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 1. Dostawa sprzętu i oprogramowania z usługami wdrożenia dla Urzędu Gminy Zamość

Ogólne warunki realizacji zamówienia

1. Przedmiot zamówienia obejmuje dostawy do siedziby Zamawiającego, tj. Urzędu Gminy Zamość 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 1. Dostawa sprzętu i oprogramowania z usługami wdrożenia dla Urzędu Gminy Zamość

## Zestawienie rzeczowo - ilościowe

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | Przedmiot dostawy | Ilość | Miejsce dostawy |
|  | Odnowienie licencji posiadanego urządzenia UTM | 1 | Urząd Gminy Zamość |
|  | Przedłużenie licencji na UTM | 1 | Urząd Gminy Zamość |
|  | Zakup redundantnego serwera fizycznego z systemem operacyjnym | 1 | Urząd Gminy Zamość |
|  | Zakup licencji oprogramowania do kompleksowej ochrony antywirusowej stacji roboczych | 70 | Urząd Gminy Zamość |
|  | Zakup oprogramowania do monitorowania sieci LAN i inwentaryzacji zasobów | 70 | Urząd Gminy Zamość |
|  | Usługa konfiguracji i wdrożenia zabezpieczeń | 1 | Urząd Gminy Zamość |
|  | Zakup redundantnego serwera NAS typu rack | 1 | Urząd Gminy Zamość |
|  | Zakup dysków USB na potrzeby backupu | 10 | Urząd Gminy Zamość |

## Odnowienie licencji posiadanego urządzenia UTM

|  |  |
| --- | --- |
| **Obszar wymagań** | **Wymagania** |
| Przedmiot zamówienia | Przedmiotem zamówienia jest odnowienie licencji na funkcje bezpieczeństwa UTM Security Pack do urządzenia UTM Stormshield SN510 posiadanego przez Zamawiającego (licencja wygasa 19.04.2025 r.) na okres do 8.04.2026 r. |

Jako rozwiązanie równoważne Zamawiający dopuszcza dostawę nowego urządzenia UTM wraz z licencją spełniającego nw. wymagania minimalne:

|  |  |
| --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** |
| Obsługa sieci | Urządzenie musi 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. |
| 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 umożliwiać 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, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. 5. Administrator ma 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, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia. 6. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. 7. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall. 8. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł. 9. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos. 10. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego). 11. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe. |
| Intrusion prevention system (IPS) | 1. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. 2. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy. 3. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. 4. Administrator ma 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 nie blokując dostępu do tej strony po usunięciu zagrożenia. 6. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS. 7. Administrator 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 umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0. 9. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych. |
| Kształtowanie pasma (Traffic Shapping) | 1. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. 2. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP. 3. Urządzenie 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. |
| Ochrona antywirusowa | 1. Urządzenie ma umożliwiać 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 wykrycia infekcji. |
| Ochrona antyspam | 1. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). 2. Ochrona antyspam ma działać w oparciu o: białe/czarne listy, DNS RBL i skaner heurystyczny. 3. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia. 4. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin. |
| Wirtualne sieci prywatne (VPN) | 1. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). 2. Urządzenie ma wspierać co najmniej następujące typy sieci VPN: PPTP VPN, IPSec VPN i SSL VPN. 3. SSL VPN ma działać co najmniej w trybach tunelu i portalu. 4. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem. 5. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal) 6. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). 7. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf. 8. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based. |
| 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 ma mieć możliwość dodawania własnych kategorii URL. 4. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:    1. blokowanie dostępu do adresu URL,    2. zezwolenie na dostęp do adresu URL,    3. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. 5. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. 6. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych. 7. Filtr URL musi uwzględniać komunikację po protokole HTTPS. 8. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. 9. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane. 10. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch |
| Uwierzytelnianie | 1. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:    1. lokalną bazę użytkowników (wewnętrzny LDAP),    2. zewnętrzną bazę użytkowników (zewnętrzny LDAP),    3. usługę katalogową Microsoft Active Directory. 2. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP. 3. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły SSL, Radius i Kerberos. 4. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy. 5. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta. 6. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny. 7. Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS). 8. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP). 9. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH. |
| Administracja łączami do Internetu (ISP) | 1. Urządzenie ma umożliwiać 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 obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. 4. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover). 5. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza. 6. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów). 7. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP. |
| Routing (trasowanie) | 1. Urządzenie ma umożliwiać statyczne trasowanie pakietów. 2. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 3. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing). 4. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP. |
| Administracja urządzeniem | 1. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego. 2. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS. 3. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP. 4. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. 5. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. 6. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH) 7. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania. 8. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS. 9. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup. 10. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych. 11. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła. 12. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording). 13. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services). 14. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników. 15. Urządzenie ma umożliwiać zapisywanie logów na wbudowanym dysku. 16. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS). 17. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX. 18. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:     1. manualnego eksportu do pliku w dowolnym momencie czasu,     2. automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu 19. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora. 20. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika. 21. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego. |
| Raportowanie | 1. Urządzenie ma 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 ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego. 4. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów. 5. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu. 6. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV. 7. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta. 8. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3. 9. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH). |
| Pozostałe usługi i funkcje | 1. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP. 2. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej. 3. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay). 4. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6. 5. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny). 6. Urządzenie ma posiadać usługę DNS Proxy. 7. Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP). 8. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN. 9. Urządzenie musi mieć zaimplementowane Open API 10. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie. |
| Gwarancja i serwis | 1. Urządzenie ma być objęte 12-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencją dla wszystkich funkcji bezpieczeństwa. 2. W okresie obowiązywania gwarancji musi być zapewnione bezpłatne wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal. |
| Parametry sprzętowe | 1. Urządzenie ma być wyposażone w dysk SSD o pojemności co najmniej 200 GB. 2. Urządzenie musi być wyposażone w redundantne zasilanie z sygnalizacją pracy poszczególnych zasilaczy. 3. Liczba portów Ethernet 2,5Gbps – co najmniej 8 z możliwością rozszerzenia do 16. 4. Liczba portów światłowodowych 1Gbps – co najmniej 2 z możliwością rozszerzenia do 10. 5. Urządzenie ma pozwalać na instalację modułu rozszerzeń z poniższej listy:    1. Moduł z 8 interfejsami miedzianymi 2,5Gbps    2. Moduł z 4 interfejsami miedzianymi 10Gbps.    3. Moduł z 4 interfejsami światłowodowymi 1Gbps.    4. Moduł z 8 interfejsami światłowodowymi 1Gbps.    5. Moduł z 4 interfejsami światłowodowymi 10Gbps. 6. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta. 7. Urządzenie ma być wyposażone w min. 2, różniące się typem, porty konsolowe. Przynajmniej jeden port konsolowy ma być typu RJ45. 8. Przepustowość Firewall (1518 bajtów UDP) – minimum 10Gbps. 9. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 5Gbps. 10. Przepustowość filtrowania Antywirusowego – minimum 1.3 Gbps. 11. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 2.5Gbps. 12. Maksymalna liczba tuneli VPN IPSec – minimum 1000. 13. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 150. 14. Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 150. 15. Obsługa interfejsów 802.11q (VLAN) – minimum 256. 16. Liczba równoczesnych sesji – minimum 600 000 i nie mniej niż 30 000 nowych sesji/sekundę. 17. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive. 18. Urządzenie nie może ograniczać liczby użytkowników. 19. Liczba reguł filtrowania – minimum 16 384. 20. Liczba tras statycznego routingu – minimum 5 120. 21. Liczba tras dynamicznego routingu – minimum 10 000. 22. Możliwość instalacji w szafie RACK 19”, wysokość urządzenia 1U. 23. Urządzenie musi być wyposażone w moduł TPM. |

## 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 kolejnych 12 miesięcy. |

## 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 ośmiordzeniowy klasy x86 dedykowany do pracy z oferowanym serwerem, uzyskujący wynik co najmniej 22 642 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:  2 dyski Hot-Plug SSD z interfejsem SATA o pojemności co najmniej 480GB każdy,  2 dyski Hot-Plug SSD z interfejsem SAS o pojemności co najmniej 1,92 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. |

## Zakup licencji oprogramowania do kompleksowej ochrony antywirusowej stacji roboczych

|  |  |
| --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** |
|  | Zamawiający (Urząd Gminy Zamość) posiada licencję oprogramowania antywirusowego ESET PROTECT Entry Cloud z ważnością do dnia: 31.07.2025 dla 70 stanowisk.  Wykonawca dostarczy licencje subskrypcyjne, które zapewnią kontynuację ochronę 70 urządzeń (urządzenia końcowe i serwery) do 8 kwietnia 2026 r.  Jako rozwiązanie równoważne Zamawiający dopuszcza dostarczenie licencji na nowe rozwiązanie (oprogramowanie do kompleksowej ochrony antywirusowej stacji roboczych) o terminie ważności licencji jak powyżej, które musi spełniać wymagania określone w dalszych wierszach tabeli. |
| 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 wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.       7. 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.       8. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.       9. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.       10. 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.       11. 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/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 przxed 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. |
| Wsparcie | 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 dla oprogramowania musi być świadczone w języku polskim przez producenta lub dystrybutora, autoryzowanego przez producenta rozwiązania. |

## Zakup oprogramowania do monitorowania sieci LAN i inwentaryzacji zasobów

|  |  |
| --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** |
| Licencja | Wymagane dostarczenie licencji bezterminowych na 70 urządzeń końcowych, uprawniającej do korzystania ze wsparcia producenta do 8 kwietnia 2026 r. |
| Zarządzanie zasobami - sprzęt informatyczny | 1. Centralne zarządzanie wynikami skanowania sprzętu i oprogramowania. 2. Zdalne wykrywanie urządzeń w sieci za pomocą protokołów PING, ARP oraz SNMP. 3. Automatyczne wykrywanie adresów IP, MAC, DNS, Systemu Operacyjnego wraz z informacją o aktualizacji. 4. Automatyczne wykrywanie czy komputer jest członkiem domeny oraz do jakiej domeny lub grupy roboczej należy. 5. Odwzorowanie struktury organizacji w oparciu o Active Directory. 6. Jednostronna synchronizacja komputerów oraz drukarek z AD (Odwzorowanie wszystkich wprowadzonych zmian w rekordach Active Directory). 7. Automatyczne skanowanie całości lub wybranych grup Active Directory oraz sieci. 8. Grupowanie wyposażenia z podziałem na wydziały organizacyjne. 9. Inwentaryzacja dowolnych elementów wyposażenia (biurka, szafy, telefony, etc.). 10. Utworzenie własnych typów elementów wyposażenia. 11. Łączenie elementów wyposażenia w zestawy. 12. Przypisywanie zasobu do wielu zestawów. 13. Grupowanie, sortowanie i filtrowanie po dowolnie nadanych atrybutach. 14. Podpięcie dowolnych załączników, np. skany faktur, gwarancji oraz wszelkich innych plików. 15. Przypisywanie sprzętu do konkretnych osób. 16. Automatyczne wyznaczanie 'Głównego użytkownika' komputera. 17. Wiązanie wielu rekordów wyposażenia z użytkownikiem. 18. Przypisywanie sprzętu do dowolnej lokalizacji. 19. Definiowanie własnych, dowolnych atrybutów sprzętu. 20. Wydruk etykiet z kodami kreskowymi do inwentaryzacji wyposażenia. 21. Grupowa zmiana domeny/grupy roboczej zasobu. 22. Ułatwienie inwentaryzacji sprzętu (kody QR, zestawy, historia). 23. Automatyczne wykrywanie typu komputera (Desktop\Notebook\Serwer\Kontroler domeny) na podstawie wyników skanowania sprzętu. 24. Automatyczne uzupełnianie informacji o procesorze, liczbie rdzeni, ilości pamięci RAM, rozmiarze dysku, nazwie karty graficznej i rozdzielczości monitora w obiekcie zasobu po wykonaniu skanowania sprzętu. 25. Odczytywanie indeksów wydajności poszczególnych komponentów komputera: CPU, GPU, HDD, RAM. 26. Automatyczna aktualizacja nazwy komputera w przypadku jej zmiany. 27. Definiowanie statusów dla sprzętu. 28. Szczegółowa informacja na temat podzespołów sprzętu (procesor, bios, płyta główna, pamięć, dyski twarde, monitory, karty graficzne i muzyczne, etc.). 29. Odczyt informacji o module TPM. 30. Inwentaryzacja osprzętu komputerowego (monitory, drukarki, myszki, urządzenia sieciowe: Switch, Router, Access Point, Bridge, Modem, NAS, UPS, itd.). 31. Automatyczne wykrywanie lokalnych drukarek (USB) na podstawie wyników skanowania sprzętu. 32. Automatyczne wykrywanie i tworzenie monitorów (producent, numer seryjny, rozdzielczość, odczyt firmy, działu, osoby odpowiedzialnej, głównego użytkownika). 33. Określanie informacji o wykorzystywanej wirtualizacji. 34. Podgląd zestawów, do których należy zasób. 35. Cykliczne wykonywanie skanowania sprzętu z różnymi ustawieniami. 36. Automatyczne odczytywanie ServiceTag oraz modelu komputera (na podstawie wyników skanowania sprzętu). 37. Automatyczna aktualizacja adresów IP komputerów bez zainstalowanego agenta. 38. Określanie adresu interfejsu webowego urządzenia sieciowego. 39. Automatyczne tworzenie historii zmian sprzętu. 40. Raport zbiorczy historii zmian w sprzęcie. 41. Ewidencja zdarzeń serwisowych. 42. Dodanie notatek\komentarzy dla zdefiniowanych obiektów zasobów. 43. Informacja na temat pojemności dysków twardych oraz wolnego miejsca. 44. Wydruk\dodanie jako załącznik protokołu przekazania\zwrotu\utylizacji sprzętu. 45. Wydruk\dodanie jako załącznik protokołu przekazania dla całego zestawu. 46. Kreator szablonów wydruków WYSIWYG. 47. Wydruk\dodanie jako załącznik Karty informacyjnej dla elementu wyposażenia. 48. Porównywarka wyników skanowania sprzętu. 49. Automatyczny monitoring i raportowanie zmian w podzespołach sprzętu. 50. Zdalne wykonywanie skryptów (batch) - Obsługa zadań jednorazowych i cyklicznych. 51. Wykonywanie zadań dla wszystkich komputerów (uwzględnia komputery, które zostaną dodane w przyszłości). 52. Edytor skryptów (batch). 53. Wykorzystywanie predefiniowanych skryptów (batch). 54. Import informacji o wyposażeniu z pliku CSV. 55. Generowanie kodów paskowych, QR dla każdego elementu wyposażenia. 56. Obsługa kodów QR. 57. Archiwum zasobów. 58. Przeniesienie utylizowanego wyposażenia do archiwum. 59. Automatyczne usunięcie informacji sieciowych oraz licencji agenta dla zasobu archiwizowanego. 60. Zarządzanie sprzętem przez aplikacje mobilną (Android, Windows Phone). 61. Powiadomienia o kończącej się gwarancji\umowie serwisowej dla zasobu. 62. Zachowanie ostatniego skanu sprzętu podczas konserwacji bazy danych. |
| Zarządzanie zasobami - licencje | 1. Inwentaryzacja licencji. 2. Automatyczne tworzenie licencji na podstawie kluczy produktów. 3. Import licencji z pliku tekstowego. 4. Automatyczne generowanie historii zmian w licencji. 5. Określanie statusu licencji. 6. Utworzenie własnych atrybutów licencji. 7. Tworzenie notatek oraz załączników w dowolnym formacie do licencji. 8. Tworzenie licencji z poziomu rozliczenia audytu legalności. 9. Tworzenie licencji z poziomu raportu kluczy licencji. 10. Tworzenie zestawów licencji. 11. Zmiana typu licencji dla wybranej grupy. 12. Kompletna informacja na temat posiadanych licencji (typ, producent, program licencjonowania, czas ważności, informacje finansowe). 13. Przypisywanie licencji do komputera. 14. Definiowanie wymaganych atrybutów legalności (faktura, nośnik, COA, etc.). 15. Definiowanie ilości posiadanych licencji w rozbiciu na użytkowników oraz stanowiska. 16. Definiowanie licencji przeznaczonych do przyszłego zakupu. 17. Definiowanie kluczy seryjnych i przypisywanie do licencji. 18. Skanowanie oprogramowania na podstawie harmonogramu oraz definicji skanera. 19. Automatyczna kontrola zmian w stanie zainstalowanego oprogramowania bez zlecania skanów. 20. Śledzenie zmian w stanie zainstalowanego oprogramowania. 21. Zdalny skan komputerów (bieżący lub okresowy). 22. Zmiana priorytetu skanowania oprogramowania. 23. Skan komputerów niepodłączonych do sieci. 24. Wysyłanie wyników skanowania offline. 25. ~~Skan oraz identyfikacja zawartości archiwów zapisanych w formatach: 7z, arj, bz2, bzip2, cab, gz, gzip, img, iso, jar, lha, lzh, lzma, msi, nrg, rar, tar, taz.~~ 26. Wbudowane profile skanowania (np. profil wzorcowy). 27. Definicja własnych ustawień skanowania. 28. Porównywanie wyników skanowania oprogramowania. 29. Wykrywanie i inwentaryzacja plików dowolnego typu (np. multimedia, czcionki, grafika) 30. Odczytywanie informacji o składnikach aplikacji, których programy instalacyjne nie są zgodne ze standardem MSI. 31. Identyfikacja SID użytkownika, dla którego zainstalowano oprogramowanie. 32. Bezpłatna, automatycznie aktualizowana baza wzorców aplikacji\pakietów\systemów operacyjnych. 33. Definiowanie katalogów wykluczonych / uwzględnionych w skanowaniu. 34. Audyt oprogramowania - informacja o stanie posiadanych licencji i faktycznie zainstalowanych programach z uwzględnieniem wybranych zestawów licencji. 35. Historia audytów (Wyniki audytów są przechowywane w bazie danych - można do nich wracać w dowolnej chwili, porównywać je i generować stosowne raporty). 36. Gotowe metryki audytowanego komputera - załącznik do protokołu przekazania stanowiska komputerowego (sprzęt + oprogramowanie). 37. Uwzględnianie w rozliczeniu oprogramowania liczby aktywacji zapisanej w szablonie licencji. 38. Mechanizm informujący o nowej bazie wzorców oprogramowania. 39. Automatyczne dodawanie informacji o wydawcy oprogramowania dla nowych wzorców, tworzonych na podstawie wyników skanowania. 40. Wykrywanie kluczy/identyfikatorów programów. 41. Odczytywanie informacji o kluczach pakietów Microsoft Office. 42. Drukowanie lub zapisywanie do pliku raportów ze szczegółami oprogramowania. 43. Zbiorcze raporty wyników skanowania oprogramowania - Pakiety, pliki, systemy operacyjne, kluczy zainstalowanych aplikacji. 44. Raport z informacjami o pakietach oprogramowania uwzględniający parametry: przybliżona wielkość, adres strony internetowej, lokalizacja pliku instalacyjnego, architektura aplikacji, itd. 45. Zdalna instalacja dowolnego oprogramowania zgodnego ze standardem Windows Installer (\*.msi). 46. Zdalne dezinstalacja oprogramowania. 47. Utworzenie harmonogramu dezinstalacji oprogramowania. 48. Generowanie skryptu deinstalacji aplikacji na podstawie otrzymanych wyników skanowania oprogramowania. 49. Raport stanu oprogramowania antywirusowego, antyszpiegowskiego oraz zapory sieciowej. 50. Raport zainstalowanych aktualizacji systemu Windows. |
| Zarządzanie użytkownikami | 1. Dane gromadzone dla konkretnych użytkowników (na bazie loginów) - jeden użytkownik może mieć przypisanych wiele loginów i pracować na różnych komputerach. 2. Grupowanie użytkowników z podziałem na jednostki organizacyjne w firmie (np. względem działów). 3. Określanie przełożonego dla użytkownika. 4. Prezentacja 'stanu użytkownika' (obecny, nieobecny, nowy). 5. Prezentacja 'statusu użytkownika' (Zatrudniony, zwolniony, itd.) 6. Zarządzanie stanowiskami użytkowników. 7. Przeniesienie rekordu użytkownika do archiwum. 8. Funkcjonalności automatycznego generowania zmian rekordu użytkownika – Historia użytkownika. 9. Odczytywanie informacji o użytkownikach z Active Directory. 10. Pełna synchronizacja rekordów użytkowników (Odwzorowanie wszystkich wprowadzonych zmian w rekordach Active Directory). 11. Baza danych teleadresowych użytkowników z możliwością tworzenia raportów i zestawień. 12. Podgląd zdjęcia przypisanego do użytkownika. 13. Przypisywanie do użytkownika załączników (pliki). 14. Przypisywanie notatek do użytkownika. 15. Ewidencja zdarzeń przypisanych do użytkowników. 16. Automatyczne tworzenie działów na podstawie informacji odczytanych z Active Directory. 17. Monitorowanie odwiedzanych strony WWW. 18. Informacje o operacjach na podłączanych nośnikach USB. 19. Blokowanie aplikacji, strony WWW i nośniki USB. 20. Analiza aktywności użytkowników. 21. Analiza zdarzeń sesji użytkownika (Logowanie, Wylogowanie, Zablokowanie, Odblokowanie, Nawiązanie połączenia RDP, Zakończenie połączenia RDP). 22. Analiza przerw w pracy. 23. Analiza jakości pracy (liczba kliknięć myszą, liczba wpisanych znaków). 24. Analiza aktywności mikrofonu oraz kamery. 25. Analiza wykorzystania poszczególnych aplikacji w czasie. 26. Analiza czasu działania aplikacji. 27. Uwzględnienie lub wyłączenie z raportu aplikacji bez aktywności użytkownika. 28. Kategoryzacja danych czasu pracy (czas pozytywny, neutralny oraz negatywny). 29. Statystyki najczęściej wykorzystywanych aplikacji. 30. Statystyki wykorzystania komputerów przez poszczególnych użytkowników. 31. Statystyki aktywności użytkownika i grup użytkowników. 32. Generowanie raportów z monitoringu użytkowników dla wybranego zakresu godzin. 33. Kontrola wydruków - historia zadań drukowania zainicjowanych przez poszczególnych użytkowników. 34. Informacje o drukowanych dokumentach (osoba, nazwa pliku, ilość stron, ilość kopii). 35. Monitoring wydruków na drukarkach sieciowych. 36. Informacja o operacjach na nośnikach zewnętrznych (CD/DVD, HDD, FDD, Pen Drive, etc.). 37. Informacje o awariach, poczynaniach użytkowników: zakończonej aktualizacji, akcji podpięcia przenośnych dysków, włożenia płyt do napędów CD/DVD, śledzenie uruchomienia aplikacji przez użytkownika, monitoring informujący o małej ilości miejsca. 38. Raport zbiorczy historii zmian w rekordach użytkowników. 39. Blokada niepożądanych aplikacji. Programy mogą być blokowane dla całej firmy lub tylko dla wybranych użytkowników. 40. Autoryzacja nośników zewnętrznych. 41. Konfigurowanie praw dostępu do plików i katalogów zapisanych na nośnikach zewnętrznych. 42. Baza informacji o napędach zewnętrznych. 43. Blokada dostępu do napędów zewnętrznych (m.in. HDD, FDD, Pen Drive, etc.) 44. Określanie praw dostępu w zależności od typu urządzenia, np. Pendrive, CD/ROM. 45. Informacje o ostatnio zalogowanych osobach na stacjach klienckich. 46. Blokada stron internetowych dla poszczególnych użytkowników, możliwość zastosowania filtrów, blokada WWW po zawartości (ContentType). 47. Blokada stron internetowych dla protokołu http \ https. 48. Kategoryzacja stron internetowych. 49. Blokada dostępu do witryn zgodnie z harmonogramem. 50. Blokada trybu incognito w przeglądarce Google Chrome. 51. Raporty dotyczące aktywności użytkowników w Internecie oparte na loginach. 52. Analiza czasu przebywania na poszczególnych stronach lub domenach (z uwzględnieniem informacji o tytule strony i wersji przeglądarki). 53. Raport informujący o plikach pobranych przez przeglądarki WWW. 54. Monitoring wysyłanych oraz pobieranych plików przez przeglądarki internetowe. 55. Raportowanie aktywności pracy. 56. Przeglądanie ostatnio zgłoszonych incydentów. 57. Dostęp webowy do statystyk monitoringu, zgłoszeń helpdesk oraz powiązanych z użytkownikiem zasobów. 58. Generowanie raportu obecności / nieobecności użytkownika wraz z korelacją jego aktywności na komputerze. 59. Zgłoszenia dotyczące wniosków nieobecności użytkowników. 60. Automatyczne typowanie użytkowników zastępujących dla zgłaszanych nieobecności. 61. Zarządzanie wnioskami nieobecności użytkowników przez przełożonych, informowanie przełożonych poziomów wyżej o urlopie użytkownika. 62. Automatyczne utworzenie relacji przełożony - podwładny na podstawie skanów Active Directory. 63. Możliwość drukowania karty informacyjnej użytkownika, zawierającej informacje kontaktowe, informacje o powiązanych zasobach, licencjach. 64. Generator struktury organizacji na podstawie powiązań użytkowników i ich przełożonych. 65. Planowanie dni wolnych w widoku kalendarza. 66. Planowanie zastępstw podczas nieobecności. |

## Usługa konfiguracji i wdrożenia zabezpieczeń

Wykonawca jest zobowiązany do:

1. Konfiguracji posiadanego urządzenia UTM, 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. Opracowania dokumentacji i przeszkolenia administratorów:
   1. Dostarczenia pełnej dokumentacji z zakresu konfiguracji UTM oraz serwera logów.
   2. Przeszkolenia administratorów urzędu w zakresie zarządzania urządzeniem UTM oraz systemem logów.
4. 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 HDD |
| Pojemność | Co najmniej 2 TB |
| Szybkość odczytu | 140 MB/s |
| Szybkość zapisu | 140 MB/s |
| Prędkość interfejsu | 5 Gbit/s |
| Funkcjonalność | * szyfrowanie wszystkich danych na dysku w czasie rzeczywistym, * funkcja automatycznego blokowania, * zgodność ze wszystkimi systemami operacyjnymi i urządzeniami posiadającymi port USB, * dostęp do danych z możliwością ustawienia własnego unikalnego kodu PIN lub z wykorzystaniem technologii biometrycznej. |
| Bezpieczeństwo fizyczne | Futerał ochronny  certyfikat IP56 |
| Gwarancja | 36 miesięcy |