

Poprawiony Załącznik nr 3 do SWZ **Opis przedmiotu zamówienia**

(Znak postępowania: Gp-Zp. 27101.1.2026)
na zadanie:

„Zakup sprzętu i oprogramowania „Cyberbezpieczna Gmina Krzyżanowice” - Etap I

Zadanie realizowane w ramach Programu Funduszy Europejskich na Rozwój Cyfrowy (FERC) 2021-2027 Priorytet II „Zaawansowane usługi cyfrowe” Działanie 2.2 „Wzmocnienie krajowego systemu cyberbezpieczeństwa”.

I. Routery sieciowe klasy UTM – Typ I - 2 sztuki:

a. Specyfikacja sprzętowa:

i. Parametry sprzętowe:

1. Interfejsy w pełni konfigurowalne (brak stałego przypisania roli portu do WAN/LAN);
2. 2 interfejsy 2,5Gb + 2 interfejsy 2,5Gb PoE+ (802.3at) + 8 interfejsów 1Gb + 1 port USB 3.0 z możliwością obsadzenia w urządzenie pamięci masowej do przechowywania dzienników zdarzeń (event logs);
3. Port konsoli lokalnej RJ45;
4. Montaż w szafie RACK 19” w wysokości montażowej 1U;

ii. Wydajność:

1. Przepustowość zapory ogniowej SPI mierzona w standardzie RFC 2544 (pakiety 1,518 bajtów UDP): co najmniej 9,8Gbps;
2. Przepustowość VPN mierzona w standardzie RFC2544 (1,424 bajtów UDP): co najmniej 1,9Gbps;
3. Przepustowość modułu anti-malware (w trybie uproszczonym lub pełnym) mierzona w standardzie wydajności HTTP (pakiety 1460 bajtów HTTP z zastosowaniem wielu strumieni): co najmniej 2,8Gbps;
4. Przepustowość modułu IPS mierzona w standardzie wydajności HTTP (pakiety 1460 bajtów HTTP z zastosowaniem wielu strumieni): co najmniej 4,4Gbps;
5. Przepustowość łączona IPS wraz z Anti-Malware mierzona w standardzie wydajności HTTP (pakiety 1460 bajtów HTTP z zastosowaniem wielu strumieni): co najmniej 2,9Gbps;
6. Maksymalna łączna ilość nawiązanych sesji TCP mierzona oprogramowaniem IXIA IxLoad: co najmniej **0,9 mln** sesji;
7. Maksymalna jednoczesna ilość połączeń IPsec VPN bez względu na rodzaj – brama-brama, klient-brama: co najmniej 280 sesji;
8. Maksymalna jednoczesna ilość połączeń SSL VPN: co najmniej 140 połączeń;
9. Minimalna ilość obsługiwanych interfejsów VLAN: co najmniej 64 interfejsy;
10. Niezawodność mierzona parametrem MTBF określonym przez producenta na poziomie co najmniej 450000 godzin przy temperaturze co najmniej 22°C;

iii. Monitorowanie:

1. Wykresy przepustowości interfejsów sieciowych oraz interfejsów VLAN na osi czasu (co najmniej 24 godzinnej);
2. Informacja tekstowa lub graficzna o alokacji zasobów sprzętowych urządzenia tj. obciążenia procesora CPU, zajęcie pamięci operacyjnej, wykorzystanie sesji, zajętość pamięci nieulotnej;
3. Informacja tekstowa i/lub graficzna wskazująca na utylizację przepustowości przez mechanizm:
 - a. Analizy warstwy aplikacji;
 - b. Określonego hosta w sieci wewnętrznej;
 - c. Interfejsy sieciowy;
 - d. Monitoring sesji NAT z typem usługi, IP inicjującym, IP docelowym oraz informacją o użytkowniku nawiązującym dane połączenia (np. w przypadku stosowania połączenia VPN przez użytkownika);
4. Statystyki wyświetlające efekty działania skanerów:
 - a. Skanowania zawartości (Content Filtering);
 - b. Filtra reputacji (IP/DNS/URL);
 - c. Modułu IPS;
 - d. Modułu anti-malware;
 - e. Modułu inspekcji SSL;
 - f. Modułu Sandboxingu;
5. Monitoring interfejsów sieciowych z następującymi informacjami:
 - a. Typ interfejsu (WAN/LAN);
 - b. Przypisanie typu interfejsu do fizycznego portu urządzenia;
 - c. Przepustowość interfejsu;
 - d. Rodzaj interfejsu LAN/WAN/VLAN;
 - e. Adresacja routera przypisana na tym interfejsie (WAN/LAN/VLAN) wraz z numerem interfejsu VLAN jeżeli dotyczy (VLAN Tag);
6. Wizualizacja danych pasywnego skanera sieci:
 - a. Adres MAC urządzenia;
 - b. Adres IP;
 - c. Nazwa hosta;
 - d. Wykrycie w interfejsie LAN/VLAN;
 - e. Typ urządzenia (komputer, urządzenie mobilne itp.);
 - f. Wykryty system operacyjny;
 - g. Data ostatniej detekcji w sieci wewnętrznej;
7. Lista użytkowników połączonych z urządzeniem w zakresie:
 - a. Połączenia HTTP/HTTPS zarządzania;
 - b. Połączeń VPN z tym połączenia VPN;
 - c. Przypisany adres IP w sieci wewnętrznej w przypadku tunelowania połączenia VPN (mapowany adres);
 - d. Adres IP hosta łączącego zdalnie np. poprzez VPN;
8. Tablica adresów serwera DHCP zawierająca:
 - a. Przypisany interfejs LAN/VLAN;
 - b. Przydzielony adres IP;
 - c. Nazwa hosta;
 - d. Wykryty adres MAC;
 - e. Stan przypisania adresu (rezerwacja stała, dzierżawa);

- f. Funkcjonalność eksportu listy do pliku tekstowego;
- 9. Monitorowanie połączeń VPN:
 - a. Nazwa użytkownika;
 - b. Przypisany adres IP;
 - c. Zdalny adres IP inicjatora;
 - d. Czas sesji VPN;
 - e. Ilość wysłanych oraz odebranych danych;
- 10. Stan licencji z podziałem na typ licencji, datę wygaśnięcia licencji oraz stan aktywacji;
- 11. Wyświetlanie informacji o ostatniej aktualizacji sygnatur bezpieczeństwa dotycząca modułów wymagających synchronizacji z chmurą producenta, zawierająca informację o dacie publikacji sygnatur oraz dacie ich aktualizacji przez urządzenie;
- 12. Monitorowanie urządzenia za pomocą protokołu SNMPv2, v3 (z szyfrowaniem);

iv. Funkcjonalność podstawowa

- 1. Routing, wsparcie dla protokołów Ethernet oraz PPPoE dla portów WAN.
- 2. Trasowanie statyczne;
- 3. Trasowanie dynamiczne oparte na identyfikacji hosta/użytkownika w sieci wewnętrznej oparte m.in. na kryteriach:
 - a. Użytkownik (obiekt/grupa);
 - b. Okienko czasowe – harmonogram (obiekt/grupa);
 - c. Źródło połączenia (obiekt/grupa);
 - d. Cel połączenia (obiekt/grupa);
 - e. Typ usługi / protokołu (obiekt/grupa);
 - f. Port źródłowy (obiekt/grupa);
- 4. Trasowanie oparte o polisy NAT/SNAT;
- 5. Funkcjonalność DHCP (server, klient, relay);
- 6. Wsparcie dla protokołu DDNS (Dynamic DNS);
- 7. Rozkładanie obciążenia interfejsów WAN, przełączanie między WAN w przypadku awarii, zarządzanie przepustowością opartą na priorytetach;
- 8. Dziennik zdarzeń wewnętrzny (w pamięci ulotnej), zewnętrzny (przechowywany na nośniku USB), zdalny – sieciowy (komunikacja z co najmniej dwoma niezależnymi serwerami SYSLOG o różnej konfiguracji w zakresie poziomu przesyłanych zdarzeń. Dla każdego typu odbiorcy dzienników (wewnętrzny/USB/zdalny) istnieje możliwość ustalenia kategorii przesyłanych danych opartych na kryteriach:
 - a. Wybór poziomu przesyłanych zdarzeń typu:
 - i. Brak
 - ii. Standardowe informacje
 - iii. Informacje typu debug
 - b. Ustalenie kategorii przesyłanych zdarzeń:
 - i. Autoryzacja;
 - ii. Bezpieczeństwo;
 - iii. Systemowe;
 - iv. Usługi ochrony;
 - v. VPN;
 - vi. Licencje;
 - vii. Sieć;

9. Aktualizacja oprogramowania układowego poprzez załadowanie pliku z firmware lub bezpośrednio przez urządzenie z chmury producenta;
10. Możliwość ustalenia automatycznego harmonogramu instalowania aktualizacji firmware;
11. Możliwość przechowywania co najmniej dwóch różnych konfiguracji urządzenia w pamięci nieulotnej urządzenia.
12. Zastosowanie technologii podwójnego obrazu firmware;
13. Autoryzacja logowania do panelu zarządzania urządzenia oraz komunikacji VPN na podstawie wbudowanej bazy danych użytkowników lub synchronizowana z bazy zewnętrznej.
14. Zarządzanie urządzeniem za pomocą HTTPS, SSH, portem konsoli.
15. Wsparcie dla pracy w trybie wysokiej dostępności (HA – High Availability) w przypadku zastosowania dwóch takich samych urządzeń;
16. Wbudowane narzędzia diagnostyczne polegające na:
 - a. Przechwytywaniu pakietów w oparciu o wybrany interfejs sieciowy, podsieć VLAN, określony adres IP, usługę, port na wbudowanej pamięci flash, nośnik USB lub na serwer FTP;
 - b. Opcja pobrania dzienników systemowych (system log) przechowywanych w pamięci flash urządzenia;
 - c. Wbudowane narzędzia NSLookup IPv4, PING IPv4, Traceroute IPv4, IPSec Trace Log;

v. Funkcjonalność z zakresu bezpieczeństwa:

1. Zapora ogniowa, routing, bridge, SPI, NAT Traversal, ALG, Anti-DOS, możliwość importu zewnętrznych list IP/DNS do modułu blokad zapory ogniowej;
2. Polisy bezpieczeństwa wsparcie dla filtrowania zawartości (content filtering), monitoring warstwy aplikacyjnej, inspekcja pakietów SSL, ustalanie budowy polis bezpieczeństwa opartych na:
 - a. Źródle (strefa - obiekt);
 - b. Destynacji (strefa – obiekt);
 - c. Inicjatorze (obiekt/grupa);
 - d. Cel (obiekt/grupa);
 - e. Usługa (obiekt/grupa);
 - f. Użytkownik (obiekt/grupa);
 - g. Czas (harmonogram – obiekt/grupa);
 - h. Typ akcji;
 - i. Logowanie operacji (nie/tak/tak z ostrzeżeniem);
 - j. Przypisanie dodatkowych mechanizmów bezpieczeństwa do danej polisy:
 - i. Kontrola warstwy aplikacji;
 - ii. Filtrowanie zawartości DNS/URL/IP;
 - iii. Inspekcja SSL;
3. Mechanizm zapobiegania podszywania się pod adres IP znanych urządzeń (IP/MAC Spoofing) obsługujący adresy IP przydzielone poprzez serwer DHCP urządzenia oraz adresy przypisane statycznie. Analiza odbywa się na zasadzie korelacji określonego adresu IP w połączeniu z adresem MAC. Istnieje możliwość zastosowania wyjątku dla określonych adresów IP które będą wyłączone z skanowania;

4. Moduł IPS bazujący m.in. na skanowaniu na podstawie sygnatur z możliwością stosowania białej i czarnej listy. Analizujący dane pod kątem zawartych w nich exploitów, ataków XSS lub SQL Injection.
5. Analityka warstwy aplikacyjnej pakietów IP umożliwiająca tworzenie reguł bezpieczeństwa opartych o komunikację danej aplikacji. Lista aplikacji z podziałem na kategorie i aktualizowana z bazą danych producenta w celu zachowania jej aktualności. Istnieje możliwość wyświetlenia statystyk komunikacyjnych dotyczących danej aplikacji.
6. Filtr przeciwdziałający szkodliwemu oprogramowaniu – Anti-Malware analizujący plik wg rozszerzeń, identyfikatorów szkodliwego oprogramowania (znanych cechach identyfikujących);
7. Sandboxing bazujący na chmurze producenta skanujący podejrzane pliki, synchronizujący sygnatury z chmurą producenta;
8. Filtr Reputacyjny adresów IP, nazw DNS oraz adresów URL polegający na oznaczaniu jako niebezpieczne adresów IP, nazw DNS oraz adresów URL klasyfikowanych i przechowywanych w usłudze producenta urządzenia z której korzysta router podczas pracy w przypadku aktywacji usługi na danej regule bezpieczeństwa. Filtr podzielony jest na kategorie aktualizowane przez producenta w ramach aktualizacji sygnatur. Wsparcia dla białej i czarnej listy określanej przez administratora. Analityka dla ruchu przychodzącego lub wychodzącego. Filtr może być zasilany zewnętrzną listą adresów publikowaną poprzez protokół HTTP z możliwością ustawienia interwału automatycznej aktualizacji.
9. Możliwość utworzenia białej/czarnej listy destynacji DNS/URL w celu całkowitego zablokowania komunikacji internetowej i dopuszczenia tylko do określonych destynacji;
10. Możliwość przekierowania wywołania dla zablokowanej strony internetowej na określoną w panelu konfiguracyjną stronę informacyjną.
11. Możliwość zmiany portów usług HTTP/HTTPS, SSH, FTP, SSL VPN;
12. Wysyłanie powiadomień poprzez wiadomość e-mail za pomocą autoryzowanego konta SMTP i z wsparciem szyfrowania TLS;
13. Możliwość konfiguracji co dziennego raportu o określonej godzinie zawierającego podstawowe informacje, m.in. zajętość procesora, pamięci operacyjnej, użycia przepustowości, stanu mechanizmów bezpieczeństwa (IPS, Anti-Malware, filtr reputacji) z ich wykryciami, tablicą adresów DHCP w poszczególnych sieciach LAN/VLAN. Wizualizacja w formie wykresów lub tabel.
14. Możliwość konfiguracji automatycznego wykonywania kopii konfiguracji oraz wysyłki na wskazane adresy e-mail w określonym dniu, godzinie lub miesiącu.
15. Inspekcja SSL, głęboka analityka pakietów TLS (w tym TLS 1.3), możliwość blokowania certyfikatów uznanych za niezaufane, integracja modułu z mechanizmami IPS, Anti-Malware, Sandboxing, analityka aplikacji oraz filtrowanie ruchu HTTP/HTTPS.
16. Możliwość wygenerowania certyfikatu self-signed oraz importu gotowego certyfikatu z przydzieleniem funkcjonalności – autoryzacja serwera, autoryzacja klienta, certyfikat IKE (Key-Exchange);
17. Kontrola nad zachowaniem usług DoH – DNS over HTTPS w celu umożliwienia korzystania z usługi przez klientów sieci lub jej zablokowania;



18. Wbudowany skaner infrastruktury wewnętrznej polegający na pasywnym analizowaniu ruchu sieciowego oraz kategoryzowaniu urządzeń na elementy infrastruktury klienckiej, sieciowej, bezprzewodowej itp.
 19. Tworzenie reguł zawierających klasyfikację celów i destynacji opartych o geolokalizację z możliwością stosowaniu reguł w oparciu co najmniej o kraj lub kontynent. Możliwość tworzenia grupy krajów i korzystania z niej w polisach bezpieczeństwa.
 20. Możliwość wykluczania określonych adresów IP z filtrowania IPS, Anti-Malware, filtrowania DNS/URL.
 21. Wsparcie dla protokołu IPSec VPN, SSL VPN z wsparciem dla tworzenia profili kompatybilnych z oprogramowaniem OpenVPN oraz konfiguracją kompatybilną z oprogramowaniem wbudowanym w systemie Windows. Wsparcie dla protokołów IKEv2, MS-CHAPv2, EAP, DES, 3DES, AES (256), MD5, SHA2, SHA2 (512). Grupy DH 2, 5, 14-16, 19-20, 28-30. Autoryzacja bazująca na certyfikatach PKI lub kluczach tekstowych (PSK). Wsparcie dla PFS, IPSec NAT-T, DPD (Dead Peer Detection). Dla protokołu SSL obsługa trybu Full oraz Split tunelu VPN. Wsparcie dla autoryzacji 2FA opartej co najmniej o aplikację Google Authentication oraz Microsoft Authenticator. Możliwość określania routingu klienta VPN polegającego na maskowaniu adresu IP VPN klienta w sieci wewnętrznej i jego translację do określonego adresu IP w danym segmencie sieci/podsieci.
 22. Wszystkie moduły bezpieczeństwa aktualizowane są wg zadanego w panelu administracyjnym interwału jednakże czas ten musi umożliwiać aktualizację w interwałach co najmniej 24 godzin;
- b. Licencje** - urządzenie dostarczone z dwuletnią licencją obejmującą wszystkie funkcjonalności opisane w specyfikacji urządzenia oraz jego mechanizmów zabezpieczających;
- c. Gwarancja producenta:** „do końca życia produktu” co oznacza że podlega ciągłej gwarancji producenta oraz 5-cio letniej gwarancji producenta od publikacji informacji o zakończeniu produkcji modelu urządzenia;

II. Routery sieciowe klasy UTM – Typ II – 1 sztuka:

a. Specyfikacja sprzętowa:

i. Parametry sprzętowe:

1. Interfejsy w pełni konfigurowalne (brak stałego przypisania roli portu do WAN/LAN);
2. 8 interfejsów 1Gb + 1 port USB 3.0 z możliwością obsadzenia w urządzenie pamięci masowej do przechowywania dzienników zdarzeń (event logs);
3. Interfejs konsoli lokalnej RJ-45;

ii. Wydajność:

1. Przepustowość zapory ogniowej SPI mierzona w standardzie RFC 2544 (pakiety 1,518 bajtów UDP): co najmniej 3,9Gbps;
2. Przepustowość VPN mierzona w standardzie RFC2544 (1,424 bajtów UDP): co najmniej 0,8Gbps;
3. Przepustowość modułu anti-malware (w trybie uproszczonym lub pełnym) mierzona w standardzie wydajności HTTP (pakiety 1460 bajtów HTTP z zastosowaniem wielu strumieni): co najmniej 0,9Gbps;
4. Przepustowość modułu IPS mierzona w standardzie wydajności HTTP (pakiety 1460 bajtów HTTP z zastosowaniem wielu strumieni): co najmniej 1,4Gbps;
5. Przepustowość łączona IPS wraz z Anti-Malware mierzona w standardzie wydajności HTTP (pakiety 1460 bajtów HTTP z zastosowaniem wielu strumieni): co najmniej 0,9Gbps;
6. Maksymalna łączna ilość nawiązanych sesji TCP mierzona oprogramowaniem IXIA IxLoad: co najmniej 0,3mln sesji;
7. Maksymalna jednoczesna ilość połączeń IPsec VPN bez względu na rodzaj – brama-brama, klient-brama: co najmniej 40 sesji;
8. Maksymalna jednoczesna ilość połączeń SSL VPN: co najmniej 20 połączeń;
9. Minimalna ilość obsługiwanych interfejsów VLAN: co najmniej 16 interfejsów;
10. Niezawodność mierzona parametrem MTBF określonym przez producenta na poziomie co najmniej 500000 godzin przy temperaturze co najmniej 22°C;

iii. Monitorowanie:

1. Wykresy przepustowości interfejsów sieciowych oraz interfejsów VLAN na osi czasu (co najmniej 24 godzinnej);
2. Informacja tekstowa lub graficzna o alokacji zasobów sprzętowych urządzenia tj. obciążenia procesora CPU, zajęcie pamięci operacyjnej, wykorzystanie sesji, zajętość pamięci nieulotnej;
3. Informacja tekstowa i/lub graficzna wskazująca na użycie przepustowości przez mechanizm:
 - a. Analizy warstwy aplikacji;
 - b. Określonego hosta w sieci wewnętrznej;
 - c. Interfejs sieciowy;
 - d. Monitoring sesji NAT z typem usługi, IP inicjującym, IP docelowym oraz informacją o użytkowniku nawiązującym dane połączenia (np. w przypadku stosowania połączenia VPN przez użytkownika);
4. Statystyki wyświetlające efekty działania skanerów:
 - a. Skanowania zawartości (Content Filtering);
 - b. Filtra reputacji (IP/DNS/URL);
 - c. Modułu IPS;

- d. Modułu anti-malware;
- e. Modułu inspekcji SSL;
- f. Modułu Sandboxingu;
5. Monitoring interfejsów sieciowych z następującymi informacjami:
 - a. Typ interfejsu (WAN/LAN);
 - b. Przypisanie typu interfejsu do fizycznego portu urządzenia;
 - c. Przepustowość interfejsu;
 - d. Rodzaj interfejsu LAN/WAN/VLAN;
 - e. Adresacja routera przypisana na tym interfejsie (WAN/LAN/VLAN) wraz z numerem interfejsu VLAN jeżeli dotyczy (VLAN Tag);
6. Wizualizacja danych pasywnego skanera sieci:
 - a. Adres MAC urządzenia;
 - b. Adres IP;
 - c. Nazwa hosta;
 - d. Wykrycie w interfejsie LAN/VLAN;
 - e. Typ urządzenia (komputer, urządzenie mobilne itp.);
 - f. Wykryty system operacyjny;
 - g. Data ostatniej detekcji w sieci wewnętrznej;
7. Lista użytkowników połączonych z urządzeniem w zakresie:
 - a. Połączenia HTTP/HTTPS zarządzania;
 - b. Połączeń VPN z tym połączenia VPN;
 - c. Przypisany adres IP w sieci wewnętrznej w przypadku tunelowania połączenia VPN (mapowany adres);
 - d. Adres IP hosta łączącego zdalnie np. poprzez VPN;
8. Tablica adresów serwera DHCP zawierająca:
 - a. Przypisany interfejs LAN/VLAN;
 - b. Przydzielony adres IP;
 - c. Nazwa hosta;
 - d. Wykryty adres MAC;
 - e. Stan przypisania adresu (rezerwacja stała, dzierżawa);
 - f. Funkcjonalność eksportu listy do pliku tekstowego;
9. Monitorowanie połączeń VPN:
 - a. Nazwa użytkownika;
 - b. Przypisany adres IP;
 - c. Zdalny adres IP inicjatora;
 - d. Czas sesji VPN;
 - e. Ilość wysłanych oraz odebranych danych;
10. Stan licencji z podziałem na typ licencji, datę wygaśnięcia licencji oraz stan aktywacji;
11. Wyświetlanie informacji o ostatniej aktualizacji sygnatur bezpieczeństwa dotycząca modułów wymagających synchronizacji z chmurą producenta, zawierająca informację o dacie publikacji sygnatur oraz dacie ich aktualizacji przez urządzenie;
12. Monitorowanie urządzenia za pomocą protokołu SNMPv2, v3 (z szyfrowaniem);

iv. Funkcjonalność podstawowa

1. Routing, wsparcie dla protokołów Ethernet oraz PPPoE dla portów WAN.
2. Trasowanie statyczne;

3. Trasowanie dynamiczne oparte na identyfikacji hosta/użytkownika w sieci wewnętrznej oparte m.in. na kryteriach:
 - a. Użytkownik (obiekt/grupa);
 - b. Okienko czasowe – harmonogram (obiekt/grupa);
 - c. Źródło połączenia (obiekt/grupa);
 - d. Cel połączenia (obiekt/grupa);
 - e. Typ usługi / protokołu (obiekt/grupa);
 - f. Port źródłowy (obiekt/grupa);
4. Trasowanie oparte o polisy NAT/SNAT;
5. Funkcjonalność DHCP (server, klient, relay);
6. Wsparcie dla protokołu DDNS (Dynamic DNS);
7. Rozkładanie obciążenia interfejsów WAN, przełączanie między WAN w przypadku awarii, zarządzanie przepustowością opartą na priorytetach;
8. Dziennik zdarzeń wewnętrzny (w pamięci ulotnej), zewnętrzny (przechowywany na nośniku USB), zewnętrzny – sieciowy (komunikacja z serwerem SYSLOG);
9. Aktualizacja oprogramowania układowego poprzez załadowanie pliku z firmware lub bezpośrednio przez urządzenie z chmury producenta;
10. Możliwość przechowywania co najmniej dwóch różnych konfiguracji urządzenia w pamięci nieulotnej urządzenia.
11. Zastosowanie technologii podwójnego obrazu firmware;
12. Autoryzacja logowania do panelu zarządzania urządzeniem oraz komunikacji VPN na podstawie wbudowanej bazy danych użytkowników lub synchronizowana z bazy zewnętrznej.
13. Zarządzanie urządzeniem za pomocą HTTPS. SSH, portem konsoli.
14. Zarządzanie oraz monitorowanie urządzenia z poziomu chmury producenta poprzez panel WWW oraz aplikację pracującą pod kontrolą systemu Android. Producent zapewnia pakiety licencyjne o różnej funkcjonalności w tym minimum jeden darmowy. Rozwiązanie chmurowe producenta kompatybilne z stosowanym rozwiązaniem chmurowym zaoferowanym w urządzeniach z pkt I, V, i X.

v. Funkcjonalność z zakresu bezpieczeństwa:

1. Zapora ogniowa, routing, bridge, SPI, NAT Travelsar, ALG, Anti-DOS, możliwość importu zewnętrznych list IP/DNS do modułu blokad zapory ogniowej;
2. Polisy bezpieczeństwa wsparcie dla filtrowania zawartości (content filtering), monitoring warstwy aplikacyjnej, inspekcja pakietów SSL, ustalanie budowy polis bezpieczeństwa opartych na:
 - a. Źródle (strefa - obiekt);
 - b. Destynacji (strefa – obiekt);
 - c. Inicjatorze (obiekt/grupa);
 - d. Cel (obiekt/grupa);
 - e. Usługa (obiekt/grupa);
 - f. Użytkownik (obiekt/grupa);
 - g. Czas (harmonogram – obiekt/grupa);
 - h. Typ akcji;
 - i. Logowanie operacji (nie/tak/tak z ostrzeżeniem);
 - j. Przypisanie dodatkowych mechanizmów bezpieczeństwa do danej polisy:
 - i. Kontrola warstwy aplikacji;
 - ii. Filtrowanie zawartości DNS/URL/IP;

iii. Inspekcja SSL;

3. Mechanizm zapobiegania podszywania się pod adres IP znanych urządzeń (IP/MAC Spoofing) obsługujący adresy IP przydzielone poprzez serwer DHCP urządzenia oraz adresy przypisane statycznie. Analiza odbywa się na zasadzie korelacji określonego adresu IP w połączeniu z adresem MAC. Istnieje możliwość zastosowania wyjątku dla określonych adresów IP które będą wyłączone z skanowania;
4. Moduł IPS bazujący m.in. na skanowaniu na podstawie sygnatur z możliwością stosowania białej i czarnej listy. Analizujący dane pod kątem zawartych w nich exploitów, ataków XSS lub SQL Injection.
5. Analityka warstwy aplikacyjnej pakietów IP umożliwiająca tworzenie reguł bezpieczeństwa opartych o komunikację danej aplikacji. Lista aplikacji z podziałem na kategorie i aktualizowana z bazą danych producenta w celu zachowania jej aktualności. Istnieje możliwość wyświetlenia statystyk komunikacyjnych dotyczących danej aplikacji.
6. Filtr przeciwdziałający szkodliwemu oprogramowaniu – Anti-Malware analizujący plik wg rozszerzeń, identyfikatorów szkodliwego oprogramowania (znanych cechach identyfikujących);
7. Sandboxing bazujący na chmurze producenta skanujący podejrzane pliki, synchronizujący sygnatury z chmurą producenta;
8. Filtr Reputacyjny adresów IP, nazw DNS oraz adresów URL polegający na oznaczaniu jako niebezpieczne adresów IP, nazw DNS oraz adresów URL klasyfikowanych i przechowywanych w usłudze producenta urządzenia z której korzysta router podczas pracy w przypadku aktywacji usługi na danej regule bezpieczeństwa. Filtr podzielony jest na kategorie aktualizowane przez producenta w ramach aktualizacji sygnatur. Wsparcia dla białej i czarnej listy określonej przez administratora. Analityka dla ruchu przychodzącego lub wychodzącego. Filtr może być zasilany zewnętrzną listą adresów publikowaną poprzez protokół HTTP z możliwością ustawienia interwału automatycznej aktualizacji.
9. Możliwość utworzenia białej/czarnej listy destynacji DNS/URL w celu całkowitego zablokowania komunikacji internetowej i dopuszczenia tylko do określonych destynacji;
10. Możliwość przekierowania wywołania dla zablokowanej strony internetowej na określoną w panelu konfiguracyjną stronę informacyjną.
11. Możliwość zmiany portów usług HTTP/HTTPS, SSH, FTP, SSL VPN;
12. Wysyłanie powiadomień poprzez wiadomość e-mail za pomocą autoryzowanego konta SMTP i z wsparciem szyfrowania TLS;
13. Możliwość konfiguracji co dziennego raportu o określonej godzinie zawierającego podstawowe informacje, m.in. zajętość procesora, pamięci operacyjnej, użycia przepustowości, stanu mechanizmów bezpieczeństwa (IPS, Anti-Malware, filtr reputacji) z ich wykryciami, tablicą adresów DHCP w poszczególnych sieciach LAN/VLAN. Wizualizacja w formie wykresów lub tabel.
14. Możliwość konfiguracji automatycznego wykonywania kopii konfiguracji oraz wysyłki na wskazane adresy e-mail w określonym dniu, godzinie lub miesiącu.
15. Inspekcja SSL, głęboka analityka pakietów TLS (w tym TLS 1.3), możliwość blokowania certyfikatów uznanych za niezaufane, integracja modułu z mechanizmami IPS, Anti-Malware, Sandboxing, analityka aplikacji oraz filtrowanie ruchu HTTP/HTTPS.



16. Możliwość wygenerowania certyfikatu self-signed oraz importu gotowego certyfikatu z przydzieleniem funkcjonalności – autoryzacja serwera, autoryzacja klienta, certyfikat IKE (Key-Exchange);
 17. Kontrola nad zachowaniem usług DoH – DNS over HTTPS w celu umożliwienia korzystania z usługi przez klientów sieci lub jej zablokowania;
 18. Wbudowany skaner infrastruktury wewnętrznej polegający na pasywnym analizowaniu ruchu sieciowego oraz kategoryzowaniu urządzeń na elementy infrastruktury klienckiej, sieciowej, bezprzewodowej itp.
 19. Tworzenie reguł zawierających klasyfikację celów i destynacji opartych o geolokalizację z możliwością stosowania reguł w oparciu co najmniej o kraj. Możliwość tworzenia grupy krajów i korzystania z niej w polisach bezpieczeństwa.
 20. Możliwość wykluczania określonych adresów IP z filtrowania IPS, Anti-Malware, filtrowania DNS/URL.
 21. Wsparcie dla protokołu IPsec VPN, SSL VPN z wsparciem dla tworzenia profili kompatybilnych z oprogramowaniem OpenVPN oraz konfiguracją kompatybilną z oprogramowaniem wbudowanym w systemie Windows. Wsparcie dla protokołów IKEv2, MS-CHAPv2, EAP, DES, 3DES, AES (256), MD5, SHA2, SHA2 (512). Grupy DH 2, 5, 14-16, 19-20, 28-30. Autoryzacja bazująca na certyfikatach PKI lub kluczach tekstowych (PSK). Wsparcie dla PFS, IPsec NAT-T, DPD (Dead Peer Detection). Dla protokołu SSL obsługa trybu Full oraz Split tunelu VPN. Wsparcie dla autoryzacji 2FA opartej co najmniej o aplikację Google Authentication oraz Microsoft Authenticator. Możliwość określania routingu klienta VPN polegającego na maskowaniu adresu IP VPN klienta w sieci wewnętrznej i jego translację do określonego adresu IP w danym segmencie sieci/podsięci.
 22. Wszystkie moduły bezpieczeństwa aktualizowane są wg zadanego w panelu administracyjnym interwału jednakże czas ten musi umożliwiać aktualizację w interwałach co najmniej 24 godzin;
- b. Licencje** - urządzenie dostarczone z dwuletnią licencją obejmującą wszystkie funkcjonalności opisane w specyfikacji urządzenia oraz jego mechanizmów zabezpieczających;
- c. Gwarancja producenta:** „do końca życia produktu” co oznacza że podlega ciągłej gwarancji producenta oraz 5-cio letniej gwarancji producenta od publikacji informacji o zakończeniu produkcji modelu urządzenia;

III. Urządzenia dostępne sieci WiFi 2,4/5Ghz – 7 sztuk;

a. Parametry techniczne:

- i. Interfejsy sieciowe: minimum 1x Ethernet z obsługą 1Gbps oraz 2.5Gbps;
- ii. Zasilanie: 802.3af PoE;
- iii. Wspierane standardy sieci bezprzewodowej: IEEE 802.11 be/ax/ac/n;
- iv. Anteny: wielokierunkowe co najmniej 2x4dBi (2x2 strumienie jednocześnie) dla 2.4Ghz, 3x6dBi dla 5Ghz (3x3 strumienie jednocześnie);
- v. Obsługiwane szerokości pasma: 20Mhz, 40Mhz, 80Mhz, 160Mhz;
- vi. Montaż: sufitowy, ścienny – dołączone adaptory montażowe;
- vii. Teoretyczna przepustowość maksymalna: co najmniej 450 Mb/s dla 2.4Ghz oraz co najmniej 2.6Gbps AC, 3.6Gbps AX, 4.3 BE dla 5Ghz;
- viii. Ilość obsługiwanych profili SSID: 8;
- ix. Izolacja w warstwie L2;
- x. Wykrywanie nieautoryzowanych punktów WiFi (Rogue AP);
- xi. Obsługa VLAN;
- xii. Wsparcie dla serwera SYSLOG;
- xiii. Harmonogram pracy sieci WiFi;
- xiv. Autoryzacja połączenia na podstawie adresów MAC;
- xv. Captive Portal;
- xvi. Obsługa PPSK;
- xvii. Band steering;
- xviii. Wireless meshing;
- xix. 802.11v, 802.11r, 802.11k
- xx. Szyfrowanie WPA/WPA2/WPA3 w wersji Personal (PSK) oraz 802.1x / Radius - Enterprise;
- xxi. Zarządzanie oraz monitorowanie urządzenia poprzez dedykowaną programową konsolę zarządzania, kontroler sprzętowy bezpośrednio poprzez panel WWW lub z poziomu chmury producenta dostępnej poprzez panel WWW oraz aplikację pracującą pod kontrolą systemu Android.

b. Gwarancja producenta: min. 24 miesiące;

IV. Oprogramowanie do inwentaryzacji zasobów informatycznych -- Typ I - 1 licencja ;

a. Architektura / budowa:

- i. System musi zapewnić stabilną obsługę co najmniej 70 klientów jednocześnie;
- ii. Klient – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej;
- iii. Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej);
- iv. Panel pracownika – aplikacja webowa, niewymagająca dodatkowego logowania, dostępna dla pracowników, udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach;
- v. Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z Klientami;
- vi. Baza danych pracująca na silniku Microsoft SQL Server w wersjach wyspecyfikowanych poniżej;
- vii. Komponenty systemu (Klient, konsola administracyjna, serwer, baza danych) aktualizują się automatycznie poprzez bezpieczne połączenie;
- viii. System zawiera mechanizmy automatycznej konserwacji zgodnie z harmonogramem;

b. Wymagania systemowe:

- i. Konsola administracyjna musi działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5;
- ii. Klient musi działać na systemach 32 i 64 bitowych: Windows Server 2012/2012R2/2016/2019/2022, Windows 7/8/8.1/10/11, MacOS 10.7/10.8, Linux dla wersji: Ubuntu v.11.04 lub wyższa, Debian v.6.0 lub wyższa, RedHat v.6.0 lub wyższa, CentOS v.6.0 lub wyższa, Fedora v.16 lub wyższa;
- iii. Klient wspiera poniższe przeglądarki internetowe w zakresie monitorowania aktywności użytkownika w sieci: Opera, Chrome, FireFox;
- iv. Serwer musi działać na systemach 64 bitowych: Windows Server 2016/2019/2022, Windows 7/8/8.1/10/11;
- v. Serwer www musi być oparty o platformę Microsoft 64 bit (Windows Server 2016/2019/2022, Windows 10 oraz Java 8 (JRE lub JDK), Apache Tomcat 9;
- vi. Baza danych musi działać na silniku Microsoft SQL Server 2014/2016/2017/2019/2022 w wersji 64 bitowych bezpłatnym (np. Microsoft SQL Server Express Edition);
- vii. System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare;

c. Interfejsy:

- i. System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie;
- ii. System musi umożliwiać import danych z CSV, Excel, Microsoft SQL Server, MySQL, PostgreSQL;

d. Funkcjonalności systemu zarządzania infrastrukturą IT:

- i. Funkcjonalność Klienta - System musi umożliwiać pełne zdalne zarządzanie Klientami, obejmujące uruchamianie i wyłączenie, zmianę konfiguracji Klienta, inicjowanie skanowania oraz wykonanie poleceń systemowych. Klient powinien wyświetlać komunikaty w HTML z dokładnymi danymi o czasie wyświetlenia i użytkownikowi;
- ii. Funkcjonalność konsoli administracyjnej:
 1. Konsola administracyjna musi być dostępna w języku Polskim i oferować intuicyjny interfejs z pełnym zestawem funkcji zarządzania (dodawanie, modyfikowanie, usuwanie). Musi także zawierać różnorodne dashboardy, w tym dashboardy użytkownika, prezentujące parametry infrastruktury, sieci oraz bezpieczeństwa. Użytkownicy powinni mieć możliwość samodzielnego konfigurowania dashboardów użytkownika, a dashboardy sieciowe i bezpieczeństwa muszą zawierać szczegółowe widżety z informacjami o stanie usług i bezpieczeństwie;
 2. W konsoli powinna istnieć funkcja filtrowania danych na dashboardach oraz możliwość personalizacji interfejsu przez użytkownika, w tym definiowanie własnych pól, filtrów i widoków, z zachowaniem tych ustawień pomiędzy sesjami. Konsola musi także umożliwiać definiowanie poziomów uprawnień dla użytkowników i grup, z opcją dziedziczenia oraz integrację z Active Directory dla zarządzania dostępem;
 3. Konsola powinna posiadać zaawansowane funkcje zarządzania rekordami, w tym wykonanie poleceń na wielu rekordach jednocześnie oraz dostęp do szczegółowych informacji o pracy urządzeń;
- iii. Funkcjonalność panelu pracownika – panel pracownika systemu musi automatycznie uruchamiać się i autoryzować przy logowaniu użytkownika, z możliwością definiowania zakresu dostępnych informacji przez administratora dla poszczególnych grup pracowników. Panel kierownika powinien dodatkowo agregować i analizować dane z paneli pracowników. Informacje w panelu muszą być organizowane w logiczne sekcje, które można indywidualnie lub grupowo włączać i wyłączać przez administratora;
- iv. Zarządzanie licencjami - system musi umożliwiać kompleksowe zarządzanie licencjami w różnych modelach i strukturach organizacyjnych, w tym audyty, zarządzanie oprogramowaniem i oprogramowaniem zabronionym, oraz przypisywanie i rozliczanie różnych typów licencji. Musi także rejestrować historię licencji oraz zapewniać funkcje inwentaryzacji i zdalnej dezinstalacji oprogramowania;
- v. Wzorce aplikacji i pakietów - system powinien posiadać rozbudowaną bazę wzorców oprogramowania, umożliwiać definiowanie własnych wzorców i automatycznie importować nowe wzorce od producenta. Musi także dostarczać szczegółowe informacje o zainstalowanych pakietach i ich wykorzystaniu, w tym edycje Microsoft Office;
- vi. Inwentaryzacja sprzętu komputerowego i urządzeń - system musi oferować rozbudowane funkcje inwentaryzacji sprzętu komputerowego, włączając automatyczną inwentaryzację zarówno w sieci lokalnej jak i zdalnej, szczegółowe skanowanie komponentów (np. RAM, monitory, dyski twarde) oraz zarządzanie informacjami o zainstalowanym sprzęcie. Powinien także umożliwiać ewidencję zmian konfiguracji sprzętu, identyfikować i klasyfikować urządzenia podłączone do komputerów oraz monitorować historię ich połączeń;
- vii. Inwentaryzacja urządzeń sieciowych - system musi posiadać zdolności do identyfikacji urządzeniami sieciowymi. Wymagane jest posiadanie skanera sieci i SNMP, które automatycznie zbierają dane, analizują jakość połączeń i identyfikują urządzenia na sieci. System powinien także umożliwiać zdalną instalację Klientów i generowanie map sieci;

- viii. Inwentaryzacja sprzętu - system musi umożliwiać wszechstronną inwentaryzację sprzętu, włączając urządzenia inne niż komputery (np. drukarki, routery). Musi zapewniać zarządzanie dokumentacją związaną z urządzeniami, monitorować ich ruch oraz przypominać o terminach gwarancji i umowach utrzymaniowych;
- ix. Ochrona danych (DLP):
1. Ochrona danych (DLP) musi obejmować automatyczne tworzenie listy podłączanych do komputerów urządzeń USB i ich klasyfikację. System powinien dostarczać informacje o historii użytkowania urządzeń zewnętrznych oraz umożliwiać zarządzanie dozwolonymi do użytku urządzeniami USB zgodnie z zdefiniowanymi regułami;
 2. Szyfrowanie dysków wewnętrznych oraz zewnętrznych;
 3. System musi obsługiwać kompleksowe szyfrowanie dysków wewnętrznych i zewnętrznych USB, z wykorzystaniem BitLocker i różnych metod szyfrowania, takich jak XTS AES 256 i AES 128. Musi umożliwiać zdalne zarządzanie procesem szyfrowania/desyfrowania, w tym masowe operacje na partycjach systemowych i niesystemowych. Klucze szyfrujące są przechowywane i chronione w konsoli administracyjnej, dostępne tylko po uwierzytelnieniu administratora. Proces szyfrowania odbywa się w sposób niewidoczny dla użytkownika i nie może być przez niego przerwany, z wyjątkiem stanów hibernacji i wyłączenia systemu, po których jest automatycznie kontynuowany;
- x. Zdalna administracja komputerami:
1. System musi oferować kompleksową zdalną administrację komputerami, włączając w to automatyczne wykonywanie dowolnych poleceń (np. zarządzanie aplikacjami, plikami, rejestrami systemowymi) oraz zarządzanie cyklicznymi zadaniami z harmonogramem. Powinien obsługiwać technologię Intel vPro dla zdalnej konfiguracji i zarządzania, a także pozwalać na zdalne przejęcie kontroli nad komputerem za pomocą technologii Ultra VNC, umożliwiając operowanie na wielu sesjach jednocześnie. System powinien integrować zaawansowane mechanizmy skryptowe wspierane przez AI dla automatycznego generowania poleceń oraz umożliwiać zarządzanie i tworzenie zadań cyklicznych z różnorodnymi opcjami cykliczności i zakończenia;
 2. System musi zezwalać na wykonywanie zapytań WMI bez zdalnego połączenia do urządzenia;
 3. System musi zezwalać na edycję rejestrów urządzenia bez wykorzystania zdalnego połączenia pulpitu;
- xi. Zdalne Zarządzanie Zaporą (Firewall) - system musi umożliwiać zdalne zarządzanie zaporą sieciową (firewall) globalnie w infrastrukturze, co obejmuje monitorowanie jej stanu w czasie rzeczywistym, definiowanie złożonych zasad zapory z centralnego panelu administracyjnego oraz szybkie identyfikowanie i reagowanie na potencjalne zagrożenia sieciowe;
- xii. Automatyzacja - system musi oferować możliwość ustalania harmonogramu dla czynności konserwacyjnych, naprawczych i porządkujących, z opcją ustalania częstotliwości i parametrów wejściowych dla każdej czynności oraz możliwością ich zatrzymania lub uruchomienia. Dodatkowo, system musi posiadać mechanizmy automatyzacji takie jak wykonywanie kopii bezpieczeństwa, identyfikacja aplikacji i pakietów, porządkowanie bazy danych oraz usuwanie nadmiarowych danych. System

- również powinien wysyłać alerty o zdarzeniach takich jak nowe komputery w bazie danych, braki w licencjach i inne zdarzenia krytyczne dla infrastruktury IT;
- xiii. Zarządzanie magazynem IT - system musi umożliwiać efektywne zarządzanie magazynem IT, włączając obsługę dowolnej ilości magazynów w różnych lokalizacjach oraz obsługę dokumentów magazynowych typu PZ, RW, WZ, i inne. System powinien prowadzić ewidencję materiałów w magazynach zgodnie z metodą FIFO. Ponadto, system powinien umożliwiać automatyczne łączenie dokumentów magazynowych z zasobami systemu oraz zapewniać przegląd wszystkich dokumentów;
 - xiv. Repozytorium - konsola administracyjna systemu musi być wyposażona w repozytorium dokumentów dowolnego typu, które umożliwia dodawanie nowych dokumentów, przeszukiwanie. Repozytorium powinno także umożliwiać definiowanie kontenerów na dokumenty, co ułatwia organizację i zarządzanie dokumentacją;
 - xv. Kody kreskowe - system musi wspierać obsługę kodów kreskowych jedno i dwuwymiarowych, umożliwiając parametryzację kodu pod względem wielkości i atrybutów graficznych. System powinien umożliwiać podgląd oraz wydruk kodów kreskowych;
 - xvi. Wysyłanie wiadomości - system musi oferować funkcję komunikatora, umożliwiającą bezpośrednią wymianę wiadomości między użytkownikami a administratorem systemu, w tym inicjowanie czatu przez administratora oraz przechowywanie historii konwersacji. System powinien także umożliwiać wysyłanie jednorazowych wiadomości ALERT oraz tworzenie szablonów wiadomości do regularnego użytku, z opcją konfiguracji terminu, po którym wiadomość wygaśnie. Ponadto, system powinien wspierać szkolenie pracowników za pomocą wiadomości tekstowych z możliwością definiowania treści szkoleniowych i automatycznego ich wysyłania;
 - xvii. System musi posiadać możliwość eksportu / importu treści;
 - xviii. Monitorowanie drukarek sieciowych i wydruków - system musi umożliwić monitorowanie i zarządzanie wydrukami z dowolnej drukarki (lokalnej czy sieciowej), rejestrując szczegółowe informacje o każdym wydruku, w tym koszty, dzięki wbudowanemu cennikowi. System powinien również prognozować przyszłe koszty drukowania oraz pozwalać na zarządzanie drukarkami według różnych parametrów, w tym statusu i materiałów eksploatacyjnych;
 - xix. Monitorowanie stron WWW - system musi oferować monitorowanie aktywności internetowej użytkowników na różnych przeglądarkach, nawet przy szyfrowanych połączeniach (https), rejestrując detale takie jak adresy IP, czas połączenia, a także analizując treści stron za pomocą algorytmów sztucznej inteligencji do klasyfikacji i kontroli treści;
 - xx. Monitorowanie serwerów WWW - system musi zapewniać monitorowanie wybranych serwerów WWW, prezentując informacje o ich statusie i aktywności, umożliwiając analizę treści stron oraz graficzną prezentację danych związanych z ich działaniem, w tym czasem odpowiedzi i aktywnością w określonym okresie;
 - xxi. Monitorowanie dziennika zdarzeń - system musi posiadać zdolność do monitorowania dziennika zdarzeń komputerów, umożliwiając definiowanie i filtrowanie zdarzeń według różnych kategorii;
 - xxii. Monitorowanie pracy komputerów - system musi oferować monitorowanie pracy komputerów, w tym dat startu i zakończenia pracy, logowania użytkowników, a także zdalne monitorowanie sesji połączeń, rejestrując szczegóły takie jak adresy IP i dane użytkowników;

- xxiii. Monitorowanie uprawnień ACL - system musi umożliwić skanowanie i monitorowanie uprawnień ACL, oferując szczegółowe raporty, automatyczną aktualizacją danych i filtrami do zarządzania informacjami;
- xxiv. Monitorowanie sensorów - system musi integrować monitoring warunków środowiskowych za pomocą sensorów po SNMP, umożliwiając graficzną prezentację danych, wysyłanie alertów;
- xxv. Repozytorium CMDB - system musi posiadać zintegrowane repozytorium CMDB, umożliwiające zarządzanie zasobami IT, w tym szczegółowe informacje o użytkownikach, urządzeniach, licencjach, a także o oprogramowaniu i jego licencjach, z możliwością importu i eksportu danych;
- xxvi. Zarządzanie czasem pracy użytkowników - system musi umożliwiać monitorowanie i analizę czasu pracy użytkowników, z możliwością definiowania grup przypisanych do przełożonych i prezentacji szczegółowych danych o aktywności użytkowników w formie widżetów i danych analitycznych. Informacje o czasie pracy, sesjach, aktywności w aplikacjach oraz produktywności powinny być możliwe do udostępnienia w panelu pracownika;
- xxvii. Raportowanie i eksport danych - System musi oferować zaawansowane możliwości raportowania i eksportu danych, umożliwiając wyeksportowanie informacji do różnych formatów, w tym xls, csv, html, oraz graficznych. Powinien także wspierać generowanie wieloparametrycznych raportów z możliwością stosowania filtrów, obsługę wieloinstancyjności raportowania oraz integrację z narzędziami do tworzenia raportów takimi jak SAP Crystal Reports i Stimulsoft, obejmując co najmniej 150 zdefiniowanych raportów. Dodatkowo, system musi posiadać możliwość konfiguracji harmonogramu umożliwiającego cykliczne wysyłanie raportów oraz zapisywanie ich w dowolnym miejscu, z automatycznym generowaniem raportu w formacie PDF jako wynikiem wykonania harmonogramu;
- xxviii. System musi zapewnić interfejs API - system musi oferować rozbudowany interfejs API, umożliwiający komunikację za pomocą REST API. Musi on zapewniać szyfrowaną komunikację z użyciem protokołu TLS 1.3 oraz możliwość tworzenia złożonych requestów JSON. Klucze zabezpieczeń powinny być modyfikowalne i mogą mieć co najmniej 32 znaki;
- xxix. Powiadomienia - system musi umożliwiać generowanie różnorodnych powiadomień, w tym alertów w konsoli, e-maili oraz wiadomości SMS, z możliwością edycji treści powiadomień i definiowania grup odbiorców. Powinien obsługiwać automatyczne wywoływanie zadań i integrować się z CMD oraz Windows PowerShell, zapewniając co najmniej 30 predefiniowanych powiadomień oraz możliwość ich personalizacji;
- xxx. Bezpieczeństwo - system musi zapewniać rozbudowane funkcje bezpieczeństwa, w tym definicję i zarządzanie prawami dostępu oraz zaawansowane opcje uwierzytelniania. Wymaga silnych haseł, obsługuje wieloskładnikowe uwierzytelnianie i posiada mechanizmy szyfrowania danych;
- xxxi. Wsparcie i pomoc techniczna producenta systemu
 1. Pomoc techniczna - musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00;
 2. Utrzymaniem Oprogramowania jest zapewnienie aktualizacji Oprogramowania (asysta techniczna) oraz nieprzerwanego działania Oprogramowania (usługi SLA), jak również zapewnienie świadczenia innych usług wspomagających korzystanie z Oprogramowania;



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

3. Czas trwania usługi SLA wynosi 24 miesięcy od dnia zakupu;

V. Oprogramowanie kryptograficzne i analityczne – moduł w pełni kompatybilny z zaoferowanym oprogramowaniem w pkt. IV integrujący informację dotyczące zakresu DLP z wizualizacją w systemie podstawowym z pkt. IV – Typ I – 1 licencja;

a. Architektura / budowa:

- i. System musi zapewnić stabilną obsługę co najmniej 70 klientów jednocześnie;
- ii. Czas aktualizacji wszystkich komponentów systemu: serwer, konsola administracyjna, baza danych, agenci - nie może przekroczyć 24h od wydania przez producenta nowej wersji dowolnego komponentu. Agenci na komputerach muszą się zaktualizować samodzielnie w czasie nie dłuższym niż 8h od pobrania aktualizacji od producenta, przy czym aktualizacja klientów musi przebiegać w pełni automatycznie z wykorzystaniem funkcjonalności wbudowanej w system (bez użycia zewnętrznych narzędzi, np. MS Active Directory). W przypadku, gdy połączenie pomiędzy systemem a serwerem aktualizacji producenta nie jest dostępne musi być możliwość dokonania aktualizacji manualnie poprzez pobranie od producenta paczki aktualizacyjnej w postaci jednego pliku z kompletną aktualizacją;
- iii. System musi w sposób w pełni automatyczny z wykorzystaniem serwera aktualizacji producenta aktualizować wzorce aplikacji, polityk, pomoc i inne wbudowane bazy wiedzy;
- iv. Klient musi być dostępny dla administratora z poziomu webowej interfejsu konsoli administracyjnej zawsze w najnowszej wersji wydanej przez producenta (bez konieczności pobierania go od producenta), w postaci pliku *.msi gotowego do zainstalowania (bez konieczności dodatkowego wykonywania zmian/ustalania parametrów) w pliku *.msi;
- v. Klient musi być możliwy do zainstalowania za pośrednictwem MS Active Directory, za pomocą skryptów lub manualnie, poprzez uruchomienie na danej stacji roboczej;
- vi. System zapewnia możliwość stworzenia instalatora (.exe) z wbudowanymi, zaszyfrowanymi poświadczeniami dla dowolnego konta. Funkcja ta umożliwi instalację usługi bezpośrednio na kontach użytkowników – zarówno lokalnych, jak i domenowych, korzystając z uprawnień zdefiniowanych dla instalatora w konsoli systemu;
- vii. Klient musi pracować w trybie niewidocznym dla użytkownika (usługa systemowa);
- viii. System powinien umożliwiać generowanie unikatowego identyfikatora Klienta – wygenerowanego losowo i unikatowo (np. za pomocą mechanizmu typu GUID) lub w sposób powtarzalny dla danego komputera) na podstawie kombinacji parametrów wybranych przez użytkownika systemu spośród następujących: nazwy producenta BIOS, numeru seryjnego komputera, system UUID, nazwy komputera, dowolnego oraz losowego ciągu znaków;
- ix. Klient musi mieć definiowalny priorytet pracy procesu w systemie operacyjnym (ABOVE_NORMAL, NORMAL, BELOW_NORMAL, IDLE), przy czym w każdym momencie administrator może automatycznie z poziomu konsoli administracyjnej systemu wydać polecenie zmiany tej konfiguracji na dowolnej grupie komputerów;
- x. Klient musi wspierać wiele różnych adresów serwera rozumianych jako adresy w sieci lokalnej, rozległej (VPN) oraz za NATem i potrafić wykorzystać adres dostępny (na którym następuje połączenie z serwerem) w dowolnym momencie działania, bez konieczności restartu Klienta;



- xi. System musi mieć możliwość współpracy komponentów klienta i serwera w taki sposób, aby serwer mógł współpracować ze wszystkimi poprzednimi wersjami Klientów;
- b. System musi mieć wbudowane mechanizmy automatycznej konserwacji/utrzymania zgodnie ze zdefiniowanym harmonogramem:**
 - i. Automaty powinny realizować co najmniej usuwanie zbędnych danych z systemu (dane z monitoringu uruchamianych aplikacji, uruchamianych procesów, odwiedzonych stron www, wydrukowanych dokumentów, indeksowanie bazy danych, kopie bezpieczeństwa przyrostowe i nie przyrostowe, zmniejszanie bazy danych);
 - ii. Harmonogram musi mieć możliwość ustalenia częstotliwości wykonywania zadania (godzina, dzień, tydzień, miesiąc), możliwość zmiany wartości parametrów wejściowych do wykonania danej konserwacji, a także zatrzymania/uruchomienia wybranych pozycji harmonogramu w dowolnym momencie;
- c. Interfejsy:**
 - i. System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie;
 - ii. Import obiektów z MS Active Directory musi być odporny na zmianę nazw obiektów (nazwy użytkownika, struktury organizacyjnej itp.) – podczas import zmienione dane muszą zostać odpowiednio zaktualizowane wg klucza UUID;
 - iii. Import z Active Directory musi wspierać obsługę protokołów SSL oraz TLS;
 - iv. Import z Active Directory musi umożliwiać podanie więcej niż jednej domeny;
 - v. System musi umożliwiać import użytkowników z zewnętrznego pliku CSV;
 - vi. System musi posiadać wbudowany, w pełni definiowalny przez administratora interfejs do importu innych niż komputery urządzeń (np. pendrive, monitory, switchy itp.) wraz z danymi o kosztach zakupu, nr dokumentu zakupowego, dostawcy, daty zakupu, gwarancji. Interfejs dodatkowo musi umożliwiać importowanie użytkowników, struktur i licencji. Import musi umożliwiać pobieranie danych z CSV, Excel, Microsoft SQL Server, MySQL, PostgreSQL z wykorzystaniem sterownika ODBC (np. z pliku tekstowego, pliku xls, pliku xml) w sposób jednorazowy lub zgodnie ze zdefiniowanym harmonogramem. Import aktualizuje te same dane wcześniej zaimportowane;
- d. Funkcjonalności systemu:**
 - i. Funkcjonalność konsoli administracyjnej:
 1. Konsola musi być w pełni polskojęzyczna;
 2. Interfejs konsoli musi być wyposażony w intuicyjne mechanizmy obsługi, musi zapewniać pełną obsługę funkcjonalną (dodawanie/modyfikacja/usuwanie);
 3. Konsola administracyjna musi posiadać dashboard – dashboard użytkownika, dashboard prezentujący parametry infrastruktury, dashboard prezentujący parametry sieci, dashboard prezentujący informacje o bezpieczeństwie;
 4. Konsola administracyjna musi być wyposażona w panel zawierający graficzne widżety prezentujące dane w postaci wykresu kołowego i słupkowego bądź w formie tabeli z danymi;
 5. Dane na widżetach muszą być aktualizowane automatycznie;
 6. System musi umożliwiać i zapamiętywać w profilu użytkownika indywidualną personalizację interfejsu konsoli administracyjnej (wybór wyświetlanych kolumn, ich kolejność, język, definiowanie filtrów, kolejność sortowania, wyświetlane widżety, ich konfigurację i kolejność);

7. Dane prezentowane na wszystkich widokach/zakładkach w systemie muszą być dynamicznie filtrowane w oparciu o reguły utworzone przez dowolnego użytkownika systemu;
8. Dane prezentowane na wszystkich widokach/zakładkach w systemie muszą mieć możliwość filtrowania kolumnowego;
9. System musi umożliwiać definiowanie poziomu uprawnień dla grupy oraz użytkownika (odczyt, usuwanie, modyfikowanie, wydruk) do wszystkich widoków danych oraz wybranych elementów struktury organizacyjnej, musi być wyposażony w opcję dziedziczenia uprawnień. Odebranie praw do widoku lub zakładki na widoku powoduje ukrycie opcji;
10. Lista użytkowników / administratorów systemu musi być importowana i aktualizowana zgodnie z harmonogramem w oparciu o mechanizm RBAC (Role Base Access Control) z wybranego obiektu Active Directory. Użytkownik wyłączony/usunięty/zablokowany w Active Directory automatycznie traci prawa do korzystania z konsoli administracyjnej systemu;
11. Konsola musi umożliwiać wykonywanie poszczególnych poleceń na wielu rekordach, w szczególności na wszystkich rekordach, również tych, które nie są widoczne w konsoli w ramach jednej strony (zaznacz wszystko);
12. Konsola administracyjna musi zawierać szczegółowe informacje dotyczące pracy wszystkich komputerów: wersja Klienta, stanu Klienta (włączony/wyłączony), zalogowanego użytkownika, historii czasu włączenia i wyłączenia komputera;
13. Konsola musi zawierać w sobie pełną dokumentację systemu;
- ii. Odczytywanie zainstalowanego oprogramowania - system powinien prezentować podgląd zainstalowanych systemów operacyjnych, pakietów oraz aplikacji na komputerach z informacjami o: nazwie, wersji, producencie, typie licencji;
- iii. Wzorce aplikacji i pakietów:
 1. System ma posiadać wbudowaną bazę wzorców dostawcy oprogramowania posiadającą co najmniej 4 tys. wzorców aplikacji, 1,3 tys. Producentów;
 2. System musi posiadać możliwość definiowania własnych wzorców aplikacji i pakietów (składających się z aplikacji) w oparciu o definiowalne reguły rozpoznawania;
 3. Własne wzorce aplikacji i pakietów muszą mieć pierwszeństwo w procesie rozpoznawania aplikacji i pakietów;
- iv. Inwentaryzacja sprzętu komputerowego:
 1. System prowadzi szczegółową ewidencję zmian konfiguracji sprzętu;
 2. System udostępnia informacje o występowaniu plików na komputerach (nazwa, rozmiar, rodzaj, wielkość, lokalizacja, w przypadku plików wykonywalnych: wersja, producent);
 3. System musi umożliwiać dokonanie klasyfikacji pliku wg dowolnie zdefiniowanych kategorii (np. audio, wideo, graficzne, erotyczne/pornograficzne, archiwa, wykonywalne);
 4. System pozwala na zdalne trwałe (bez możliwości odzyskania) usunięcie dowolnego pliku/plików na dowolnie zdefiniowanej grupie komputerów;
 5. System udostępnia informacje o zmianach w systemie plików (dodano plik, usunięto plik);
 6. System umożliwia dodawanie notatek do każdej pozycji sprzętu;

7. System musi umożliwiać ewidencję zdarzeń serwisowych dowolnego typu (np. naprawy sprzętu, wymiany części):
 - a. System musi umożliwiać definiowanie typów serwisów;
 - b. System musi umożliwiać definiowanie wartości serwisu;
 - c. System musi umożliwiać definiowanie daty ważności serwisu oraz daty gwarancji;
8. System musi pozwalać na dołączanie do urządzeń dokumentów z repozytorium;
9. System umożliwia samodzielną definicję, ewidencję oraz wydruk wszelkiego typu protokołów (przyjęcie, przekazanie do użytkownika, likwidacja);
- v. Inwentaryzacja urządzeń podłączanych do komputera:
 1. System automatycznie identyfikuje i klasyfikuje urządzenia podłączane do komputera (pendrive, kamera, aparat, monitor zewnętrzny, pamięć masowa, telefon, urządzenie multimedialne itp.);
 2. System pozwala na automatycznie lub ręczne przypisanie podłączonego urządzenia do komputera oraz użytkownika;
 3. System ewidencjonuje historię podłączanych urządzeń zewnętrznych w zakresie: komputer, data, godzina, kto podłączył, czy urządzenia było podłączane na innym komputerze, czy urządzenie było podłączane przez innego użytkownika);
- vi. Zdalna administracja komputerami:
 1. System ma automatycznie wykonywać dowolne polecenia na dowolnych komputerach: wykonywanie poleceń powłoki, uruchamianie aplikacji, instalacja/deinstalacja oprogramowania, zmiany w rejestrach systemowych (dodawanie, usuwanie, modyfikowanie), usuwanie oraz kopiowanie plików i folderów, dostarczanie wyników zwróconych przez wykonane zadanie do bazy danych i prezentowanie ich w konsoli zarządzającej, możliwość wykonywania zadań z uprawnieniami dowolnego użytkownika;
 2. System musi posiadać predefiniowane zadania (polecenia) możliwe do wykonania zdalnie – niezwłocznie lub zgodnie z harmonogramem o funkcjonalnościach typowego harmonogramu Windows; zadania powinny być podzielone na typy: administracyjne, bezpieczeństwo, konserwacyjne a użytkownik może utworzyć dowolny nowy typ zadania;
 3. Minimalne zadania predefiniowane: wyświetlanie aktywnych połączeń sieciowych, czyszczenie buforu DNS, pobranie listy zalogowanych użytkowników, ping, tracert, pobranie listy procesów, wyłączenie/włączenie komputera, wyłączenie/włączenie usługi, wyłączenie/włączenie/restart zapory Windows, włączenie usługi Windows Update, pobranie zmiennych środowiskowych, opróżnienie kosza, usunięcie plików tymczasowych, wymuszenie sprawdzenia dostępności aktualizacji Windows Update, wymuszenie aktualizacji zasad grup (AD), konserwację dysku twardego;
 4. Każde wykonanie zadania musi mieć odzwierciedlenie w statusie wykonania zadania (poprawne, z błędem) oraz udostępniać informację zwrotną o przebiegu wykonania (godzina, data, status);
 5. System musi umożliwiać zdefiniowanie dowolnego własnego zadania z poziomu konsoli administracyjnej z wykorzystaniem poleceń cmd, Windows PowerShell. System posiada co najmniej 70 predefiniowanych poleceń. System musi umożliwiać użytkownikom automatyczne definiowanie poleceń cmd/PowerShell. Funkcjonalność ta pozwala na wprowadzanie opisów zadanych czynności, a



następnie, wykorzystując zaawansowane algorytmy AI, system automatycznie generuje adekwatne skrypty;

6. System musi wspierać obsługę dowolnych poleceń powłoki na stacjach roboczych (kopiowanie plików, usuwanie plików, przenoszenie plików, zmiana ustawień systemu, wykonywanie programów, instalacja oprogramowania, instalacja poprawek itp.);
7. System musi umożliwić wykonanie poleceń z uprawnieniami dowolnego użytkownika (Uruchom jako);
8. System musi umożliwiać tworzenie zadań cyklicznych dla komputerów;
9. Obsługa zadań cyklicznych definiowanych na podstawie harmonogramu czasowego z podziałem co najmniej na dni, tygodnie, miesiące oraz lata;
10. System musi obsługiwać zadania cykliczne: bez daty końcowej, z końcem cyklu po n wystąpieniach, z końcem cyklu w określonej dacie;

e. Zarządzanie politykami bezpieczeństwa:

- i. System musi monitorować i zapobiegać wyciekom danych (DLP) poprzez bieżące (w czasie rzeczywistym) monitorowanie działań użytkowników wg ściśle zdefiniowanych polityk bezpieczeństwa oraz reguł ich opisujących;
- ii. System musi zapewniać automatyczne uruchamianie ochrony zasobów w czasie rzeczywistym zgodnie ze zdefiniowanymi politykami;
- iii. System musi zapewniać ciągłą ochronę danych niezależnie od położenia komputera (w sieci lokalnej, sieci VPN, poza siecią);
- iv. System musi na bieżąco monitorować i chronić za pomocą odpowiednio zdefiniowanych polityk i reguł dane w ruchu, dane w spoczynku oraz dane w użyciu;
- v. Przez dane w spoczynku rozumie się dane, które nie są (ale mogą być) w ruchu lub w użyciu, wymagają inwentaryzacji i zabezpieczenia;
- vi. Przez dane w użyciu należy rozumieć dane, które są aktywnie przetwarzane przez dowolną aplikację i/lub punkt końcowy (komputer). Przykłady danych w użyciu: edycja dokumentu MS Word, Excel, PowerPoint, edycja pliku tekstowego CSV, TXT, tworzenie pliku, przechwytywanie ekranu (screenshot), kopiowanie / wklejanie danych;
- vii. Przez dane w ruchu należy rozumieć dane, które są przesyłane, np. kopiowanie danych (plików) z dysku sieciowego na nośnik USB, kopiowanie danych (plików) z komputera na komputer, przesyłanie danych e-mailem w treści lub w postaci załącznika, pobieranie danych z serwera FTP, przesyłanie danych za pomocą komunikatora;
- viii. Obiekty docelowe reguł muszą być definiowalne za pomocą parametrów takich jak: nazwa komputera, adres IP, unikatowy identyfikator agenta, status połączenia do systemu (online/offline), zainstalowany system operacyjny, nazwę zalogowanego użytkownika, model komputera, producent komputera, dostawca komputera, budżet, z którego zakupiony został komputer, strukturę organizacyjną;
- ix. Przy definiowaniu obiektów docelowych dla reguł DLP można korzystać ze znaków wieloznacznych;
- x. System musi posiadać funkcjonalności monitorowania, blokowania, powiadomieniu użytkownika o wystąpieniu naruszenia zdefiniowanej polityki oraz pełnego logowania zdarzeń dotyczących polityki dla celów administracyjnych (powiadomienie administratora systemu);
- xi. System musi mieć możliwość konfiguracji i instalacji dowolnej ilości reguł dla dowolnych polityk DLP;



- xii. System musi mieć możliwość czasowej dezaktywacji danej reguły bez jej usuwania i utraty konfiguracji;
- xiii. Nowy komputer zgłaszający się do systemu po raz pierwszy musi bez dodatkowej ingerencji administratora automatycznie pobrać oraz wdrożyć (uruchomić) przeznaczoną dla niego politykę;
- xiv. System musi mieć możliwość określenia ram czasowych działania danej reguły;
- xv. System musi dysponować mechanizmami dostępu do plików na poziomie jądra systemu operacyjnego MS Windows (32-bit i 64-bit), co uniemożliwia obejście zabezpieczeń nawet osobie z uprawnieniami administratora na poziomie systemu operacyjnego;

f. System musi w pełni wspierać następujące polityki ochrony danych:

- i. Zdefiniowanie schematu, w którym można określić, które aplikacje są zabronione, zalecane, dodatkowe bądź nieokreślone. Schemat oprogramowania można przypisać do dowolnej grupy komputerów. Mechanizm musi umożliwić automatyczne odinstalowanie oprogramowania, które wg zdefiniowanego schematu jest zabronione;
- ii. Monitorowanie wykonywanych zrzutów ekranu, blokowanie możliwości zapisania i wykorzystania zrzutów ekranu;
- iii. Przechwytywanie zrzutów ekranu z komputerów użytkowników wyzwalany akcją użytkownika lub na życzenie administratora zgodnie z wcześniej ustawionym interwałem czasowym;
- iv. Umożliwienie powiadamianie o przekroczeniu dozwolonego czasu pracy komputer;
- v. Wyświetlanie komunikatu na komputerach użytkowników podczas uruchamiania stacji roboczej. Komunikaty muszą być definiowalne z poziomu konsoli administracyjnej z wykorzystaniem edytora (możliwość utworzenia tabeli, dołączenia obrazu, wstawienia linku);
- vi. Kontrola i ochrona urządzeń
 - 1. Blokowanie dostępu do wybranych typów urządzeń od strony sprzętowej. Wsparcie dla CD-ROM, portów USB, kart sieciowych, GPS, kart graficznych, modemów, klawiatur, czytników kart, drukarek, urządzeń Bluetooth i innych, monitorowanie podłączanych urządzeń.
 - 2. Blokowanie dostępu do urządzeń USB, tworzenie czarnych list urządzeń, monitorowane podłączanych urządzeń USB.
 - 3. Zarządzanie dostępem do sieci społecznościowych, serwisów informacyjnych, blogów, bibliotek, forów dyskusyjnych oraz dowolnych stron www.
 - 4. Blokowanie sieci ze względu na zdefiniowany typ i maskę sieci WIFI. Polityka musi zapewniać blokowanie dostępu do sieci zarówno otwartych jak i zabezpieczonych.
- vii. Klasyfikacja i ochrona dokumentów
 - 1. Oznaczanie na dowolnym komputerze (znakowanie przez agenta) określonych plików wybranymi, niewidocznymi, dowolnie zdefiniowanymi znacznikami.
 - 2. Znakowanie określonych plików przechowywanych w zasobach serwerów lub udostępnionych zasobach (np. samodzielna macierz dyskowa) wybranymi, niewidocznymi, dowolnie zdefiniowanymi znacznikami, z wykorzystaniem harmonogramu.
 - 3. Monitorowania i blokowania operacji (otwieranie/ usuwanie/ tworzenie/ zapis/ zmiana nazwy) na plikach.
- viii. Ochrona danych w użyciu
 - 1. Podjęcie działania w momencie uruchomienia określonego procesu.
 - 2. Podjęcie działań monitorowania i blokowania operacji w momencie próby kopiowania tekstu, zdjęcia czy ścieżki plików do schowka.



g. Raportowanie i eksport danych:

- i. System musi umożliwiać wyeksportowanie wybranych lub wszystkich danych do formatu .xls, .xlsx, .csv, .calc (OpenOffice), .html, .mht, .xml, .jpeg, .png, .gif, .bmp.;
- ii. System musi umożliwiać generowanie raportów bezpośrednio z każdego widoku w aplikacji z zastosowaniem bieżących filtrów, przy czym generowanie raportu musi odbywać się po stronie serwera www;
- iii. System powinien umożliwiać eksport danych z raportu do formatów: pdf, xls, doc, rtf;
- iv. System musi obsługiwać raporty parametryczne z parametrami statycznymi (wprowadzanymi w momencie generowania raportów) oraz dynamicznymi (pobieranymi z bazy danych w momencie generowania raportu);
- v. System musi istnieć możliwość tworzenia i dodawania własnych raportów przez użytkownika;

h. Bezpieczeństwo:

- i. System musi być wyposażony w mechanizmy definicji praw dostępu do poszczególnych widoków danych i opcji w konsoli administracyjnej:
 1. Uwierzytelnianie do systemu musi być realizowane:
 - a. z wykorzystaniem imiennego konta użytkownika i hasła;
 - b. z wykorzystaniem imiennego konta administratorów aplikacji i hasła;
 - c. za pośrednictwem uwierzytelniania poprzez Active Directory;
 - d. za pośrednictwem uwierzytelniania poprzez CAS;
 2. Hasła w systemie i bazach danych nie mogą w żadnym z przypadków występować w formie jawnej;
 3. Siła hasła musi być definiowalna w zakresie atrybutów: ilość znaków, ilość liter, ilość znaków specjalnych, ilość małych znaków, ilość wielkich znaków, ilość cyfr, ilość znaków specjalnych, ilość znaków alfanumerycznych, lista dopuszczalnych znaków specjalnych, lista wyłączonych znaków);
 4. System musi umożliwiać zastosowanie dodatkowej autentykacji podczas logowania przy użyciu certyfikatu SSL w systemie lub na tokenie (MFA):
 - a. Uwierzytelnianie z wykorzystaniem obrazu wideo;
 - b. Uwierzytelnianie z jednorazowym kodem wysyłanym na e-mail użytkownika;
 - c. Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji kont operatorów w konsoli zarządzającej poprzez fizyczne zabezpieczenie sprzętowe wraz z hasłem, które umożliwia jednoczesną pracę wielu użytkowników. Logowanie użytkowników konsoli zarządzającej musi umożliwiać integrację z kontami Active Directory/LDAP;
 5. Wymagane zabezpieczenie sprzętowe musi posiadać mechanizm szyfrowania w oparciu o RSA 512/1024/RSA 2048 bit, ECDSA 192/256 bit, DES/3DES, AES 128/192/256 bit, SHA-1 / SHA-256;
 - a. Wykorzystywane klucze muszą posiadać wsparcie dla systemów Windows 7/8.1/10/11 i Windows Server 2012/2016/2019/2022;
 6. System musi umożliwiać blokadę dostępu po nieudanej próbie zalogowania się do systemu. Ponadto, system powinien oferować:
 - a. Podgląd wszystkich zablokowanych administratorów systemu, w tym informacje o typie, elemencie, czasie trwania blokady [s] oraz o ostatniej aktywności;
 - b. Możliwość odblokowania zablokowanego administratora systemu z poziomu konsoli administracyjnej przez osobę uprawnioną;

7. Prawa dostępu muszą opierać się na grupach i użytkownikach w zakresie: przeglądanie / edycja / usuwanie/ eksport;
8. System musi oferować możliwość podglądu wszystkich aktualnie otwartych sesji administratorów w konsoli administracyjnej, obejmując takie informacje jak: data utworzenia sesji, login, IP oraz SID a dodatkowo, system powinien umożliwiać wyszukiwanie zalogowanych administratorów po nazwie;
9. System musi udostępniać historię działań wybranych użytkowników/administratorów w zakresie, adresy URL i nagłówki http;
10. System musi posiadać wbudowany mechanizm automatycznej synchronizacji czasu pomiędzy Klientami oraz serwerem, gdzie wzorcowy czas jest po stronie serwera;
11. System musi posiadać mechanizmy automatycznego wykonywania kopii bezpieczeństwa w zadanych interwałach czasowych w formie kopii przyrostowej i nie przyrostowej oraz udostępniać informacje o rezultacie wykonania kopii.
12. System musi pobierać dane z widoków (view) zdefiniowanych w bazie danych a nie bezpośrednio z tabel bazy danych;
13. W przypadku wystąpienia awarii systemu i konieczności instalacji systemu na nowo system musi automatycznie z serwera aktualizacji producenta w ciągu 24 godzin dokonać aktualizacji wszystkich komponentów (konsola administracyjna, agenci, serwer, baza danych, bazy wiedzy);
14. System musi być wyposażony w mechanizmy powtórne załadowania danych historycznych pochodzących od Klientów;
15. System musi zapewniać:
 - a. Pełne logowanie błędów w celu weryfikowania nieprawidłowości;
 - b. Przechowywanie logów systemowych;
 - c. Przechowywanie logów bezpieczeństwa;
 - d. Przechowywanie logów aktywności użytkowników i administratorów;
 - e. Pobieranie logów z Klientów z poziomu konsoli administracyjnej;
 - f. Możliwość eksportu logów;
 - g. Definiowanie maksymalnego czasu przechowywania plików log;
 - h. System musi zapewniać mechanizmy zapewniające integralność, poufność i dostępność przechowywanych informacji;
 - i. Definiowanie ścieżki do kopii zapasowej;
 - j. Definiowanie ścieżki do importu danych;
 - k. Definiowanie ścieżki do zapisu raportów;
 - l. Definiowanie serwera do importu danych;

i. Wsparcie i pomoc:

- i. System musi posiadać dokumentację w postaci min. 5 filmów instruktażowych/nagrań z webinarów w języku polskim.;
- ii. System musi posiadać wbudowaną dokumentację pomocy użytkownika w języku polskim;
- iii. Pomoc techniczna:
 1. Musi być świadczona przez producenta systemu co najmniej w dni robocze w godzinach od 8.00-16.00;
 2. Utrzymaniem Oprogramowania jest zapewnienie aktualizacji Oprogramowania (asysta techniczna) oraz nieprzerwanego działania Oprogramowania (usługi SLA), jak również zapewnienie świadczenia innych usług wspomagających korzystanie z Oprogramowania;

3. Czas trwania usługi SLA wynosi 24 miesiące od dnia zakupu;
4. Usługi Utrzymania Oprogramowania obejmują:
 - a. asystę techniczną;
 - b. świadczenie usług SLA, w ramach, których realizowana jest obsługa zgłoszeń w zakresie:
 1. reakcja na zgłoszenia błędów w określonym czasie reakcji;
 2. dokonywanie analizy przyczyn błędów;
 3. zapewnianie obejścia dla błędów występujących z przyczyn leżących po stronie oprogramowania podmiotów trzecich;
 4. zapewnianie obejścia dla błędów występujących z przyczyn leżących po stronie infrastruktury zamawiającego;
 5. usuwania błędów w czasie naprawy;
 6. usuwania błędów występujących z przyczyn leżących po stronie oprogramowania podmiotów trzecich – po udostępnieniu odpowiedniej aktualizacji przez producenta tego oprogramowania oraz jej uzyskaniu – w czasie naprawy;

VI. Oprogramowanie do inwentaryzacji zasobów informatycznych -- Typ II - 1 licencja ;

a. Architektura / budowa:

- i. System musi zapewnić stabilną obsługę co najmniej 50 klientów jednocześnie;
- ii. Klient – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej;
- iii. Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej);
- iv. Panel pracownika – aplikacja webowa, niewymagająca dodatkowego logowania, dostępna dla pracowników, udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach;
- v. Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z Klientami;
- vi. Baza danych pracująca na silniku Microsoft SQL Server w wersjach wyspecyfikowanych poniżej;
- vii. Komponenty systemu (Klient, konsola administracyjna, serwer, baza danych) aktualizują się automatycznie poprzez bezpieczne połączenie;
- viii. System zawiera mechanizmy automatycznej konserwacji zgodnie z harmonogramem;

b. Wymagania systemowe:

- i. Konsola administracyjna musi działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5;
- ii. Klient musi działać na systemach 32 i 64 bitowych: Windows Server 2012/2012R2/2016/2019/2022, Windows 7/8/8.1/10/11, MacOS 10.7/10.8, Linux dla wersji: Ubuntu v.11.04 lub wyższa, Debian v.6.0 lub wyższa, RedHat v.6.0 lub wyższa, CentOS v.6.0 lub wyższa, Fedora v.16 lub wyższa;
- iii. Klient wspiera poniższe przeglądarki internetowe w zakresie monitorowania aktywności użytkownika w sieci: Opera, Chrome, FireFox;

- iv. Serwer musi działać na systemach 64 bitowych: Windows Server 2016/2019/2022, Windows 7/8/8.1/10/11;
- v. Serwer www musi być oparty o platformę Microsoft 64 bit (Windows Server 2016/2019/2022, Windows 10 oraz Java 8 (JRE lub JDK), Apache Tomcat 9;
- vi. Baza danych musi działać na silniku Microsoft SQL Server 2014/2016/2017/2019/2022 w wersji 64 bitowych bezpłatnym (np. Microsoft SQL Server Express Edition);
- vii. System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare;

c. Interfejsy:

- i. System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie;
- ii. System musi umożliwiać import danych z CSV, Excel, Microsoft SQL Server, MySQL, PostgreSQL;

d. Funkcjonalności systemu zarządzania infrastrukturą IT:

- i. Funkcjonalność Klienta - System musi umożliwiać pełne zdalne zarządzanie Klientami, obejmujące uruchamianie i wyłączenie, zmianę konfiguracji Klienta, inicjowanie skanowania oraz wykonanie poleceń systemowych. Klient powinien wyświetlać komunikaty w HTML z dokładnymi danymi o czasie wyświetlenia i użytkownikowi;
- ii. Funkcjonalność konsoli administracyjnej:
 - 1. Konsola administracyjna musi być dostępna w języku Polskim i oferować intuicyjny interfejs z pełnym zestawem funkcji zarządzania (dodawanie, modyfikowanie, usuwanie). Musi także zawierać różnorodne dashboardy, w tym dashboardy użytkownika, prezentujące parametry infrastruktury, sieci oraz bezpieczeństwa. Użytkownicy powinni mieć możliwość samodzielnego konfigurowania dashboardów użytkownika, a dashboardy sieciowe i bezpieczeństwa muszą zawierać szczegółowe widżety z informacjami o stanie usług i bezpieczeństwie;
 - 2. W konsoli powinna istnieć funkcja filtrowania danych na dashboardach oraz możliwość personalizacji interfejsu przez użytkownika, w tym definiowanie własnych pól, filtrów i widoków, z zachowaniem tych ustawień pomiędzy sesjami. Konsola musi także umożliwiać definiowanie poziomów uprawnień dla użytkowników i grup, z opcją dziedziczenia oraz integrację z Active Directory dla zarządzania dostępem;
 - 3. Konsola powinna posiadać zaawansowane funkcje zarządzania rekordami, w tym wykonanie poleceń na wielu rekordach jednocześnie oraz dostęp do szczegółowych informacji o pracy urządzeń;
- iii. Funkcjonalność panelu pracownika – panel pracownika systemu musi automatycznie uruchamiać się i autoryzować przy logowaniu użytkownika, z możliwością definiowania zakresu dostępnych informacji przez administratora dla poszczególnych grup pracowników. Panel kierownika powinien dodatkowo agregować i analizować dane z paneli pracowników. Informacje w panelu muszą być organizowane w logiczne sekcje, które można indywidualnie lub grupowo włączać i wyłączać przez administratora;
- iv. Zarządzanie licencjami - system musi umożliwiać kompleksowe zarządzanie licencjami w różnych modelach i strukturach organizacyjnych, w tym audyty, zarządzanie oprogramowaniem i oprogramowaniem zabronionym, oraz przypisywanie i rozliczanie

- różnych typów licencji. Musi także rejestrować historię licencji oraz zapewniać funkcje inwentaryzacji i zdalnej dezinstalacji oprogramowania;
- v. Wzorce aplikacji i pakietów - system powinien posiadać rozbudowaną bazę wzorców oprogramowania, umożliwiać definiowanie własnych wzorców i automatycznie importować nowe wzorce od producenta. Musi także dostarczać szczegółowe informacje o zainstalowanych pakietach i ich wykorzystaniu, w tym edycje Microsoft Office;
 - vi. Inwentaryzacja sprzętu komputerowego i urządzeń - system musi oferować rozbudowane funkcje inwentaryzacji sprzętu komputerowego, włączając automatyczną inwentaryzację zarówno w sieci lokalnej jak i zdalnej, szczegółowe skanowanie komponentów (np. RAM, monitory, dyski twarde) oraz zarządzanie informacjami o zainstalowanym sprzęcie. Powinien także umożliwiać ewidencję zmian konfiguracji sprzętu, identyfikować i klasyfikować urządzenia podłączane do komputerów oraz monitorować historię ich podłączeń;
 - vii. Inwentaryzacja urządzeń sieciowych - system musi posiadać zdolności do identyfikacji urządzeniami sieciowymi. Wymagane jest posiadanie skanera sieci i SNMP, które automatycznie zbierają dane, analizują jakość połączeń i identyfikują urządzenia na sieci. System powinien także umożliwiać zdalną instalację Klientów i generowanie map sieci;
 - viii. Inwentaryzacja sprzętu - system musi umożliwiać wszechstronną inwentaryzację sprzętu, włączając urządzenia inne niż komputery (np. drukarki, routery). Musi zapewniać zarządzanie dokumentacją związaną z urządzeniami, monitorować ich ruch oraz przypominać o terminach gwarancji i umowach utrzymaniowych;
 - ix. Ochrona danych (DLP):
 1. Ochrona danych (DLP) musi obejmować automatyczne tworzenie listy podłączanych do komputerów urządzeń USB i ich klasyfikację. System powinien dostarczać informacje o historii użytkowania urządzeń zewnętrznych oraz umożliwiać zarządzanie dozwolonymi do użytku urządzeniami USB zgodnie z zdefiniowanymi regułami;
 2. Szyfrowanie dysków wewnętrznych oraz zewnętrznych;
 3. System musi obsługiwać kompleksowe szyfrowanie dysków wewnętrznych i zewnętrznych USB, z wykorzystaniem BitLocker i różnych metod szyfrowania, takich jak XTS AES 256 i AES 128. Musi umożliwiać zdalne zarządzanie procesem szyfrowania/desyfrowania, w tym masowe operacje na partycjach systemowych i niesystemowych. Klucze szyfrujące są przechowywane i chronione w konsoli administracyjnej, dostępne tylko po uwierzytelnieniu administratora. Proces szyfrowania odbywa się w sposób niewidoczny dla użytkownika i nie może być przez niego przerwany, z wyjątkiem stanów hibernacji i wyłączenia systemu, po których jest automatycznie kontynuowany;
 - x. Zdalna administracja komputerami:
 1. System musi oferować kompleksową zdalną administrację komputerami, włączając w to automatyczne wykonywanie dowolnych poleceń (np. zarządzanie aplikacjami, plikami, rejestrami systemowymi) oraz zarządzanie cyklicznymi zadaniami z harmonogramem. Powinien obsługiwać technologię Intel vPro dla zdalnej konfiguracji i zarządzania, a także pozwalać na zdalne przejęcie kontroli nad komputerem za pomocą technologii Ultra VNC, umożliwiając operowanie na wielu sesjach jednocześnie. System powinien integrować zaawansowane mechanizmy skryptowe wspierane przez AI dla automatycznego generowania poleceń oraz

- umożliwiać zarządzanie i tworzenie zadań cyklicznych z różnorodnymi opcjami cykliczności i zakończenia;
2. System musi zezwalać na wykonywanie zapytań WMI bez zdalnego połączenia do urzędu;
 3. System musi zezwalać na edycję rejestrów urzędu bez wykorzystania zdalnego połączenia pulpitu;
- xi. Zdalne Zarządzanie Zaporą (Firewall) - system musi umożliwiać zdalne zarządzanie zaporą sieciową (firewall) globalnie w infrastrukturze, co obejmuje monitorowanie jej stanu w czasie rzeczywistym, definiowanie złożonych zasad zapory z centralnego panelu administracyjnego oraz szybkie identyfikowanie i reagowanie na potencjalne zagrożenia sieciowe;
- xii. Automatyzacja - system musi oferować możliwość ustalania harmonogramu dla czynności konserwacyjnych, naprawczych i porządkujących, z opcją ustalania częstotliwości i parametrów wejściowych dla każdej czynności oraz możliwością ich zatrzymania lub uruchomienia. Dodatkowo, system musi posiadać mechanizmy automatyzacji takie jak wykonywanie kopii bezpieczeństwa, identyfikacja aplikacji i pakietów, porządkowanie bazy danych oraz usuwanie nadmiarowych danych. System również powinien wysyłać alerty o zdarzeniach takich jak nowe komputery w bazie danych, braki w licencjach i inne zdarzenia krytyczne dla infrastruktury IT;
- xiii. Zarządzanie magazynem IT - system musi umożliwiać efektywne zarządzanie magazynem IT, włączając obsługę dowolnej ilości magazynów w różnych lokalizacjach oraz obsługę dokumentów magazynowych typu PZ, RW, WZ, i inne. System powinien prowadzić ewidencję materiałów w magazynach zgodnie z metodą FIFO. Ponadto, system powinien umożliwiać automatyczne łączenie dokumentów magazynowych z zasobami systemu oraz zapewniać przegląd wszystkich dokumentów;
- xiv. Repozytorium - konsola administracyjna systemu musi być wyposażona w repozytorium dokumentów dowolnego typu, które umożliwia dodawanie nowych dokumentów, przeszukiwanie. Repozytorium powinno także umożliwiać definiowanie kontenerów na dokumenty, co ułatwia organizację i zarządzanie dokumentacją;
- xv. Kody kreskowe - system musi wspierać obsługę kodów kreskowych jedno i dwuwymiarowych, umożliwiając parametryzację kodu pod względem wielkości i atrybutów graficznych. System powinien umożliwiać podgląd oraz wydruk kodów kreskowych;
- xvi. Wysyłanie wiadomości - system musi oferować funkcję komunikatora, umożliwiającą bezpośrednią wymianę wiadomości między użytkownikami a administratorem systemu, w tym inicjowanie czatu przez administratora oraz przechowywanie historii konwersacji. System powinien także umożliwiać wysyłanie jednorazowych wiadomości ALERT oraz tworzenie szablonów wiadomości do regularnego użytku, z opcją konfiguracji terminu, po którym wiadomość wygaśnie. Ponadto, system powinien wspierać szkolenie pracowników za pomocą wiadomości tekstowych z możliwością definiowania treści szkoleniowych i automatycznego ich wysyłania;
- xvii. System musi posiadać możliwość eksportu / importu treści;
- xviii. Monitorowanie drukarek sieciowych i wydruków - system musi umożliwić monitorowanie i zarządzanie wydrukami z dowolnej drukarki (lokalnej czy sieciowej), rejestrując szczegółowe informacje o każdym wydruku, w tym koszty, dzięki wbudowanemu cennikowi. System powinien również prognozować przyszłe koszty



- drukowania oraz pozwalając na zarządzanie drukarkami według różnych parametrów, w tym statusu i materiałów eksploatacyjnych;
- xix. Monitorowanie stron WWW - system musi oferować monitorowanie aktywności internetowej użytkowników na różnych przeglądarkach, nawet przy szyfrowanych połączeniach (https), rejestrując detale takie jak adresy IP, czas połączenia, a także analizując treści stron za pomocą algorytmów sztucznej inteligencji do klasyfikacji i kontroli treści;
 - xx. Monitorowanie serwerów WWW - system musi zapewniać monitorowanie wybranych serwerów WWW, prezentując informacje o ich statusie i aktywności, umożliwiając analizę treści stron oraz graficzną prezentację danych związanych z ich działaniem, w tym czasem odpowiedzi i aktywnością w określonym okresie;
 - xxi. Monitorowanie dziennika zdarzeń - system musi posiadać zdolność do monitorowania dziennika zdarzeń komputerów, umożliwiając definiowanie i filtrowanie zdarzeń według różnych kategorii;
 - xxii. Monitorowanie pracy komputerów - system musi oferować monitorowanie pracy komputerów, w tym dat startu i zakończenia pracy, logowania użytkowników, a także zdalne monitorowanie sesji połączeń, rejestrując szczegóły takie jak adresy IP i dane użytkowników;
 - xxiii. Monitorowanie uprawnień ACL - system musi umożliwić skanowanie i monitorowanie uprawnień ACL, oferując szczegółowe raporty, automatyczną aktualizacją danych i filtrami do zarządzania informacjami;
 - xxiv. Monitorowanie sensorów - system musi integrować monitoring warunków środowiskowych za pomocą sensorów po SNMP, umożliwiając graficzną prezentację danych, wysyłanie alertów;
 - xxv. Repozytorium CMDB - system musi posiadać zintegrowane repozytorium CMDB, umożliwiające zarządzanie zasobami IT, w tym szczegółowe informacje o użytkownikach, urządzeniach, licencjach, a także o oprogramowaniu i jego licencjach, z możliwością importu i eksportu danych;
 - xxvi. Zarządzanie czasem pracy użytkowników - system musi umożliwiać monitorowanie i analizę czasu pracy użytkowników, z możliwością definiowania grup przypisanych do przełożonych i prezentacji szczegółowych danych o aktywności użytkowników w formie widżetów i danych analitycznych. Informacje o czasie pracy, sesjach, aktywności w aplikacjach oraz produktywności powinny być możliwe do udostępnienia w panelu pracownika;
 - xxvii. Raportowanie i eksport danych - System musi oferować zaawansowane możliwości raportowania i eksportu danych, umożliwiając wyeksportowanie informacji do różnych formatów, w tym xls, csv, html, oraz graficznych. Powinien także wspierać generowanie wieloparametrycznych raportów z możliwością stosowania filtrów, obsługę wieloinstancyjności raportowania oraz integrację z narzędziami do tworzenia raportów takimi jak SAP Crystal Reports i Stimulsoft, obejmując co najmniej 150 zdefiniowanych raportów. Dodatkowo, system musi posiadać możliwość konfiguracji harmonogramu umożliwiającego cykliczne wysyłanie raportów oraz zapisywanie ich w dowolnym miejscu, z automatycznym generowaniem raportu w formacie PDF jako wynikiem wykonania harmonogramu;
 - xxviii. System musi zapewnić interfejs API - system musi oferować rozbudowany interfejs API, umożliwiający komunikację za pomocą REST API. Musi on zapewniać szyfrowaną komunikację z użyciem protokołu TLS 1.3 oraz możliwość tworzenia złożonych



requestów JSON. Klucze zabezpieczeń powinny być modyfikowalne i mogą mieć co najmniej 32 znaki;

- xxix. Powiadomienia - system musi umożliwiać generowanie różnorodnych powiadomień, w tym alertów w konsoli, e-maili oraz wiadomości SMS, z możliwością edycji treści powiadomień i definiowania grup odbiorców. Powinien obsługiwać automatyczne wywoływanie zadań i integrować się z CMD oraz Windows PowerShell, zapewniając co najmniej 30 predefiniowanych powiadomień oraz możliwość ich personalizacji;
- xxx. Bezpieczeństwo - system musi zapewniać rozbudowane funkcje bezpieczeństwa, w tym definicję i zarządzanie prawami dostępu oraz zaawansowane opcje uwierzytelniania. Wymaga silnych haseł, obsługuje wieloskładnikowe uwierzytelnianie i posiada mechanizmy szyfrowania danych;
- xxxi. Wsparcie i pomoc techniczna producenta systemu
 1. Pomoc techniczna - musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00;
 2. Utrzymaniem Oprogramowania jest zapewnienie aktualizacji Oprogramowania (asysta techniczna) oraz nieprzerwanego działania Oprogramowania (usługi SLA), jak również zapewnienie świadczenia innych usług wspomagających korzystanie z Oprogramowania;
 3. Czas trwania usługi SLA wynosi 24 miesięcy od dnia zakupu;

VII. Oprogramowanie kryptograficzne i analityczne – moduł w pełni kompatybilny z zaoferowanym oprogramowaniem w pkt. VI integrujący informację dotyczące zakresu DLP z wizualizacją w systemie podstawowym z pkt. VI – Typ II – 1 licencja;

a. Architektura / budowa:

- i. System musi zapewnić stabilną obsługę co najmniej 50 klientów jednocześnie;
- ii. Czas aktualizacji wszystkich komponentów systemu: serwer, konsola administracyjna, baza danych, agenci - nie może przekroczyć 24h od wydania przez producenta nowej wersji dowolnego komponentu. Agenci na komputerach muszą się zaktualizować samodzielnie w czasie nie dłuższym niż 8h od pobrania aktualizacji od producenta, przy czym aktualizacja klientów musi przebiegać w pełni automatycznie z wykorzystaniem funkcjonalności wbudowanej w system (bez użycia zewnętrznych narzędzi, np. MS Active Directory). W przypadku, gdy połączenie pomiędzy systemem a serwerem aktualizacji producenta nie jest dostępne musi być możliwość dokonania aktualizacji manualnie poprzez pobranie od producenta paczki aktualizacyjnej w postaci jednego pliku z kompletną aktualizacją;
- iii. System musi w sposób w pełni automatyczny z wykorzystaniem serwera aktualizacji producenta aktualizować wzorce aplikacji, polityk, pomoc i inne wbudowane bazy wiedzy;
- iv. Klient musi być dostępny dla administratora z poziomu webowej interfejsu konsoli administracyjnej zawsze w najnowszej wersji wydanej przez producenta (bez konieczności pobierania go od producenta), w postaci pliku *.msi gotowego do zainstalowania (bez konieczności dodatkowego wykonywania zmian/ustalania parametrów) w pliku *.msi;
- v. Klient musi być możliwy do zainstalowania za pośrednictwem MS Active Directory, za pomocą skryptów lub manualnie, poprzez uruchomienie na danej stacji roboczej;
- vi. System zapewnia możliwość stworzenia instalatora (.exe) z wbudowanymi, zaszyfrowanymi poświadczeniami dla dowolnego konta. Funkcja ta umożliwi instalację usługi bezpośrednio na kontach użytkowników – zarówno lokalnych, jak i domenowych, korzystając z uprawnień zdefiniowanych dla instalatora w konsoli systemu;
- vii. Klient musi pracować w trybie niewidocznym dla użytkownika (usługa systemowa);
- viii. System powinien umożliwiać generowanie unikatowego identyfikatora Klienta – wygenerowanego losowo i unikatowo (np. za pomocą mechanizmu typu GUID) lub w sposób powtarzalny dla danego komputera) na podstawie kombinacji parametrów wybranych przez użytkownika systemu spośród następujących: nazwy producenta BIOS, numeru seryjnego komputera, system UUID, nazwy komputera, dowolnego oraz losowego ciągu znaków;
- ix. Klient musi mieć definiowalny priorytet pracy procesu w systemie operacyjnym (ABOVE_NORMAL, NORMAL, BELOW_NORMAL, IDLE), przy czym w każdym momencie administrator może automatycznie z poziomu konsoli administracyjnej systemu wydać polecenie zmiany tej konfiguracji na dowolnej grupie komputerów;
- x. Klient musi wspierać wiele różnych adresów serwera rozumianych jako adresy w sieci lokalnej, rozległej (VPN) oraz za NATem i potrafić wykorzystać adres dostępny (na którym następuje połączenie z serwerem) w dowolnym momencie działania, bez konieczności restartu Klienta;



- xi. System musi mieć możliwość współpracy komponentów klienta i serwera w taki sposób, aby serwer mógł współpracować ze wszystkimi poprzednimi wersjami Klientów;
- b. System musi mieć wbudowane mechanizmy automatycznej konserwacji/utrzymania zgodnie ze zdefiniowanym harmonogramem:**
 - i. Automaty powinny realizować co najmniej usuwanie zbędnych danych z systemu (dane z monitoringu uruchamianych aplikacji, uruchamianych procesów, odwiedzonych stron www, wydrukowanych dokumentów, indeksowanie bazy danych, kopie bezpieczeństwa przyrostowe i nie przyrostowe, zmniejszanie bazy danych);
 - ii. Harmonogram musi mieć możliwość ustalenia częstotliwości wykonywania zadania (godzina, dzień, tydzień, miesiąc), możliwość zmiany wartości parametrów wejściowych do wykonania danej konserwacji, a także zatrzymania/uruchomienia wybranych pozycji harmonogramu w dowolnym momencie;
- c. Interfejsy:**
 - i. System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie;
 - ii. Import obiektów z MS Active Directory musi być odporny na zmianę nazw obiektów (nazwy użytkownika, struktury organizacyjnej itp.) – podczas import zmienione dane muszą zostać odpowiednio zaktualizowane wg klucza UUID;
 - iii. Import z Active Directory musi wspierać obsługę protokołów SSL oraz TLS;
 - iv. Import z Active Directory musi umożliwiać podanie więcej niż jednej domeny;
 - v. System musi umożliwiać import użytkowników z zewnętrznego pliku CSV;
 - vi. System musi posiadać wbudowany, w pełni definiowalny przez administratora interfejs do importu innych niż komputery urządzeń (np. pendrive, monitory, switche itp.) wraz z danymi o kosztach zakupu, nr dokumentu zakupowego, dostawcy, daty zakupu, gwarancji. Interfejs dodatkowo musi umożliwiać importowanie użytkowników, struktur i licencji. Import musi umożliwiać pobieranie danych z CSV, Excel, Microsoft SQL Server, MySQL, PostgreSQL z wykorzystaniem sterownika ODBC (np. z pliku tekstowego, pliku xls, pliku xml) w sposób jednorazowy lub zgodnie ze zdefiniowanym harmonogramem. Import aktualizuje te same dane wcześniej zaimportowane;
- d. Funkcjonalności systemu:**
 - i. Funkcjonalność konsoli administracyjnej:
 1. Konsola musi być w pełni polskojęzyczna;
 2. Interfejs konsoli musi być wyposażony w intuicyjne mechanizmy obsługi, musi zapewniać pełną obsługę funkcjonalną (dodawanie/modyfikacja/usuwanie);
 3. Konsola administracyjna musi posiadać dashboard – dashboard użytkownika, dashboard prezentujący parametry infrastruktury, dashboard prezentujący parametry sieci, dashboard prezentujący informacje o bezpieczeństwie;
 4. Konsola administracyjna musi być wyposażona w panel zawierający graficzne widżety prezentujące dane w postaci wykresu kołowego i słupkowego bądź w formie tabeli z danymi;
 5. Dane na widżetach muszą być aktualizowane automatycznie;
 6. System musi umożliwiać i zapamiętywać w profilu użytkownika indywidualną personalizację interfejsu konsoli administracyjnej (wybór wyświetlanych kolumn, ich kolejność, język, definiowanie filtrów, kolejność sortowania, wyświetlane widżety, ich konfigurację i kolejność);

7. Dane prezentowane na wszystkich widokach/zakładkach w systemie muszą być dynamicznie filtrowane w oparciu o reguły utworzone przez dowolnego użytkownika systemu;
 8. Dane prezentowane na wszystkich widokach/zakładkach w systemie muszą mieć możliwość filtrowania kolumnowego;
 9. System musi umożliwiać definiowanie poziomu uprawnień dla grupy oraz użytkownika (odczyt, usuwanie, modyfikowanie, wydruk) do wszystkich widoków danych oraz wybranych elementów struktury organizacyjnej, musi być wyposażony w opcję dziedziczenia uprawnień. Odebranie praw do widoku lub zakładki na widoku powoduje ukrycie opcji;
 10. Lista użytkowników / administratorów systemu musi być importowana i aktualizowana zgodnie z harmonogramem w oparciu o mechanizm RBAC (Role Base Access Control) z wybranego obiektu Active Directory. Użytkownik wyłączony/usunięty/zablokowany w Active Directory automatycznie traci prawa do korzystania z konsoli administracyjnej systemu;
 11. Konsola musi umożliwiać wykonywanie poszczególnych poleceń na wielu rekordach, w szczególności na wszystkich rekordach, również tych, które nie są widoczne w konsoli w ramach jednej strony (zaznacz wszystko);
 12. Konsola administracyjna musi zawierać szczegółowe informacje dotyczące pracy wszystkich komputerów: wersja Klienta, stanu Klienta (włączony/wyłączony), zalogowanego użytkownika, historii czasu włączenia i wyłączenia komputera;
 13. Konsola musi zawierać w sobie pełną dokumentację systemu;
- ii. Odczytywanie zainstalowanego oprogramowania - system powinien prezentować podgląd zainstalowanych systemów operacyjnych, pakietów oraz aplikacji na komputerach z informacjami o: nazwie, wersji, producencie, typie licencji;
- iii. Wzorce aplikacji i pakietów:
1. System ma posiadać wbudowaną bazę wzorców dostawcy oprogramowania posiadającą co najmniej 4 tys. wzorców aplikacji, 1,3 tys. Producentów;
 2. System musi posiadać możliwość definiowania własnych wzorców aplikacji i pakietów (składających się z aplikacji) w oparciu o definiowalne reguły rozpoznawania;
 3. Własne wzorce aplikacji i pakietów muszą mieć pierwszeństwo w procesie rozpoznawania aplikacji i pakietów;
- iv. Inwentaryzacja sprzętu komputerowego:
1. System prowadzi szczegółową ewidencję zmian konfiguracji sprzętu;
 2. System udostępnia informacje o występowaniu plików na komputerach (nazwa, rozmiar, rodzaj, wielkość, lokalizacja, w przypadku plików wykonywalnych: wersja, producent);
 3. System musi umożliwiać dokonanie klasyfikacji pliku wg dowolnie zdefiniowanych kategorii (np. audio, wideo, graficzne, erotyczne/pornograficzne, archiwa, wykonywalne);
 4. System pozwala na zdalne trwałe (bez możliwości odzyskania) usunięcie dowolnego pliku/plików na dowolnie zdefiniowanej grupie komputerów;
 5. System udostępnia informacje o zmianach w systemie plików (dodano plik, usunięto plik);
 6. System umożliwia dodawanie notatek do każdej pozycji sprzętu;

7. System musi umożliwiać ewidencję zdarzeń serwisowych dowolnego typu (np. naprawy sprzętu, wymiany części):
 - a. System musi umożliwiać definiowanie typów serwisów;
 - b. System musi umożliwiać definiowanie wartości serwisu;
 - c. System musi umożliwiać definiowanie daty ważności serwisu oraz daty gwarancji;
8. System musi pozwalać na dołączanie do urządzeń dokumentów z repozytorium;
9. System umożliwia samodzielną definicję, ewidencję oraz wydruk wszelkiego typu protokołów (przyjęcie, przekazanie do użytkownika, likwidacja);
- v. Inwentaryzacja urządzeń podłączanych do komputera:
 1. System automatycznie identyfikuje i klasyfikuje urządzenia podłączane do komputera (pendrive, kamera, aparat, monitor zewnętrzny, pamięć masowa, telefon, urządzenie multimedialne itp.);
 2. System pozwala na automatycznie lub ręczne przypisanie podłączonego urządzenia do komputera oraz użytkownika;
 3. System ewidencjonuje historię podłączanych urządzeń zewnętrznych w zakresie: komputer, data, godzina, kto podłączył, czy urządzenia było podłączane na innym komputerze, czy urządzenie było podłączane przez innego użytkownika);
- vi. Zdalna administracja komputerami:
 1. System ma automatycznie wykonywać dowolne polecenia na dowolnych komputerach: wykonywanie poleceń powłoki, uruchamianie aplikacji, instalacja/deinstalacja oprogramowania, zmiany w rejestrach systemowych (dodawanie, usuwanie, modyfikowanie), usuwanie oraz kopiowanie plików i folderów, dostarczanie wyników zwróconych przez wykonane zadanie do bazy danych i prezentowanie ich w konsoli zarządzającej, możliwość wykonywania zadań z uprawnieniami dowolnego użytkownika;
 2. System musi posiadać predefiniowane zadania (polecenia) możliwe do wykonania zdalnie – niezwłocznie lub zgodnie z harmonogramem o funkcjonalnościach typowego harmonogramu Windows; zadania powinny być podzielone na typy: administracyjne, bezpieczeństwo, konserwacyjne a użytkownik może utworzyć dowolny nowy typ zadania;
 3. Minimalne zadania predefiniowane: wyświetlanie aktywnych połączeń sieciowych, czyszczenie buforu DNS, pobranie listy zalogowanych użytkowników, ping, tracert, pobranie listy procesów, wyłączenie/włączenie komputera, wyłączenie/włączenie usługi, wyłączenie/włączenie/restart zapory Windows, włączenie usługi Windows Update, pobranie zmiennych środowiskowych, opróżnienie kosza, usunięcie plików tymczasowych, wymuszenie sprawdzenia dostępności aktualizacji Windows Update, wymuszenie aktualizacji zasad grup (AD), konserwację dysku twardego;
 4. Każde wykonanie zadania musi mieć odzwierciedlenie w statusie wykonania zadania (poprawne, z błędem) oraz udostępniać informację zwrotną o przebiegu wykonania (godzina, data, status);
 5. System musi umożliwiać zdefiniowanie dowolnego własnego zadania z poziomu konsoli administracyjnej z wykorzystaniem poleceń cmd, Windows PowerShell. System posiada co najmniej 70 predefiniowanych poleceń. System musi umożliwiać użytkownikom automatyczne definiowanie poleceń cmd/PowerShell. Funkcjonalność ta pozwala na wprowadzanie opisów zadanych czynności, a

następnie, wykorzystując zaawansowane algorytmy AI, system automatycznie generuje adekwatne skrypty;

6. System musi wspierać obsługę dowolnych poleceń powłoki na stacjach roboczych (kopiowanie plików, usuwanie plików, przenoszenie plików, zmiana ustawień systemu, wykonywanie programów, instalacja oprogramowania, instalacja poprawek itp.);
7. System musi umożliwić wykonanie poleceń z uprawnieniami dowolnego użytkownika (Uruchom jako);
8. System musi umożliwiać tworzenie zadań cyklicznych dla komputerów;
9. Obsługa zadań cyklicznych definiowanych na podstawie harmonogramu czasowego z podziałem co najmniej na dni, tygodnie, miesiące oraz lata;
10. System musi obsługiwać zadania cykliczne: bez daty końcowej, z końcem cyklu po n wystąpieniach, z końcem cyklu w określonej dacie;

e. Zarządzanie politykami bezpieczeństwa:

- i. System musi monitorować i zapobiegać wyciekom danych (DLP) poprzez bieżące (w czasie rzeczywistym) monitorowanie działań użytkowników wg ściśle zdefiniowanych polityk bezpieczeństwa oraz reguł ich opisujących;
- ii. System musi zapewniać automatyczne uruchamianie ochrony zasobów w czasie rzeczywistym zgodnie ze zdefiniowanymi politykami;
- iii. System musi zapewniać ciągłą ochronę danych niezależnie od położenia komputera (w sieci lokalnej, sieci VPN, poza siecią);
- iv. System musi na bieżąco monitorować i chronić za pomocą odpowiednio zdefiniowanych polityk i reguł dane w ruchu, dane w spoczynku oraz dane w użyciu;
- v. Przez dane w spoczynku rozumie się dane, które nie są (ale mogą być) w ruchu lub w użyciu, wymagają inwentaryzacji i zabezpieczenia;
- vi. Przez dane w użyciu należy rozumieć dane, które są aktywnie przetwarzane przez dowolną aplikację i/lub punkt końcowy (komputer). Przykłady danych w użyciu: edycja dokumentu MS Word, Excel, PowerPoint, edycja pliku tekstowego CSV, TXT, tworzenie pliku, przechwytywanie ekranu (screenshot), kopiowanie / wklejanie danych;
- vii. Przez dane w ruchu należy rozumieć dane, które są przesyłane, np. kopiowanie danych (plików) z dysku sieciowego na nośnik USB, kopiowanie danych (plików) z komputera na komputer, przesyłanie danych e-mailem w treści lub w postaci załącznika, pobieranie danych z serwera FTP, przesyłanie danych za pomocą komunikatora;
- viii. Obiekty docelowe reguł muszą być definiowalne za pomocą parametrów takich jak: nazwa komputera, adres IP, unikatowy identyfikator agenta, status połączenia do systemu (online/offline), zainstalowany system operacyjny, nazwę zalogowanego użytkownika, model komputera, producent komputera, dostawca komputera, budżet, z którego zakupiony został komputer, strukturę organizacyjną;
- ix. Przy definiowaniu obiektów docelowych dla reguł DLP można korzystać ze znaków wieloznacznych;
- x. System musi posiadać funkcjonalności monitorowania, blokowania, powiadomieniu użytkownika o wystąpieniu naruszenia zdefiniowanej polityki oraz pełnego logowania zdarzeń dotyczących polityki dla celów administracyjnych (powiadomienie administratora systemu);
- xi. System musi mieć możliwość konfiguracji i instalacji dowolnej ilości reguł dla dowolnych polityk DLP;

- xii. System musi mieć możliwość czasowej dezaktywacji danej reguły bez jej usuwania i utraty konfiguracji;
- xiii. Nowy komputer zgłaszający się do systemu po raz pierwszy musi bez dodatkowej ingerencji administratora automatycznie pobrać oraz wdrożyć (uruchomić) przeznaczoną dla niego politykę;
- xiv. System musi mieć możliwość określenia ram czasowych działania danej reguły;
- xv. System musi dysponować mechanizmami dostępu do plików na poziomie jądra systemu operacyjnego MS Windows (32-bit i 64-bit), co uniemożliwia obejście zabezpieczeń nawet osobie z uprawnieniami administratora na poziomie systemu operacyjnego;

f. System musi w pełni wspierać następujące polityki ochrony danych:

- i. Zdefiniowanie schematu, w którym można określić, które aplikacje są zabronione, zalecane, dodatkowe bądź nieokreślone. Schemat oprogramowania można przypisać do dowolnej grupy komputerów. Mechanizm musi umożliwić automatyczne odinstalowanie oprogramowania, które wg zdefiniowanego schematu jest zabronione;
- ii. Monitorowanie wykonywanych zrzutów ekranu, blokowanie możliwości zapisania i wykorzystania zrzutów ekranu;
- iii. Przechwytywanie zrzutów ekranu z komputerów użytkowników wyzwalany akcją użytkownika lub na życzenie administratora zgodnie z wcześniej ustawionym interwałem czasowym;
- iv. Umożliwienie powiadamianie o przekroczeniu dozwolonego czasu pracy komputer;
- v. Wyświetlanie komunikatu na komputerach użytkowników podczas uruchamiania stacji roboczej. Komunikaty muszą być definiowalne z poziomu konsoli administracyjnej z wykorzystaniem edytora (możliwość utworzenia tabeli, dołączenia obrazu, wstawienia linku);
- vi. Kontrola i ochrona urządzeń
 - 1. Blokowanie dostępu do wybranych typów urządzeń od strony sprzętowej. Wsparcie dla CD-ROM, portów USB, kart sieciowych, GPS, kart graficznych, modemów, klawiatur, czytników kart, drukarek, urządzeń Bluetooth i innych, monitorowanie podłączanych urządzeń.
 - 2. Blokowanie dostępu do urządzeń USB, tworzenie czarnych list urządzeń, monitorowane podłączanych urządzeń USB.
 - 3. Zarządzanie dostępem do sieci społecznościowych, serwisów informacyjnych, blogów, bibliotek, forów dyskusyjnych oraz dowolnych stron www.
 - 4. Blokowanie sieci ze względu na zdefiniowany typ i maskę sieci WIFI. Polityka musi zapewniać blokowanie dostępu do sieci zarówno otwartych jak i zabezpieczonych.
- vii. Klasyfikacja i ochrona dokumentów
 - 1. Oznaczanie na dowolnym komputerze (znakowanie przez agenta) określonych plików wybranymi, niewidocznymi, dowolnie zdefiniowanymi znacznikami.
 - 2. Znakowanie określonych plików przechowywanych w zasobach serwerów lub udostępnionych zasobach (np. samodzielna macierz dyskowa) wybranymi, niewidocznymi, dowolnie zdefiniowanymi znacznikami, z wykorzystaniem harmonogramu.
 - 3. Monitorowania i blokowania operacji (otwieranie/ usuwanie/ tworzenie/ zapis/ zmiana nazwy) na plikach.
- viii. Ochrona danych w użyciu
 - 1. Podjęcie działania w momencie uruchomienia określonego procesu.
 - 2. Podjęcie działań monitorowania i blokowania operacji w momencie próby kopiowania tekstu, zdjęcia czy ścieżki plików do schowka.



g. Raportowanie i eksport danych:

- i. System musi umożliwiać wyeksportowanie wybranych lub wszystkich danych do formatu .xls, .xlsx, .csv, .calc (OpenOffice), .html, .mht, .xml, .jpeg, .png, .gif, .bmp.;
- ii. System musi umożliwiać generowanie raportów bezpośrednio z każdego widoku w aplikacji z zastosowaniem bieżących filtrów, przy czym generowanie raportu musi odbywać się po stronie serwera www;
- iii. System powinien umożliwiać eksport danych z raportu do formatów: pdf, xls, doc, rtf;
- iv. System musi obsługiwać raporty parametryczne z parametrami statycznymi (wprowadzanymi w momencie generowania raportów) oraz dynamicznymi (pobieranymi z bazy danych w momencie generowania raportu);
- v. System musi istnieć możliwość tworzenia i dodawania własnych raportów przez użytkownika;

h. Bezpieczeństwo:

- i. System musi być wyposażony w mechanizmy definicji praw dostępu do poszczególnych widoków danych i opcji w konsoli administracyjnej:
 1. Uwierzytelnianie do systemu musi być realizowane:
 - a. z wykorzystaniem imiennego konta użytkownika i hasła;
 - b. z wykorzystaniem imiennego konta administratorów aplikacji i hasła;
 - c. za pośrednictwem uwierzytelniania poprzez Active Directory;
 - d. za pośrednictwem uwierzytelniania poprzez CAS;
 2. Hasła w systemie i bazach danych nie mogą w żadnym z przypadków występować w formie jawnej;
 3. Siła hasła musi być definiowalna w zakresie atrybutów: ilość znaków, ilość liter, ilość znaków specjalnych, ilość małych znaków, ilość wielkich znaków, ilość cyfr, ilość znaków specjalnych, ilość znaków alfanumerycznych, lista dopuszczalnych znaków specjalnych, lista wyłączonych znaków);
 4. System musi umożliwiać zastosowanie dodatkowej autentykacji podczas logowania przy użyciu certyfikatu SSL w systemie lub na tokenie (MFA):
 - a. Uwierzytelnianie z wykorzystaniem obrazu wideo;
 - b. Uwierzytelnianie z jednorazowym kodem wysłanym na e-mail użytkownika;
 - c. Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji kont operatorów w konsoli zarządzającej poprzez fizyczne zabezpieczenie sprzętowe wraz z hasłem, które umożliwia jednoczesną pracę wielu użytkownikom. Logowanie użytkowników konsoli zarządzającej musi umożliwiać integrację z kontami Active Directory/LDAP;
 5. Wymagane zabezpieczenie sprzętowe musi posiadać mechanizm szyfrowania w oparciu o RSA 512/1024/RSA 2048 bit, ECDSA 192/256 bit, DES/3DES, AES 128/192/256 bit, SHA-1 / SHA-256;
 - a. Wykorzystywane klucze muszą posiadać wsparcie dla systemów Windows 7/8.1/10/11 i Windows Server 2012/2016/2019/2022;
 6. System musi umożliwiać blokadę dostępu po nieudanej próbie zalogowania się do systemu. Ponadto, system powinien oferować:
 - a. Podgląd wszystkich zablokowanych administratorów systemu, w tym informacje o typie, elemencie, czasie trwania blokady [s] oraz o ostatniej aktywności;
 - b. Możliwość odblokowania zablokowanego administratora systemu z poziomu konsoli administracyjnej przez osobę uprawnioną;



7. Prawa dostępu muszą opierać się na grupach i użytkownikach w zakresie: przeglądanie / edycja / usuwanie/ eksport;
8. System musi oferować możliwość podglądu wszystkich aktualnie otwartych sesji administratorów w konsoli administracyjnej, obejmując takie informacje jak: data utworzenia sesji, login, IP oraz SID a dodatkowo, system powinien umożliwiać wyszukiwanie zalogowanych administratorów po nazwie;
9. System musi udostępniać historię działań wybranych użytkowników/administratorów w zakresie, adresy URL i nagłówki http;
10. System musi posiadać wbudowany mechanizm automatycznej synchronizacji czasu pomiędzy Klientami oraz serwerem, gdzie wzorcowy czas jest po stronie serwera;
11. System musi posiadać mechanizmy automatycznego wykonywania kopii bezpieczeństwa w zadanych interwałach czasowych w formie kopii przyrostowej i nie przyrostowej oraz udostępniać informacje o rezultacie wykonania kopii.
12. System musi pobierać dane z widoków (view) zdefiniowanych w bazie danych a nie bezpośrednio z tabel bazy danych;
13. W przypadku wystąpienia awarii systemu i konieczności instalacji systemu na nowo system musi automatycznie z serwera aktualizacji producenta w ciągu 24 godzin dokonać aktualizacji wszystkich komponentów (konsola administracyjna, agenci, serwer, baza danych, bazy wiedzy);
14. System musi być wyposażony w mechanizmy powtórnej załadunku danych historycznych pochodzących od Klientów;
15. System musi zapewniać:
 - a. Pełne logowanie błędów w celu weryfikowania nieprawidłowości;
 - b. Przechowywanie logów systemowych;
 - c. Przechowywanie logów bezpieczeństwa;
 - d. Przechowywanie logów aktywności użytkowników i administratorów;
 - e. Pobieranie logów z Klientów z poziomu konsoli administracyjnej;
 - f. Możliwość eksportu logów;
 - g. Definiowanie maksymalnego czasu przechowywania plików log;
 - h. System musi zapewniać mechanizmy zapewniające integralność, poufność i dostępność przechowywanych informacji;
 - i. Definiowanie ścieżki do kopii zapasowej;
 - j. Definiowanie ścieżki do importu danych;
 - k. Definiowanie ścieżki do zapisu raportów;
 - l. Definiowanie serwera do importu danych;

i. Wsparcie i pomoc:

- i. System musi posiadać dokumentację w postaci min. 5 filmów instruktażowych/nagrań z webinarów w języku polskim.;
- ii. System musi posiadać wbudowaną dokumentację pomocy użytkownika w języku polskim;
- iii. Pomoc techniczna:
 1. Musi być świadczona przez producenta systemu co najmniej w dni robocze w godzinach od 8.00-16.00;
 2. Utrzymaniem Oprogramowania jest zapewnienie aktualizacji Oprogramowania (asysta techniczna) oraz nieprzerwanego działania Oprogramowania (usługi SLA), jak również zapewnienie świadczenia innych usług wspomagających korzystanie z Oprogramowania;



3. Czas trwania usługi SLA wynosi 24 miesiące od dnia zakupu;
4. Usługi Utrzymania Oprogramowania obejmują:
 - a. asystę techniczną;
 - b. świadczenie usług SLA, w ramach, których realizowana jest obsługa zgłoszeń w zakresie:
 1. reakcja na zgłoszenia błędów w określonym czasie reakcji;
 2. dokonywanie analizy przyczyn błędów;
 3. zapewnianie obejścia dla błędów występujących z przyczyn leżących po stronie oprogramowania podmiotów trzecich;
 4. zapewnianie obejścia dla błędów występujących z przyczyn leżących po stronie infrastruktury zamawiającego;
 5. usuwania błędów w czasie naprawy;
 6. usuwania błędów występujących z przyczyn leżących po stronie oprogramowania podmiotów trzecich – po udostępnieniu odpowiedniej aktualizacji przez producenta tego oprogramowania oraz jej uzyskaniu – w czasie naprawy;

VIII. Urządzenie pamięci masowej NAS - Typ I – 1 sztuka;

a. Parametry techniczne:

- i. Procesor: cztero-rdzeniowy o taktowaniu bazowym minimum 2,2GHz z sprzętowym wsparciem szyfrowania AES-NI i wydajnością na poziomie minimum 4400 pkt., wg testów wydajności opublikowanych na stronie internetowej https://www.cpubenchmark.net/cpu_list.php;
- ii. Pamięć operacyjna: minimum 16GB DDR4 ECC SODIMM;
- iii. Obsługiwane dyski twarde: minimum 8 dysków twardych 3,5" lub 2,5", kompatybilność z dyskami twardymi HDD oraz SSD. Każdy z dysków umieszczony w kieszeni umożliwiającej wyciągnięcie dysku podczas pracy urządzenia „na gorąco” (hot-plug) bez dodatkowych narzędzi;
- iv. Możliwość rozbudowania maksymalnej pojemności dysków twardych do 12 sztuk za pomocą dedykowanej stacji rozszerzającej;
- v. Obsadzenie dysków twardych: minimum 8 dysków HDD o pojemności minimum 12TB w formacie 3,5" w pełni kompatybilne z oferowaną macierzą dyskową oraz wykazane na liście kompatybilności z możliwością aktualizacji oprogramowania układowego dysku twardego z poziomu konsoli zarządzania pamięcią masową;
- vi. Porty zewnętrzne: minimum 2 porty USB 3.2 1-wszej generacji;
- vii. Montaż: urządzenie dedykowane do montażu w szafie RACK 19" o wysokości montażowej 2U wyposażone w szyny umożliwiające wysunięcie urządzenia;
- viii. Interfejsy LAN Ethernet: minimum 4 porty LAN Ethernet 1Gbps oraz minimum 2 porty LAN Ethernet SFP+ 10Gbe wraz z zainstalowanymi modułami SFP+ - jeden moduł SFP+ LC Duplex MultiMod, jeden moduł SFP+ RJ45 10Gbe;
- ix. Urządzenie wyposażone w dwa redundantne zasilacze;
- x. Wraz z pamięcią masową należy dostarczyć patchocord 1m MultiMod LC Duplex / SC Duplex 50/125 OM3 kompatybilny z zastosowaną wkładką SFP+ 10Gbe;
- xi. Zaplanowane włączanie oraz wyłączenie wg ustalonego harmonogramu: dostępne;
- xii. Zasilanie wejściowe: 230V/AC;

- xiii. Funkcjonalność programowa dostępna bez konieczności zakupu dodatkowych licencji;
- xiv. Funkcjonalność ustalania limitów przydzielonych zasobów plikowych (tzw. quota) dla udostępnianych zasobów plikowych;
- xv. Wewnętrzne mechanizmy analizujące stan pamięci masowej, jej podzespołów oraz stan działania macierzy RAID skonfigurowanej w serwerze macierzy dyskowej wraz z raportowaniem stanu poprzez protokół SNMP, oraz powiadomienia e-mail do wyznaczonych odbiorców;
- xvi. Wsparcie dla przesyłania dzienników do zewnętrznego systemu logowania opartego o SYSLOG;
- xvii. Technologia migawek danych zawartych na pamięci masowej - folderów współdzielonych, partycji utworzonych przez użytkownika lub zbiorów danych np. jednostek LUN, umożliwiająca w zależności od typu przechowywanych danych (plików, folderów, obrazów dysków wirtualnych) przywracanie poszczególnych plików lub folderów z danego zakresu czasowego, objętego migawką. Migawki wykonywane według ustalonego harmonogramu umożliwiające ustalenie precyzji do dnia, godziny, minuty z konfigurowalną powtarzalnością w ciągu dnia, tygodnia, miesiąca;
- xviii. Funkcjonalność polegająca na instalacji oprogramowania agentowego na stacjach roboczych oraz serwerach pracujących pod kontrolą m.in. systemu Microsoft Windows oraz Linux, polegająca na ustalaniu harmonogramu wykonywania kopii zapasowych wyznaczonych plików oraz folderów z przestrzeni dyskowej klienta oprogramowania wraz z możliwością tworzenia pełnych obrazów dysku twardego komputera klienckiego umożliwiające odtworzenia klienta oprogramowania w trybie „bare-metal” wraz z funkcjonalnością przygotowania środowiska odzyskiwania służącego przeprowadzeniu procesu odtworzenia kopii dysku twardego w trybie „bare-metal”. Wymagana jest obsługa wykonywania migawek przy użyciu Volume Shadow Copy lub innego rozwiązania producenta, realizującego tą samą funkcję – wykonanie kopii danych które są w użyciu;
- xix. Funkcjonalność polegająca na wykonywaniu replikacji poza zasoby pamięci masowej wcześniej wykonanych migawek na urządzeniu w celu zapewnienia możliwości ich odtworzenia w przypadku krytycznej awarii pamięci masowej i potrzeby jej wymiany na nowy egzemplarz;
- xx. Funkcjonalność tworzenia kompletnej kopii danych zawartych na pamięci masowej wraz z aplikacjami zainstalowanymi w obrębie pamięci masowej w wybranej przestrzeni dyskowej – lokalnej (osobnej macierzy RAID lub na nośniku USB) lub zdalnej za pomocą protokołu SMB bądź FTP;
- xxi. Wszystkie procesy kopii zapasowych oraz migawek posiadają możliwość konfiguracji okresu przechowywania, opartego co najmniej o wartość liczbową ilości ostatnio wykonanych kopii;
- xxii. Wspierane protokoły sieciowe (co najmniej): SNMP, SSH, iSCSI, FTP, NFS, SMB;
- xxiii. Zewnętrzne systemu plików (co najmniej) – np. poprzez podłączenie nośnika USB: BTFRS, EXT4, EXT3, FAT32, exFAT, NTFS, NFS+;
- xxiv. Obsługiwane typy wewnętrznej macierzy dyskowej (RAID) (co najmniej): RAID0, RAID1, RAID10, RAID5, RAID6;
- xxv. Maksymalny rozmiar pojedynczego woluminu: minimum 90TB;
- xxvi. Maksymalna liczba migawek systemu: minimum 90;
- xxvii. Maksymalna liczba woluminów wewnętrznych: minimum 40;
- xxviii. Maksymalna liczba połączeń sieciowych SMB/CIFS/NFS/FTP: minimum 500;

- xxix. Wsparcie dla kontroli uprawnień systemu plików NTFS poprzez listy ACL: dostępne;
 - xxx. Wsparcie dla tworzenia oraz udostępniania zasobów sieciowych za pomocą protokołu plików SMB/CIFS w środowiskach domenowych Active Directory z prawidłowym rozpoznawaniem oraz ustawianiem uprawnień dostępu ACL systemu plików NTFS oraz uwierzytelnianiem przy pomocy aktywnych serwerów Active Directory Services: TAK;
 - xxxi. Wbudowana zapora ogniowa (Firewall), konfigurowalna dla konkretnego interfejsu sieciowego z regułami ustawianymi na poziomie usług oraz portów z rozróżnieniem ruchu TCP/UDP oraz przychodzącego adresu IP, grupy adresów lub podsieci;
 - xxxii. Wsparcie dla segmentacji sieci LAN poprzez ustawienie identyfikatora VLAN TAG dla interfejsu sieciowego;
 - xxxiii. Zarządzanie oraz konfiguracja urządzenia za pomocą protokołu HTTP, HTTPS, opcjonalnie SSH;
 - xxxiv. Wsparcie dla zasilaczy awaryjnych UPS podłączonych za pomocą interfejsu USB, kompatybilny z urządzeniem „zasilacz awaryjny UPS o mocy pozornej 3000VA” z pkt. XIIb;
- b. Gwarancja producenta:** 36 miesięcy;

IX. Urządzenie pamięci masowej NAS - Typ II – 1 sztuka;

c. Parametry techniczne:

- i. Procesor: cztero-rdzeniowy o taktowaniu bazowym minimum 2,2GHz z sprzętowym wsparciem szyfrowania AES-NI i wydajnością na poziomie minimum 4400 pkt., wg testów wydajności opublikowanych na stronie internetowej https://www.cpubenchmark.net/cpu_list.php;
- ii. Pamięć operacyjna: minimum 16GB DDR4 ECC SODIMM;
- iii. Obsługiwane dyski twarde: minimum 5 dysków twardych 3,5” lub 2,5”, kompatybilność z dyskami twardymi HDD oraz SSD. Każdy z dysków umieszczony w kieszeni umożliwiającej wyciągnięcie dysku podczas pracy urządzenia „na gorąco” (hot-plug) bez dodatkowych narzędzi;
- iv. Możliwość rozbudowania maksymalnej pojemności dysków twardych do 15 sztuk za pomocą dedykowanej stacji rozszerzającej;
- v. Obsadzenie dysków twardych: minimum 5 dysków HDD o pojemności minimum 12TB w formacie 3,5” w pełni kompatybilne z oferowaną macierzą dyskową oraz wykazane na liście kompatybilności z możliwością aktualizacji oprogramowania układowego dysku twardego z poziomu konsoli zarządzania pamięcią masową;
- vi. Porty zewnętrzne: minimum 2 porty USB 3.2 1-wszej generacji;
- vii. Montaż: urządzenie dedykowane do montażu w obudowie wolnostojącej typu desktop;
- viii. Interfejsy LAN Ethernet: minimum 2 porty LAN Ethernet 2,5Gbps oraz minimum 1 slot umożliwiający rozbudowę interfejsów sieciowych dedykowaną kartą rozszerzeń obsługującą połączenie do 10Gbps;
- ix. Zaplanowane włączanie oraz wyłączanie wg ustalonego harmonogramu: dostępne;
- x. Zasilanie wejściowe: 230V/AC;
- xi. Funkcjonalność programowa dostępna bez konieczności zakupu dodatkowych licencji;
- xii. Funkcjonalność ustalania limitów przydzielonych zasobów plikowych (tzw. quota) dla udostępnianych zasobów plikowych;
- xiii. Wewnętrzne mechanizmy analizujące stan pamięci masowej, jej podzespołów oraz stan działania macierzy RAID skonfigurowanej w serwerze macierzy dyskowej wraz z



- raportowaniem stanu poprzez protokół SNMP, oraz powiadomienia e-mail do wyznaczonych odbiorców;
- xiv. Wsparcie dla przesyłania dzienników do zewnętrznego systemu logowania opartego o SYSLOG;
 - xv. Technologia migawek danych zawartych na pamięci masowej - folderów współdzielonych, partycji utworzonych przez użytkownika lub zbiorów danych np. jednostek LUN, umożliwiająca w zależności od typu przechowywanych danych (plików, folderów, obrazów dysków wirtualnych) przywracanie poszczególnych plików lub folderów z danego zakresu czasowego, objętego migawką. Migawki wykonywane według ustalonego harmonogramu umożliwiające ustalenie precyzji do dnia, godziny, minuty z konfigurowalną powtarzalnością w ciągu dnia, tygodnia, miesiąca;
 - xvi. Funkcjonalność polegająca na instalacji oprogramowania agentowego na stacjach roboczych oraz serwerach pracujących pod kontrolą m.in. systemu Microsoft Windows oraz Linux, polegająca na ustalaniu harmonogramu wykonywania kopii zapasowych wyznaczonych plików oraz folderów z przestrzeni dyskowej klienta oprogramowania wraz z możliwością tworzenia pełnych obrazów dysku twardego komputera klienckiego umożliwiające odtworzenia klienta oprogramowania w trybie „bare-metal” wraz z funkcjonalnością przygotowania środowiska odzyskiwania służącego przeprowadzeniu procesu odtworzenia kopii dysku twardego w trybie „bare-metal”. Wymagana jest obsługa wykonywania migawek przy użyciu Volume Shadow Copy lub innego rozwiązania producenta, realizującego tą samą funkcję – wykonanie kopii danych które są w użyciu;
 - xvii. Funkcjonalność polegająca na wykonywaniu replikacji poza zasoby pamięci masowej wcześniej wykonanych migawek na urządzeniu w celu zapewnienia możliwości ich odtworzenia w przypadku krytycznej awarii pamięci masowej i potrzeby jej wymiany na nowy egzemplarz;
 - xviii. Funkcjonalność tworzenia kompletnej kopii danych zawartych na pamięci masowej wraz z aplikacjami zainstalowanymi w obrębie pamięci masowej w wybranej przestrzeni dyskowej – lokalnej (osobnej macierzy RAID lub na nośniku USB) lub zdalnej za pomocą protokołu SMB bądź FTP;
 - xix. Wszystkie procesy kopii zapasowych oraz migawek posiadają możliwość konfiguracji okresu przechowywania, opartego co najmniej o wartość liczbową ilości ostatnio wykonanych kopii;
 - xx. Wspierane protokoły sieciowe (co najmniej): SNMP, SSH, iSCSI, FTP, NFS, SMB;
 - xxi. Zewnętrzne systemu plików (co najmniej) – np. poprzez podłączenie nośnika USB: BTFRS, EXT4, EXT3, FAT32, exFAT, NTFS, NFS+;
 - xxii. Obsługiwane typy wewnętrznej macierzy dyskowej (RAID) (co najmniej): RAID0, RAID1, RAID10, RAID5, RAID6;
 - xxiii. Maksymalny rozmiar pojedynczego woluminu: minimum 108TB;
 - xxiv. Maksymalna liczba migawek systemu: minimum 64;
 - xxv. Maksymalna liczba woluminów wewnętrznych: minimum 32;
 - xxvi. Maksymalna liczba połączeń sieciowych SMB/CIFS/NFS/FTP: minimum 40;
 - xxvii. Wsparcie dla kontroli uprawnień systemu plików NTFS poprzez listy ACL: dostępne;
 - xxviii. Wsparcie dla tworzenia oraz udostępniania zasobów sieciowych za pomocą protokołu plików SMB/CIFS w środowiskach domenowych Active Directory z prawidłowym rozpoznawaniem oraz ustawianiem uprawnień dostępu ACL systemu plików NTFS oraz uwierzytelnianiem przy pomocy aktywnych serwerów Active Directory Services: TAK;

- xxix. Wbudowana zaporą ogniową (Firewall), konfigurowalna dla konkretnego interfejsu sieciowego z regułami ustawianymi na poziomie usług oraz portów z rozróżnieniem ruchu TCP/UDP oraz przychodzącego adresu IP, grupy adresów lub podsieci;
 - xxx. Wsparcie dla segmentacji sieci LAN poprzez ustawienie identyfikatora VLAN TAG dla interfejsu sieciowego;
 - xxxi. Zarządzanie oraz konfiguracja urządzenia za pomocą protokołu HTTP, HTTPS, opcjonalnie SSH;
 - xxxii. Wsparcie dla zasilaczy awaryjnych UPS podłączonych za pomocą interfejsu USB, kompatybilny z urządzeniem „zasilacz awaryjny UPS o mocy pozornej 1500VA” z pkt. XIIa;
- d. Gwarancja producenta:** 36 miesięcy;

X. Przełącznik sieciowy – zarządzalny – Typ I – 1 sztuka:

a. Parametry techniczne:

- i. Typ przełącznika: SMART, zarządzalny;
 - ii. Łączna liczba portów: minimum 28 portów;
 - iii. Ilość portów 100/1000Mbps Ethernet – miedzianych – minimum 24 w tym 24 porty PoE 802.3af/at;
 - iv. Budżet mocy PoE 8023.af/at przełącznika sieciowego: minimum 350W;
 - v. Ilość portów 10Gigabit Ethernet – światłowodowych typu SFP+ - minimum 4 sztuki;
 - vi. Przepustowość magistrali wewnętrznej: minimum 100 Gigabitów/sekundę;
 - vii. Tablica adresów MAC: 14000 wpisów;
 - viii. Napięcie wejściowe: 220 - 240V/AC 50/60Hz;
 - ix. Wysokość instalacyjna RACK: 19" 1U;
 - x. Czas bezawaryjnej pracy (parametr MTBF): minimum 1,2mln godzin;
 - xi. Konfiguracja: minimum poprzez przeglądarkę WWW z użyciem protokołu SSL, opcjonalnie poprzez interfejs SSH lub Telnet;
 - xii. Konfiguracja: możliwość importu oraz eksportu konfiguracji do pliku;
 - xiii. Ustawianie czasu wewnętrznego urządzenia w oparciu o serwer czasu: NTP lub SNTP;
 - xiv. Aktualizacja firmware urządzenia: poprzez przeglądarkę WWW opcjonalnie poprzez FTP, SSH, TFTP;
 - xv. Obsługa wkładek w slotach SFP+: jedno oraz wielomodowych o przepustowościach 1Gbps oraz 10Gbps działających na dystansach minimum 250m dla światłowodów wielomodowych oraz minimum 8km dla światłowodów jedno-modowych. Wsparcie dla kabli DAC (Direct Attach Cable) o przepustowościach do 10Gbps;
 - xvi. Wymagane wsparcie dla protokołów: IEEE 802.3z 1000BASE-X, IEEE 802.3ab 1000BASE-T Ethernet, , IEEE 802.3ae 10 Gbit/s Ethernet, IEEE 802.3ad LACP aggregation, IEEE 802.1D Spanning Tree Protocol (STP), IEEE 802.1w Rapid Spanning Tree Protocol (RSTP), IEEE 802.1s Multiple Spanning Tree Protocol (MSTP), IEEE 802.1X port authentication, ochrona przed pętlą w sieci LAN, 802.1Q – statyczne oraz dynamiczne VLAN, PVID VLAN, VLAN TAG, VLAN Trunking, SYSLOG IPv4, SNMP (v1,v2c, v3), SNMP trap, RMON;
 - xvii. Zarządzanie oraz monitorowanie urządzenia z poziomu chmury producenta poprzez panel WWW oraz aplikację pracującą pod kontrolą systemu Android. Producent zapewnia pakiety licencyjne o różnej funkcjonalności w tym minimum jeden darmowy. Rozwiązanie chmurowe producenta kompatybilne z stosowanym rozwiązaniem chmurowym zaoferowanym w urządzeniach z pkt. I, V, VII;
- b. Gwarancja producenta:** „do końca życia produktu” co oznacza że podlega ciągłej gwarancji producenta oraz 5-cio letniej gwarancji producenta od publikacji informacji o zakończeniu produkcji modelu urządzenia;

XI. Przełącznik sieciowy – zarządzalny – Typ II – 4 sztuki:

a. Parametry techniczne:

- i. Typ przełącznika: SMART, zarządzalny;
- ii. Łączna liczba portów: minimum 12 portów;
- iii. Ilość portów 100/1000Mbps Ethernet – miedzianych – minimum 8;
- iv. Ilość portów 1G/2.5G/5G/10G Ethernet – miedzianych – minimum 3;
- v. Ilość portów 10Gigabit Ethernet – światłowodowych typu SFP+ - minimum 1 sztuki;
- vi. Przepustowość magistrali wewnętrznej: minimum 90 Gigabitów/sekundę;

- vii. Tablica adresów MAC: 14000 wpisów;
 - viii. Napięcie wejściowe: 220 - 240V/AC 50/60Hz, zasilacz zewnętrzny;
 - ix. Wysokość instalacyjna/obudowa: desktop, możliwy montaż naścienny;
 - x. Konfiguracja: minimum poprzez przeglądarkę WWW z użyciem protokołu SSL;
 - xi. Konfiguracja: możliwość importu oraz eksportu konfiguracji do pliku;
 - xii. Ustawianie czasu wewnętrznego urządzenia w oparciu o serwer czasu: NTP lub SNTP;
 - xiii. Aktualizacja firmware urządzenia: poprzez przeglądarkę WWW;
 - xiv. Obsługa wkładek w slotach SFP+: jedno oraz wielomodowych o przepustowościach 1Gbps oraz 10Gbps działających na dystansach minimum 250m dla światłowodów wielomodowych oraz minimum 8km dla światłowodów jedno-modowych. Wsparcie dla kabli DAC (Direct Attach Cable) o przepustowościach do 10Gbps;
 - xv. Wymagane wsparcie dla protokołów: IEEE 802.3ab 1000BASE-T Ethernet, IEEE 802.3an 10GBASE-T, IEEE 802.3ae 10 Gbit/s Ethernet over fiber , ochrona przed pętlą w sieci LAN, 802.1Q – statyczne oraz dynamiczne VLAN, PVID VLAN, VLAN TAG;
 - xvi. Maksymalny pobór mocy: 21W;
- b. Gwarancja producenta:** „do końca życia produktu” co oznacza że podlega ciągłej gwarancji producenta oraz 5-cio letniej gwarancji producenta od publikacji informacji o zakończeniu produkcji modelu urządzenia;

XII. Zasilacze awaryjne

- a. Zasilacz awaryjny UPS o mocy pozornej 1500VA kompatybilny z pamięcią masową z punktu IX – 1 sztuka;**
- i. Parametry techniczne:**
- 1. Moc znamionowa w VA: 1500VA;
 - 2. Moc znamionowa w W: 1000W;
 - 3. Napięcie wejściowe: 230V przy 50Hz;
 - 4. Złącza wyjściowe: 8 wyjść IEC 320 C13 podzielone co najmniej na dwie niezależnie sterowane grupy wyjść;
 - 5. Wysokość obudowy typu TOWER: max 220mm;
 - 6. Głębokość urządzenia: nieprzekraczająca 440cm;
 - 7. Waga urządzenia: nieprzekraczająca 30kg;
 - 8. Żywotność akumulatora wg założeń producenta: minimum 3 lata;
 - 9. Czas podtrzymania dla obciążenia 200W: co najmniej 83 minut;
 - 10. Czas podtrzymania dla obciążenia 400W: co najmniej 30 minuty;
 - 11. Topologia urządzenia: Line-Interactive;
 - 12. Przebieg wyjścia napięcia przy zasilaniu bateryjnym: sinusoida;
 - 13. Zarządzanie przez panel LCD z przyciskami sterującymi umożliwiające weryfikację podstawowych parametrów pracy (m.in. obciążenia, czasu podtrzymania akumulatorowego, napięcie wejściowe, wyjściowe, uruchomienie procedury diagnostycznej, stanu naładowania akumulatorów);
 - 14. Funkcjonalność oprogramowania do zarządzania producenta zasilacza umożliwiająca konfigurację powiadomień e-mail w zakresie stanów pracy zasilacza, m.in. praca na baterii, praca na zasilaniu AC, informacja o udanej lub nieudanej diagnostyce, potrzebie wymiany baterii, przeciążeniu urządzenia, uruchomieniu procedury zamykania urządzenia.
 - a. Funkcjonalność oprogramowania instalowanego w systemie operacyjnym: komunikacja przy użyciu portu komunikacyjnego USB musi posiadać

możliwość pracy w trybie usługi pod kontrolą systemu Windows lub Linux co wiąże się z jego automatycznym uruchomieniem podczas startu systemu operacyjnego oraz rozpoczęciu komunikacji z zasilaczem awaryjnym. Dostęp do aplikacji chroniony poprzez login oraz hasło ustawiane podczas instalacji lub po pierwszym uruchomieniu. Konfiguracja aplikacji poprzez interfejs WWW udostępniany przez usługę pracującą w tle z możliwością zarządzania zasilaczem awaryjnym, podgląd stanu obciążenia oraz szacowanego czasu podtrzymania, przeglądanie dzienników historycznych pracy urządzenia w tym stanów odnotowanych w dzienniku zdarzeń (np. zanik zasilania, powrót zasilania), konfiguracja grup wyjść zasilania, czasów opóźnień oraz sposobu działania w wypadku utraty zasilania sieciowego. Możliwość konfiguracji skryptu .bat/.sh (w zależności od systemu operacyjnego) wywoływanego w sytuacji zaniku zasilania oraz doprowadzenia do określonego poziomu naładowania baterii lub pozostałego czasu podtrzymania zasilania;

- b. Funkcjonalność dostępna poprzez bezpośrednie połączenie przeglądarką internetową z modułem Ethernet: dostęp chroniony poprzez login oraz hasło ustawiane w urządzeniu. Podgląd stanu obciążenia oraz szacowanego czasu podtrzymania, przeglądanie dzienników historycznych pracy urządzenia w tym stanów odnotowanych w dzienniku zdarzeń (np. zanik zasilania, powrót zasilania), konfiguracja grup wyjść zasilania, czasów opóźnień oraz sposobu działania w wypadku utraty zasilania sieciowego. Realizacja powiadomień za pomocą wiadomości e-mail z użyciem połączeń autoryzowanych SMTP przy wsparciu protokołu SSL lub TLS;

ii. **Gwarancja producenta:** 36 miesięcy na elektronikę, 24 miesiące na moduły bateryjne;

b. Zasilacz awaryjny UPS o mocy pozornej 3000VA kompatybilny z pamięcią masową z punktu VIII – 3 sztuki;

i. Parametry techniczne:

1. Moc znamionowa w VA: 3000VA;
2. Moc znamionowa w W: 2700W;
3. Napięcie wejściowe: 230V przy 50Hz;
4. Złącza wyjściowe: 8 wyjścia IEC 320 C13 podzielone co najmniej na dwie niezależnie sterowane grupy wyjść;
5. Wysokość obudowy typu TOWER: max 440mm;
6. Głębokość urządzenia: nieprzekraczająca 55cm;
7. Waga urządzenia: nieprzekraczająca 55kg;
8. Żywotność akumulatora wg założeń producenta: minimum 3 lata;
9. Czas podtrzymania dla obciążenia 500W: co najmniej 55 minut;
10. Czas podtrzymania dla obciążenia 100W: co najmniej 25 minut;
11. Topologia urządzenia: Line-Interactive;
12. Przebieg wyjścia napięcia przy zasilaniu bateryjnym: sinusoida;
13. Zarządzanie przez panel LCD z przyciskami sterującymi umożliwiającymi weryfikację podstawowych parametrów pracy (m.in. obciążenia, czasu podtrzymania akumulatorowego, napięcie wejściowe, wyjściowe, uruchomienie procedury diagnostycznej, stanu naładowania akumulatorów);
14. Funkcjonalność oprogramowania do zarządzania producenta zasilacza umożliwiającą konfigurację powiadomień e-mail w zakresie stanów pracy zasilacza,

m.in. praca na baterii, praca na zasilaniu AC, informacja o udanej lub nieudanej diagnostyce, potrzebie wymiany baterii, przeciążeniu urządzenia, uruchomieniu procedury zamykania urządzenia.

- a. Funkcjonalność oprogramowania instalowanego w systemie operacyjnym: komunikacja przy użyciu portu komunikacyjnego USB musi posiadać możliwość pracy w trybie usługi pod kontrolą systemu Windows lub Linux co wiąże się z jego automatycznym uruchomieniem podczas startu systemu operacyjnego oraz rozpoczęciu komunikacji z zasilaczem awaryjnym. Dostęp do aplikacji chroniony poprzez login oraz hasło ustawiane podczas instalacji lub po pierwszym uruchomieniu. Konfiguracja aplikacji poprzez interfejs WWW udostępniany przez usługę pracującą w tle z możliwością zarządzania zasilaczem awaryjnym, podgląd stanu obciążenia oraz szacowanego czasu podtrzymania, przeglądanie dzienników historycznych pracy urządzenia w tym stanów odnotowanych w dzienniku zdarzeń (np. zanik zasilania, powrót zasilania), konfiguracja grup wyjść zasilania, czasów opóźnień oraz sposobu działania w wypadku utraty zasilania sieciowego. Możliwość konfiguracji skryptu .bat/.sh (w zależności od systemu operacyjnego) wywoływanego w sytuacji zaniku zasilania oraz doprowadzenia do określonego poziomu naładowania baterii lub pozostałego czasu podtrzymania zasilania;
- b. Funkcjonalność dostępna poprzez bezpośrednie połączenie przeglądarką internetową z modułem Ethernet: dostęp chroniony poprzez login oraz hasło ustawiane w urządzeniu. Podgląd stanu obciążenia oraz szacowanego czasu podtrzymania, przeglądanie dzienników historycznych pracy urządzenia w tym stanów odnotowanych w dzienniku zdarzeń (np. zanik zasilania, powrót zasilania), konfiguracja grup wyjść zasilania, czasów opóźnień oraz sposobu działania w wypadku utraty zasilania sieciowego. Realizacja powiadomień za pomocą wiadomości e-mail z użyciem połączeń autoryzowanych SMTP przy wsparciu protokołu SSL lub TLS;

ii. **Gwarancja producenta:** 36 miesięcy na elektronikę, 24 miesiące na moduły bateryjne;