważniająca do korzystania z usługi typu Sandbox w chmurze. 5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. |
| Ochrona przed atakami | 1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 4. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 5. 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. 6. 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. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 3. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 4. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. |
| Kontrola WWW | 1. Moduł kontroli WWW musi korzystać z bazy 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.  1. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 2. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. 3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. |
| Zarządzanie | 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. |
| Logowanie | 1. 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. 2. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 3. Musi istnieć możliwość logowania do serwera SYSLOG. |
| Licencje | Z urządzeniem należy dostarczyć licencje upoważniające do korzystania na urządzenie z aktualnych baz funkcji ochronnych producenta i serwisów przez okres 12 miesięcy w zakresie:  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. |
| Gwarancja | Co najmniej pięcioletnia gwarancja producenta. warunki świadczenia serwisu gwarancyjnego:   * usługi serwisu gwarancyjnego w miejscu instalacji urządzenia, * czas reakcji serwisu - do końca następnego dnia roboczego. |

## Przedłużenie licencji na UTM

|  |  |
| --- | --- |
| **Obszar wymagań** | **Wymagania** |
| Przedmiot zamówienia | Przedmiotem zamówienia jest przedłużenie licencji na funkcje bezpieczeństwa, o której mowa w poz. 1.1. na okres następujący po upływie ważności tej licencji do 08.04.2026 r. |

## Zakup redundantnego switcha zarządzalnego

|  |  |
| --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** |
| Typ urządzenia | Przełącznik zarządzalny warstwy L2 |
| Obudowa | Obudowa do montażu w szafie rack, maksymalnie 1U |
| Porty | Co najmniej:  48 x Base-T 1Gb/s 10/100/1000 Mbps PoE  4 x SFP+ 10Gb/s |
| Zarządzanie | Web GUI |
| Wydajność | Przepustowość co najmniej 40 Gbps  Rozmiar tablicy MAC co najmniej 8000 adresów  Maksymalna ilość VLAN co najmniej 64 |
| Standardy komunikacyjne | IEEE 802.3, IEEE 802.3ab, IEEE 802.3u, IEEE 802.3x |
| Funkcje | Pełny dupleks  Protokół drzewa rozpinającego  Agregator połączenia  Podpora kontroli przepływu  Obsługa sieci VLAN |
| Wymagane wyposażenie | Elementy montażowe do zamontowania w szafie  Kabel zasilający |
| Gwarancja | Co najmniej 3 lata gwarancji producenta |

## Zakup redundantnego serwera fizycznego z systemem operacyjnym

|  |  |
| --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** |
| Obudowa | Typu rack o wysokości maksymalnie 1U z możliwością instalacji do 8 dysków 2.5" Hot-Plug, z kompletem szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. |
| Procesor | Jeden procesor 32-rdzeniowy klasy x86 dedykowany do pracy z oferowanym serwerem, uzyskujący wynik co najmniej 55 000 punktów w teście PassMark - CPU Mark według wyników procesorów publikowanych na stronie http://www.cpubenchmark.net 30 dni przed terminem składania ofert lub później.  Do oferty należy załączyć wydruk z ww. strony, dopuszcza się wydruk w języku angielskim. |
| Pamięć RAM | Zainstalowane co najmniej 64 GB DDR4. |
| Grafika | Zintegrowana karta graficzna |
| Sieć | Wbudowane co najmniej 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT. |
| Dyski twarde | Możliwość instalacji dysków SATA, SAS, SSD.  Zainstalowane:1 dysk Hot-Plug SSD z interfejsem SATA o pojemności co najmniej 480GB,  2 dyski Hot-Plug SSD z interfejsem SAS o pojemności co najmniej 960 TB każdy. |
| Kontrolery dyskowe | Sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów RAID: 0, 1, 10 |
| Porty | Co najmniej 2 zewnętrzne porty USB 3.x.  Co najmniej 1 port VGA. |
| Zasilanie | Redundantne zasilacze hotplug o mocy nie większej niż 750W każdy. |
| Zarządzanie | Dedykowany moduł zdalnego zarządzania, diagnostyki i monitorowania pracy serwera, niezależny od systemu operacyjnego, posiadający dedykowany port GbE. |
| Bezpieczeństwo, diagnostyka | * Blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. * Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. * Moduł TPM 2.0 * Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy |
| System operacyjny | Zainstalowany na serwerze system operacyjny, kompatybilny z oferowanym serwerem, spełniający nw. wymagania minimalne:   1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 3. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 4. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 6. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 7. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 8. Wbudowane wsparcie instalacji i pracy na wolumenach, które:    1. pozwalają na zmianę rozmiaru w czasie pracy systemu,    2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,    3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,    4. umożliwiają zdefiniowanie list kontroli dostępu (ACL). 9. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 10. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 11. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 12. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 13. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 14. Dostępne dwa rodzaje graficznego interfejsu użytkownika:     1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,     2. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 15. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 16. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 17. Mechanizmy logowania w oparciu o:     1. login i hasło,     2. karty z certyfikatami (smartcard),     3. wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 18. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych. 19. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 20. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 21. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 22. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 23. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 24. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:     1. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,     2. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:        1. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,        2. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,        3. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.        4. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1 i wyższych.     3. Zdalna dystrybucja oprogramowania na stacje robocze.     4. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej.     5. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:        1. dystrybucję certyfikatów poprzez http,        2. konsolidację CA dla wielu lasów domeny,        3. automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,        4. automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.     6. Szyfrowanie plików i folderów.     7. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).     8. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.     9. Serwis udostępniania stron WWW.     10. Wsparcie dla protokołu IP w wersji 6 (IPv6),     11. Wsparcie dla algorytmów Suite B (RFC 4869),     12. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,     13. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:         1. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,         2. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.         3. Obsługi 4-KB sektorów dysków         4. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra         5. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.         6. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) 25. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 26. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 27. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 28. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 29. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. 30. Zorganizowany system szkoleń i dostępne materiały edukacyjne w języku polskim.   Zaoferowana wraz z serwerem licencja na system operacyjny:   1. musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta i pozwalała na legalne używanie na oferowanym serwerze, 2. musi obejmować najnowszą wersję systemu dostępną na dzień składania oferty, 3. musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie instancji wirtualnej tego serwerowego systemu operacyjnego, 4. musi umożliwiać dostęp dla 25 użytkowników.   Do oferty należy załączyć potwierdzenie kompatybilności serwera z oferowanym systemem operacyjnym (wydruk ze strony producenta systemu operacyjnego, dopuszcza się wydruk w języku angielskim). |
| Warunki gwarancyjne | Co najmniej pięcioletnia gwarancja producenta, obejmująca wszystkie komponenty urządzenia wchodzące w skład oferowanej konfiguracji.  Usługi serwisu gwarancyjnego muszą być realizowane w miejscu instalacji urządzenia. Czas reakcji serwisu - do końca następnego dnia roboczego. W przypadku awarii dysk twardy pozostaje u zamawiającego.  Możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta lub dedykowany portal techniczny producenta.  W czasie obowiązywania gwarancji na sprzęt, możliwość weryfikacji - na podstawie numeru seryjnego urządzenia - czasu obowiązywania i typ udzielonej gwarancji. Usługa realizowana przez portal lub infolinię producenta. |

## Licencja dostępu klienta usług pulpitu zdalnego

|  |  |
| --- | --- |
| **Obszar wymagań** | **Wymagania** |
| Przedmiot zamówienia | Przedmiotem zamówienia jest dostawa licencji dostępu klienta usług pulpitu zdalnego (uprawniających do korzystania ze zdalnego dostępu do środowiska pracy serwera) serwerowego systemu operacyjnego zainstalowanego na serwerze będącym przedmiotem dostawy dla 5 użytkowników. |

## Licencja na serwerowy system operacyjny

|  |  |
| --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** |
| Funkcjonalność | 1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 3. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 4. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 6. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 7. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 8. Wbudowane wsparcie instalacji i pracy na wolumenach, które:    1. pozwalają na zmianę rozmiaru w czasie pracy systemu,    2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,    3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,    4. umożliwiają zdefiniowanie list kontroli dostępu (ACL). 9. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 10. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 11. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 12. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 13. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 14. Dostępne dwa rodzaje graficznego interfejsu użytkownika:     1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,     2. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 15. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 16. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 17. Mechanizmy logowania w oparciu o:     1. login i hasło,     2. karty z certyfikatami (smartcard),     3. wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 18. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych. 19. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 20. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 21. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 22. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 23. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 24. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:     1. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,     2. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:        1. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,        2. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,        3. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.        4. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1 i wyższych.     3. Zdalna dystrybucja oprogramowania na stacje robocze.     4. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej.     5. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:        1. dystrybucję certyfikatów poprzez http,        2. konsolidację CA dla wielu lasów domeny,        3. automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,        4. automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.     6. Szyfrowanie plików i folderów.     7. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).     8. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.     9. Serwis udostępniania stron WWW.     10. Wsparcie dla protokołu IP w wersji 6 (IPv6),     11. Wsparcie dla algorytmów Suite B (RFC 4869),     12. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,     13. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:         1. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,         2. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.         3. Obsługi 4-KB sektorów dysków         4. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra         5. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.         6. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) 25. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 26. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 27. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 28. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 29. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. 30. Zorganizowany system szkoleń i dostępne materiały edukacyjne w języku polskim. |
| Licencje | Zaoferowana licencja na system operacyjny:   1. musi obejmować najnowszą wersję systemu dostępną na dzień składania oferty, 2. musi uprawniać do zainstalowania serwerowego systemu operacyjnego na serwerze, który posiada 16 rdzeni procesorowych, 3. musi uprawniać do zainstalowania dwóch instancji wirtualnych serwerowego systemu operacyjnego w ww. środowisku fizycznym. |

## Licencje dostępowe do serwerowego systemu operacyjnego

|  |  |
| --- | --- |
| **Obszar wymagań** | **Wymagania** |
| Przedmiot zamówienia | Przedmiotem zamówienia jest dostawa licencji dostępowych dla 32 użytkowników umożliwiającej użytkownikom dostęp do serwerowego systemu operacyjnego zainstalowanego na serwerze będącym przedmiotem dostawy. |

## Zakup licencji oprogramowania do kompleksowej ochrony antywirusowej stacji roboczych i serwera

|  |  |
| --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** |
| Licencje | Dostarczone licencje muszą zapewniać ochronę 33 urządzeń (urządzenia końcowe i serwery) do dnia 8.04.2026 r..  Wymagane wsparcie producenta lub dystrybutora na okres równy okresowi licencjonowania, w tym:   * nielimitowany dostęp do poprawek i aktualizacji, * dostęp do nowych funkcji i funkcjonalności w obrębie modułów licencyjnych, * wsparcie telefoniczne i mailowe producenta w trybie 24 x 7.   Wsparcie techniczne do programu musi być świadczone w języku polskim przez producenta lub dystrybutora, autoryzowanego przez producenta rozwiązania. |
| Administracja zdalna w chmurze | * + - 1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.       2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.       3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.       4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.       5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.       6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.       7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.       8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.       9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.       10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.       11. 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.       12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej. |
| Ochrona stacji roboczych | 1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10 i 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 oraz podejrzanych 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 integrować się z Intel Threat Detection Technology. 11. 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). 12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 13. 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. 14. 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. 15. 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. 16. 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 programu pocztowego Microsoft Outlook. 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 140 kategorii i podkategorii. 6. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. 7. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum. |
| Ochrona serwera | 1. Rozwiązanie musi wspierać systemy Microsoft Windows Server. 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.   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. |
| Szyfrowanie | 1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10 i Microsoft Windows 11. 2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault). 3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia. 4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI. |
| Sandbox w chmurze | 1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. 2. Rozwiązanie musi wykorzystywać do działania chmurę producenta. 3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do 4. chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, 5. dokumenty oraz inne pliki typu .jar, .reg, .msi. 6. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta. 7. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek. 8. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania. 9. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów. 10. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy. 11. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione. 12. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych. 13. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo. 14. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem: czysty, podejrzany, bardzo podejrzany albo szkodliwy. 15. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum. 16. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki. 17. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia. |
| Moduł XDR | 1. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW. 2. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta. 3. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL. 4. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa. 5. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”. 6. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia. 7. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika. 8. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta. 9. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej. 10. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku. 11. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania. 12. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny. 13. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej. 14. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych. 15. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: 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) oraz wylistowanie zainstalowanego oprogramowania firm trzecich. 16. Konsola administracyjna musi mieć możliwość tagowania obiektów. 17. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell. |

## Zakup oprogramowania do monitorowania sieci LAN i inwentaryzacji zasobów

|  |  |
| --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** |
| Licencja | Wymagane dostarczenie licencji bezterminowej umożliwiającej nadzór nad siecią obejmującą 32 stanowisk roboczych  Licencja musi uprawniać korzystania ze wsparcia producenta polegającego na zapewnieniu możliwości bezpłatnego pobierania aktualizacji i korzystania z pomocy technicznej producenta przez okres co najmniej 12 miesięcy.  Licencja musi uprawniać do skorzystania w okresie wsparcia technicznego ze szkolenia zdalnego dla administratora (szkolenie realizowane przez producenta lub jego przedstawiciela). |
| Wymagania ogólne | Oprogramowanie musi posiadać budowę modułową, składającą się z serwera zarządzającego, zdalnych konsoli oraz Agentów.  Komunikacja pomiędzy Serwerem a Agentami i Konsolami musi być realizowana przy użyciu szyfrowanego protokołu TLS 1.2. Program musi umożliwiać zmianę portu komunikacyjnego wykorzystywanego przez konsolę zarządzającą.  Moduły oprogramowania muszą umożliwiać monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych.  Program powinien wykorzystywać darmowy silnik bazy danych z kodem źródłowym dostępnym na licencji open-source (PostgreSQL w wersji 12).  Dane, które dotyczą działań pracownika na komputerze, a więc: historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., powinny być odseparowane od danych stricte technicznych tj. informacji o stacji roboczej. Powinny być również grupowane w osobnym, dedykowanym oknie. Powyższe musi pozwalać na, zgodne z RODO, usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej. Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, musi być objęty kontrolą na poziomie wybranych administratorów – w programie musi istnieć możliwość nadawania kontom administracyjnym różnych poziomów dostępu oraz uprawnień zarówno do funkcji programu, grup urządzeń, jak i użytkowników. Główny administrator powinien mieć możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną np. może wyłączyć możliwość zdalnej deinstalacji agenta, ograniczyć dostęp do opcji programu oraz logów działań innych administratorów. Działania administratorów powinny być logowane, co oznacza, że program powinien posiadać dziennik z listą czynności wykonanych przez administratorów, którzy zmodyfikowali obiekty znajdujące się w systemie w tym m.in. logowanie dostępu do opcji programu, logowanie dostępu do informacji o aktywności użytkownika, logowanie poleceń deinstalacji agenta. Działania administratorów mogą być automatycznie eksportowane do zewnętrznego kolektora Syslog.  Lista kont użytkowników, w tym administratorów, powinna być synchronizowana z Active Directory, również przez szyfrowane połączenie LDAPS. Program powinien umożliwiać konfigurację polityki haseł do lokalnych kont użytkowników konsoli. Polityki powinny pozwalać na określenie: minimalnej długości hasła, liter, cyfr, znaków specjalnych oraz automatycznie wymusza dostosowanie bieżących haseł do obowiązujących zasad.  Program powinien zawierać mechanizmy uwierzytelniania logowań administratorów do konsoli z wykorzystaniem weryfikacji dwuskładnikowej (MFA). Kod autoryzacyjny może być wysyłany za pomocą e-mail i/lub SMS. W weryfikacji MFA powinna istnieć możliwość skonfigurowania okresu, po którym należy ponownie zautoryzować logowanie. W przypadku awarii autoryzacja logowania może być pominięta tylko w lokalnej konsoli serwera. |
| Inwentaryzacja | W zakresie inwentaryzacji program musi automatycznie gromadzić informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz:   * + prezentować szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.,   + umożliwiać odczyt parametrów S.M.A.R.T. dysków twardych, dysków SSD, w tym NVMe,   + obejmować m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade,   + informować o zainstalowanych aplikacjach oraz aktualizacjach Windows, co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji,   + zbierać informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.,   + posiadać możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera,   + umożliwiać odczytanie numeru seryjnego (klucze licencyjne),   + umożliwiać automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych,   + umożliwiać przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.,   + umożliwiać utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu),   + umożliwiać wymianę plików do i ze stacją roboczą poprzez funkcję menedżera plików, działania administratorów wykonywane w tej funkcji muszą być logowane.   + Moduł inwentaryzacji zasobów powinien umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania w zakresie:   + przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji,   + przydzielania dostępu administratorów do zasobów na podstawie praw do oddziałów,   + tworzenia powiązań między zasobami a urządzeniami,   + tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych,   + wskazania osób uprawnionych do użycia zasobów poprzez rozbudowane mechanizmy,   + definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz,   + określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów,   + określenia atrybutów dodatkowych tylko dla wybranych typów zasobów,   + masową edycję atrybutów zasobów,   + definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie,   + importu danych z zewnętrznego źródła (.CSV),   + przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp.,   + tworzenia powiązań między zasobami a dokumentami w relacji 1:N,   + oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp.,   + ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności,   + generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania,   + przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji,   + konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca,   + konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca,   + archiwizacji i porównywania audytów zasobów,   + tworzenia kodów kreskowych dla zasobów,   + drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy,   + inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet,   + możliwość zmiany portu komunikacyjnego wykorzystywanego przez aplikację mobilną dla systemu Android,   + inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline),   + definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja”).   Inwentaryzacja oprogramowania powinna zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:   * + informacje o aplikacjach używanych w organizacji,   + tworzenie własnych wzorców aplikacji,   + tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.,   + informacje o komputerach, na których aplikacja została wykryta,   + zarządzanie posiadanymi licencjami,   + wskazywanie osób odpowiedzialnych za licencję,   + wskazanie użytkowników licencji,   + tworzenie powiązań między licencjami a dokumentami w relacji 1:N,   + rozbudowane i konfigurowalne scenariusze zarządzania licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu,   + łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych,   + zarządzanie posiadanymi licencjami: raport zgodności licencji,   + możliwość przypisania do programów numerów seryjnych, wartości itp. |
| Użytkownicy | Moduł powinien umożliwiać monitorowania co najmniej:   * + faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy),   + procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach,   + rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność,   + informacji o edytowanych przez użytkownika dokumentach,   + historii pracy (cykliczne zrzuty ekranowe),   + listy odwiedzanych stron WWW (tytuły, adresy, liczba i czas wizyt),   + transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika),   + wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program ma możliwość monitorowania kosztów wydruków,   + nagłówków przesyłanej w aplikacjach klienckich poczty e-mail.   Moduł ponadto musi zapewniać możliwość:   * + wykrywania podejrzanej aktywności przez popularne „jigglery”, mającej na celu symulowanie faktycznej pracy,   + zdefiniowania czasu, gdy wykrywana będzie symulowana aktywność wyłącznie przez ruch myszą bez kliknięcia lub wprowadzanie tego samego znaku z klawiatury.   + wyszczególnienia podejrzanej aktywności w raportach,   + wygenerowania alarmu i wykonania akcji po wykryciu podejrzanej aktywności,   + automatycznego włączenia zapisywania zrzutów ekranowych po wykryciu podejrzanej aktywności,   + blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. \*.domena.pl); reguły w postaci listy domen muszą być tworzone dla użytkownika lub grupy użytkowników i być kopiowane lub współdzielone pomiędzy grupami lub kontami,   + integracji list stron w formie plików .TXT z dowolnego adresu zewnętrznego np. CERT,   + skorzystania z wbudowanej listy stron sklasyfikowanych jako zagrożenia,   + automatycznego odświeżania list stron zintegrowanych z adresów zewnętrznych,   + blokowania ruchu na wskazanych portach TCP/IP,   + blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem,   + prowadzenia rejestru naruszeń blokad,   + wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia, naruszy skonfigurowane blokady,   + przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika),   + definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone. |
| Helpdesk - pomoc techniczna | W zakresie helpdesk – pomocy technicznej system musi posiadać następującą funkcjonalność:   * + zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej,   + rozmowy również między „zwykłymi” użytkownikami,   + przesyłanie plików między rozmówcami w trybie on-line,   + tworzenie pokojów tematycznych, rozmów grupowych,   + oznaczanie kontaktów jako „ulubionych” na liście kontaktów,   + uruchomienie z poziomu ikony dostępowej Agenta oraz bezpośrednio w interfejsie WWW heldpesku,   + może być wyświetlany w trybie jasnym lub ciemnym,   Moduł pomocy zdalnej musi umożliwiać również:   * + pobieranie listy użytkowników z Active Directory,   + wyświetlanie w systemie zgłoszeń wizytówki użytkownika wraz z jego numerem telefonu, adresem e-mail oraz informacją o przełożonym,   + zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont,   + zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez rozbudowany system zarządzania regułami widoczności zgłoszeń,   + zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii zgłoszeń,   + zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii artykułów bazy wiedzy,   + tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO,   + automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników,   + definiowanie ścieżek akceptacji zgłoszeń – procesu, w którym użytkownik uzyskuje akceptację na realizację zgłoszenia od wyznaczonych osób w organizacji,   + przypisywanie ścieżek akceptacji zgłoszeń do określonych kategorii,   + procesowanie zgłoszeń użytkowników z wiadomości e-mail,   + eksportowania listy zgłoszeń do plików CSV i XLSX,   + integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0,   + tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń,   + wykonywanie operacji na wielu zgłoszeniach równocześnie,   + dołączanie załączników do zgłoszeń,   + rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy,   + szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników,   + wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia,   + zrzuty ekranowe (podgląd pulpitu),   + zdalną modyfikację rejestrów,   + dystrybucję oprogramowania przez Agentów,   + definiowanie aplikacji dozwolonych do samodzielnej instalacji przez użytkowników z pakietów MSI w postaci Kiosku z Aplikacjami,   + przypisywanie dostępnych w Kiosku instalatorów do grup użytkowników,   + dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI),   + zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku,   + możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu,   + planowanie nieobecności pracowników helpdesk,   + obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem,   + generowanie raportów obsługi helpdesk,   + zdalne wykonywanie poleceń poprzez Agentów (np. utworzenie / edycja konta lokalnego użytkownika systemu). |
| Ochrona danych | Moduł powinien posiadać następujące funkcjonalności w zakresie:   * + blokowania urządzeń i nośników danych; program powinien mieć możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny,   + blokowania urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek,   + blokowania interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA,   + możliwość blokowania tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane,   + alarmowania o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych.   Funkcje wspierające bezpieczeństwo systemu:   * + integracja i zarządzanie ustawieniami Windows Defender,   + monitorowanie stanu szyfrowania dysków BitLocker,   + zdalne szyfrowanie dysków za pomocą BitLocker,   + zapisywanie klucza odzyskiwania do pliku oraz jako zasób w bazie danych programu,   + integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu,   + odczytanie informacji o aktywnym oprogramowaniu antywirusowym firm trzecich, innym niż Windows Defender,   + monitorowanie stanu modułu TPM.   W zakresie zarządzanie prawami dostępu do urządzeń:   * + definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików,   + autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive’ów, dysków itp. - urządzenia prywatne są blokowane,   + całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników,   + centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci,   + możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane.   + Audyt operacji na plikach na urządzeniach przenośnych:   + zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych,   + podłączenie/odłączenie urządzenia przenośnego. |
| Monitorowanie infrastruktury | Moduł powinien posiadać następujące funkcjonalności:   * + wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping,   + wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU),   + wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci,   + wizualizacji urządzeń na mapach z funkcją siatki umożliwiającej korygowanie pozycji ikon na mapie do najbliższej linii siatki,   + wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła,   + wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku,   + wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach o dowolnym rozmiarze i kolorze,   + wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie,   + wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny,   + zablokowania mapy urządzeń przed przypadkową edycją,   + serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów,   + serwerów pocztowych:   + monitorowanie czasu logowania do serwisu odbierającego oraz czas wysyłania poczty,   + monitorowanie stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem),   + możliwość wykonywania operacji testowych,   + możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa,   + monitorowania serwerów WWW i adresów URL,   + cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS,   + obsługi szyfrowania SSL/TLS w powiadomieniach e-mail,   + obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID,   + obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych,   + monitoringu routerów i przełączników według:   + zmian stanu interfejsów sieciowych,   + ruchu sieciowego,   + podłączonych stacji roboczych – graficzna prezentacja panelu switcha,   + ruchu generowanego przez podłączone do portów stacje robocze,   + serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie. |

## Zakup UPS typu rack

|  |  |
| --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** |
| Typ urządzenia | Zasilacz awaryjny w obudowie tower z możliwością montażu w szafie rack, zajmujący maksymalnie 2U |
| Moc | Co najmniej 2700 W, moc pozorna co najmniej 3000 VA |
| Napięcie wejściowe | 230 V |
| Częstotliwość | 50 Hz |
| Topologia | Online |
| Typ przebiegu | Sinusoida |
| Czas podtrzymania | Co najmniej 8 min. przy obciążeniu 50 % |
| Gniazda | Co najmniej 9 gniazd wyjściowych z podtrzymaniem / ochroną |
| Komunikacja | Karta komunikacyjna Ethernet |
| Zabezpieczenia | Przeciwprzepięciowe, przeciwzwarciowe, przeciwprzeciążeniowe |
| Sygnalizacja | Wyświetlacz LCD lub diody LED, alarm dźwiękowy |
| Gwarancja | Co najmniej 24 miesiące. |

## Usługi konfiguracji i wdrożenia zabezpieczeń

Wykonawca jest zobowiązany do:

1. Konfiguracji urządzenia UTM będącego przedmiotem dostawy, w tym:
   1. Skonfigurowania sieci LAN/WAN: ustawienie 5 połączeń VPN (Site-to-Site oraz Client-to-Site) zgodnie z wytycznymi Zamawiającego.
   2. Konfiguracji 3 VLAN-ów:
      1. VLAN dla dostępu do Internetu,
      2. VLAN dla sieci LAN z możliwością opcjonalnego dostępu do Internetu,
      3. VLAN dla DHCP.
   3. Wdrożenia kontroli antywirusowej:
      1. Skonfigurowania silnika antywirusowego umożliwiającego skanowanie ruchu w obu kierunkach, w tym dla protokołów działających na niestandardowych portach.
      2. Umożliwienia skanowania archiwów, takich jak ZIP i RAR.
   4. Wdrożenia ochrony przed atakami:
      1. Konfiguracji systemu IPS opartego na analizie sygnaturowej i anomalii w protokołach sieciowych.
      2. Zabezpieczenia aplikacji pracujących na niestandardowych portach.
      3. Aktualizacji bazy sygnatur.
   5. Konfiguracji ochrony przed malware i kontrolą poczty:
      1. Uruchomienia ochrony przed malware dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
      2. Uruchomienia modułu antyspamowego dla poczty (SMTP, POP3, IMAP).
   6. Wdrożenia kontroli aplikacji i WWW:
      1. Skonfigurowania kontroli aplikacji z wykorzystaniem bazy sygnatur.
      2. Ustawienia filtrów WWW na podstawie kategorii bezpieczeństwa (w tym malware, phishing, spam).
2. Konfiguracji opensourcowego serwera logów:
   1. Instalacji i konfiguracji serwera logów w serwerowym systemie operacyjnym dostarczanym wraz z serwerem będącym przedmiotem zamówienia:
   2. Umożliwienia rejestrowania logów systemowych oraz dziennika zdarzeń systemu operacyjnego.
   3. Monitorowania logów w czasie rzeczywistym i centralnego przechowywania powiadomień o błędach.
   4. Zapewnienia dostępu do logów przez przeglądarkę internetową:
   5. Konfiguracji kont administracyjnych i użytkowników z różnymi poziomami dostępu.
   6. Wyświetlania logów w czytelnej, graficznej formie, z kolorowaniem według rodzaju i klasyfikacji komunikatów.
   7. Wdrożenia zaawansowanych funkcji logowania:
      1. Filtrowania zdarzeń po adresie IP i słowach kluczowych.
      2. Automatycznego archiwizowania plików logów w formacie ZIP z opcją szyfrowania.
      3. Wyświetlania statystyk i wykresów dotyczących ilości otrzymanych komunikatów.
3. Wdrożenia usług katalogowych w oparciu o serwerowy system operacyjny, w tym:
   1. Instalacji systemu operacyjnego serwera i przygotowania go jako kontrolera domeny.
   2. Utworzenia domeny i skonfigurowania struktury jednostek organizacyjnych (OU) zgodnie z wymaganiami urzędu.
   3. Utworzenia i konfiguracji użytkowników oraz grup:
      1. Dodania kont użytkowników i grup w domenie, uwzględniając podział ról i przypisanie odpowiednich uprawnień.
      2. Skonfigurowania zasad bezpieczeństwa haseł oraz reguł dotyczących uwierzytelniania użytkowników.
   4. Konfiguracji polityk grupowych (GPO): opracowania polityk grupowych do centralnego zarządzania stacjami roboczymi i użytkownikami, w tym zasad bezpieczeństwa oraz dostępu do zasobów sieciowych.
   5. Integracji z istniejącą infrastrukturą sieciową:
      1. Konfiguracji systemu DNS dla poprawnej pracy domeny.
      2. Integracji systemu katalogowego z istniejącymi usługami sieciowymi i aplikacjami.
   6. Przeprowadzenia testów działania systemu katalogowego, w tym logowania, funkcjonowania polityk grupowych oraz dostępu do zasobów.
4. Opracowania dokumentacji i przeszkolenia administratorów:
   1. Dostarczenia pełnej dokumentacji z zakresu konfiguracji UTM oraz serwera logów.
   2. Dostarczenia pełnej dokumentacji dotyczącej konfiguracji systemu oraz polityk zarządzania.
   3. Przeszkolenia administratorów urzędu w zakresie zarządzania urządzeniem UTM oraz systemem logów.
   4. Przeprowadzenia szkolenia z zakresu obsługi systemu katalogowego, tworzenia użytkowników i grup, zarządzania politykami grupowymi oraz zasad bezpieczeństwa.
5. Usługi wdrożenia muszą zapewniać zgodność z zasadami bezpieczeństwa danych, w tym RODO, oraz z dobrymi praktykami w zakresie ochrony infrastruktury sieciowej.

## Zakup redundantnego serwera NAS typu rack

|  |  |
| --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** |
| Budowa | Obudowa do montażu w szafie rack, wymagane wyposażenie w szyny do szafy rack  Redundantne wentylatory |
| Procesor | Ośmiordzeniowy procesor 64-bitowy, uzyskujący wynik co najmniej 8 500 punktów w teście PassMark - CPU Mark według wyników dostępnych na stronie http://www.cpubenchmark.net 30 dni przed terminem składania ofert lub później.  Do oferty należy załączyć wydruk z ww. strony, dopuszcza się wydruk w języku angielskim. |
| Pamięć RAM | Zainstalowane co najmniej 32 GB pamięci RAM, możliwość rozszerzenia do co najmniej 64 GB. |
| Obsługa dysków | Ilość kieszeni dysków: co najmniej 8 (możliwość rozbudowy do 12 dysków z wykorzystaniem jednostki rozszerzającej lub równoważnie obudowa na 12 dysków).  Obsługiwane typy dysków: 3,5” SATA HDD, 2.5" SATA HDD, 2,5” SATA SSD. |
| Zamontowane dyski | Zamontowane co najmniej 8 dysków o pojemności co najmniej 8 TB każdy, o prędkości interfejsu co najmniej 6Gbps i deklarowanym średnim czasem bezawaryjnej pracy co najmniej 1,2 mln godzin.  Oferowane dyski muszą znajdować się na liście kompatybilności producenta urządzenia dyskowego NAS. |
| RAID | Obsługa RAID co najmniej: Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6 i RAID 10. |
| Oprogramowanie | Serwer musi zostać dostarczony wraz z zainstalowanym oprogramowaniem, wymaganym do jego prawidłowego działania do których jest przeznaczony, oprogramowanie musi być w pełni zintegrowane z oferowanym serwerem NAS  Możliwość instalacji oprogramowania do kopii zapasowej za pomocą interfejsu GUI w/w urządzenia. |
| Porty | Co najmniej 2 porty RJ-45 obsługujące 1GbE  Co najmniej 2 porty USB 3.x |
| Zasilanie | Wbudowane redundantne zasilacze |
| Gwarancja | Gwarancja producenta co najmniej 36 miesięcy. |

## Zakup dysków USB na potrzeby backupu

|  |  |
| --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** |
| Typ | Zewnętrzny, przenośny dysk SSD |
| Pojemność | Co najmniej 2 TB |
| Szybkość odczytu | 2000 MB/s |
| Szybkość zapisu | 2000 MB/s |
| Prędkość interfejsu | 20 Gbit/s |
| Inne wymagania | Odporny na wibracje i upadki |

## Zakup UPS stanowiskowych

|  |  |
| --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** |
| Typ urządzenia | Zasilacz awaryjny w obudowie typu desktop |
| Moc | Co najmniej 400W, moc pozorna co najmniej 650 VA |
| Napięcie wejściowe | 230 V |
| Częstotliwość | 50 Hz |
| Czas przełączania | Maksymalnie 5ms |
| Czas podtrzymania | 9 min. dla obciążenia 50% lub dłużej  2,4 min. dla obciążenia 100% lub dłużej |
| Gniazda | Co najmniej 3 gniazda wyjściowe |
| Sygnalizacja | Sygnalizacja optyczno-akustyczna |
| Inne wymagania | Filtracja napięcia wyjściowego - filtr przeciwzakłóceniowy RFI/EMI, tłumik warystorowy  Zabezpieczenie przeciążeniowe - bezpiecznik topikowy  Zabezpieczenie przeciwzwarciowe akumulatora - elektroniczne  akumulatora – elektroniczne  Zimny start |
| Gwarancja | Gwarancja producenta co najmniej 24 miesiące. |