IP-III.272.3.2025 Załącznik nr 1

**Opis Przedmiotu Zamówienia**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa i opis przedmiotu zamówienia** | **Oferowany przedmiot zamówienia (nazwa producenta, model, kod produktu pozwalający na jednoznaczne stwierdzenie zgodności oferowanego sprzętu )** |
| 1. | **Zakup serwerów wraz z systemem serwerowym Windows Serwer – 2 szt.**  **Obudowa**   * Typu RACK, wysokość 2U; * Szyny umożliwiające wysunięcie serwera z szafy stelażowej wraz z ramieniem porządkującym kable z tyłu obudowy; * Możliwość zainstalowania 16 dysków twardych hot plug 2,5”; * Możliwość zainstalowania fizycznego zabezpieczenia (np. na klucz lub elektrozamek) uniemożliwiającego fizyczny dostęp do dysków twardych; * Zainstalowane 8 szt. dysków SSD SATA 7,68TB Read-Int Hot-Plug skonfigurowane w RAID podpięte do sprzętowego kontrolera; * Możliwość zainstalowania dysku M.2 NVMe PCIe4.0 x4; * Możliwość zainstalowania dedykowanego wewnętrznego napędu blu-ray. * Możliwość zainstalowania dedykowanego wewnętrznego napędu LTO-8.   **Płyta główna**   * Dwuprocesorowa; * Wyprodukowana i zaprojektowana przez producenta serwera; * Możliwość instalacji procesorów 60-rdzeniowych; * Zainstalowany moduł TPM 2.0; * 6 złącz PCI Express generacji 5 w tym:   + 4 fizyczne złącza o prędkości x16;   + 2 fizyczne złącza o prędkości x8;   + Opcjonalnie możliwość uzyskania 2 złącz typu pełnej wysokości;   + Opcjonalnie możliwość uzyskania 9 aktywnych interfejsów PCI-e; * 32 gniazda pamięci RAM; * Obsługa minimum 8 TB pamięci RAM DDR5; * Wsparcie dla technologii:   + Memory Scrubbing;   + SDDC;   + ECC;   + Memory Mirroring;   + ADDDC; * Możliwość instalacji 2 dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express)  dyski nie mogą zajmować klatek  dla dysków hot-plug.   **Procesory**   * Dwa procesory 16-rdzeniowe, taktowanie bazowe 2.0 GHz, architektura x86\_64; * osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017\_fp\_base 397 pkt  (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie <http://spec.org/cpu2017/results/cpu2017.html> dla oferowanego serwera;   **Pamięć RAM**   * 256 GB pamięci RAM; * DDR5 Registered 4800MT/s;   Pamięci obsadzone w sposób gwarantujący najwyższa możliwość wydajność;  **Kontrolery LAN**  Interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express:   * 5x 1Gbit Base-T; * Możliwość uzyskania dwóch interfejsów 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe;   Interfejsy LAN zainstalowane w slotach PCI-e:   * 2x 10Gbit SFP+ obsadzone wkładkami MMF LC.   **Kontrolery I/O**   * Kontroler SAS RAID dla dysków wewnętrznych posiadający min. 4GB pamięci cache, obsługujący poziomy RAID: 0,1,10,5,50,6,60  z podtrzymaniem pamięci cache w przypadku utraty zasilania;   **Porty**   * Zintegrowana karta graficzna ze złączem VGA z tyłu serwera; * 1 porty USB 3.0 wewnętrzny; * 2 porty USB 3.0 dostępne z tyłu serwera; * 2 porty USB 3.0 na panelu przednim; * Opcjonalny port serial, możliwość wykorzystania portu serial  do zarządzania serwerem; * Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.   **Zasilanie, chłodzenie**   * Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy min. 900W; * Redundantne wentylatory hotplug.   **Zarządzanie**   * Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii; * informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:   + karty rozszerzeń zainstalowane w dowolnym  slocie PCI Express;   + procesory CPU;   + pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM;   + status karty zarządzającej serwera;   + wentylatory;   + bateria podtrzymująca ustawienia BIOS płyty głównej;   + zasilacze;   + system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie  w celu uruchomienia przy odłączonym zasilaniu sieciowym); * Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: * Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; * Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania  z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; * Dostęp poprzez przeglądarkę Web, SSH; * Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii; * Zarządzanie alarmami (zdarzenia poprzez SNMP); * Możliwość przejęcia konsoli tekstowej; * Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM); * Obsługa serwerów proxy (autentykacja); * Obsługa VLAN; * Możliwość konfiguracji parametru Max. Transmission Unit (MTU); * Wsparcie dla protokołu SSDP; * Obsługa protokołów TLS 1.2, SSL v3; * Obsługa protokołu LDAP; * Integracja z HP SIM; * Synchronizacja czasu poprzez protokół NTP; * Możliwość backupu i odtwarzania ustawień bios serwera  oraz ustawień karty zarządzającej;   Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna);  Wbudowania w kartę zarządzającą (lub zainstalowana) pamięć flash dająca możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;  Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych  i wewnętrznych poza obrębem karty zarządzającej.  **Wspierane OS**   * Microsoft Windows Server 2025, 2022, 2019; * VMWare vSphere 8.0; * Suse Linux Enterprise Server 15; * Red Hat Enterprise Linux 9, 8; * Microsoft Hyper-V Server 2019.   **Gwarancja**   * Min.5 lat gwarancji producenta serwera w trybie on-site  z gwarantowaną skuteczną naprawą w miejscu użytkowania sprzętu do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis.  Dyski twarde nie podlegają zwrotowi organizacji serwisowej; * Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu; * Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych; * Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona  w ofercie; * Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty).   **Dokumentacja, inne**   * Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane  oraz całe muszą być objęte gwarancją producenta, o wymaganym  w specyfikacji poziomie SLA – wymagane oświadczenie wykonawcy lub producenta; * Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy  lub producenta; * Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki; * W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji; * Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; * Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 8 - 85 %; * Zgodność z normami: CB, RoHS, WEEE  oraz CE.   Licencja na serwerowy system operacyjny w najnowszej aktualnie ofertowanej wersji przez producenta musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego.  Licencja musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze. Poniższy opis należy traktować jako zbiór wymagań minimalnych, ponieważ Wykonawca musi zapewnić odpowiednie parametry i spełnić wszystkie wymagania licencyjne oferowanego systemu operacyjnego, niezbędne do poprawnego uruchomienia rozwiązania.  Wymaga się, aby oferowane licencje umożliwiały korzystanie 140 urządzeniom.   * Licencja systemu operacyjnego: **Microsoft Windows Server 2025 Standard (64-bit) lub równoważny**, * **140 szt. licencji dostępnych typu Device CAL (Client Access License)** – dostarczonych w ramach tej samej dostawy co serwer.   **Wymagania dotyczące systemu operacyjnego**  **System:**   * Microsoft Windows Server 2025 Standard, 64-bit lub równoważny * Licencja wieczysta (perpetual), oparta na rdzeniach procesora (minimum 16 Core), * Uprawnienie do uruchomienia 2 maszyn wirtualnych na 1 instancji fizycznej, * Pełna funkcjonalność serwerowa (AD DS, DNS, DHCP, Hyper-V, File Services, itp.), * Wersja polska lub możliwość instalacji języka polskiego, * Wsparcie dla technologii zabezpieczeń: TPM 2.0, Secure Boot, BitLocker, szyfrowanie EFS.   **Wymagania dotyczące licencji CAL**  **Rodzaj licencji:**  **140 sztuk licencji dostępowych (CAL)** typu **Device** – przypisanych do urządzeń (nie użytkowników),   * Licencje muszą być:   + wieczyste (perpetual),   + kompatybilne z systemem Windows Server 2025 Standard,   + fabrycznie nowe, nieaktywowane, z legalnego kanału dystrybucji Microsoft (np. CSP, MOLP, OEM, Open License),   + dostarczone fizycznie lub elektronicznie (klucz licencyjny + dokument licencyjny).   **Dostawa:**   * Licencje CAL muszą być **dostarczone w ramach tej samej dostawy co serwer fizyczny** i stanowić integralny element przedmiotu zamówienia. |  |
| 2. | **Zakup rozwiązania UTM i aktualizacja bieżącego rozwiązania – 1 szt.**  **OBSŁUGA SIECI**   1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.   **ZAPORA KORPORACYJNA (Firewall)**   1. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. 2. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. 3. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). 4. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. 5. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia. 6. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. 7. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall. 8. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł. 9. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos. 10. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego). 11. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.   **INTRUSION PREVENTION SYSTEM (IPS)**   1. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. 2. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy. 3. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. 4. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS. 5. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia. 6. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS. 7. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP. 8. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0. 9. Moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV). 10. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.   **KSZTAŁTOWANIE PASMA (Traffic Shapping)**   1. Urządzenie ma umożliwiać kształtowanie pasma w oparciu  o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. 2. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP. 3. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring). 4. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.   **OCHRONA ANTYWIRUSOWA**   1. Urządzenie ma być dostarczone wraz z komercyjnym, zaawansowanym skanerem antywirusowym oraz umożliwiać skanowanie plików w oparciu o sandboxing zlokalizowany w Internecie na serwerach producenta i na terenie Unii Europejskiej. Nie dopuszcza się aby analiza sandboxingu była przeprowadzana na urządzeniu lub wymagała instalacji dodatkowego urządzenia lub oprogramowania.  Nie dopuszcza się również żeby analiza sandboxingu była przeprowadzana przez firmy trzecie. 2. Skaner antywirusowy ma być dostarczany przez firmy trzecie (inne niż producent rozwiązania). 3. Administrator ma mieć możliwość określenia akcji w przypadku wykrycia zagrożenia bądź gdy analiza skanerem antywirusowym została zakończona błędem. 4. Skaner antywirusowy ma pochodzić od europejskiego producenta. 5. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. 6. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.   **OCHRONA ANTYSPAM**   1. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).    1. Ochrona antyspam ma działać w oparciu o: białe/czarne listy,    2. DNS RBL,    3. Skaner heurystyczny.    4. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.    5. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.   **WIRTUALNE SIECI PRYWATNE (VPN)**   1. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). 2. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:    1. PPTP VPN,    2. IPSec VPN,    3. SSL VPN. 3. SSL VPN ma działać w trybie tunelu. 4. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem. 5. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal) 6. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). 7. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf. 8. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.   **FILTR DOSTĘPU DO STRON WWW**   1. Urządzenie ma posiadać wbudowany filtr URL. 2. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 77 kategorii tematycznych stron internetowych. Rozszerzony URL Filtering posiada miliony sklasyfikowanych stron internetowych. 3. Klasyfikacja URL musi się odbywać w oparciu o komunikację z serwerami producenta znajdującymi się w sieci Internet, a nie na bazie danych przechowywanej lokalnie w urządzeniu. 4. Administrator ma mieć możliwość dodawania własnych kategorii URL. 5. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii.  Do wyboru ma być przynajmniej:  * blokowanie dostępu do adresu URL, * zezwolenie na dostęp do adresu URL, * blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.  1. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.  * Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych. * Filtr URL musi uwzględniać komunikację po protokole HTTPS. * Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. * Urządzenie ma umożliwiać stworzenie listy stron dostępnych  po protokole HTTPS, które nie będą deszyfrowane. * Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch   **UWIERZYTELNIANIE**   1. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o: lokalną bazę użytkowników (wewnętrzny LDAP),  * zewnętrzną bazę użytkowników (zewnętrzny LDAP), * usługę katalogową Microsoft Active Directory. * Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP. * Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły: SSL, Radius, Kerberos.  1. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory  w oparciu o co najmniej dwa mechanizmy. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.  * Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny. * Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS). * Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP). * Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.  1. Rozwiązanie musi zapewniać Zero-Trust Network Access (ZTNA), dając dostęp do zasobów na podstawie analizy polityk bezpieczeństwa w oparciu co najmniej o weryfikację wersji systemu operacyjnego, statusu zapory sieciowej czy zainstalowanego programu antywirusowego na stacji roboczej.   **ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)**   1. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).    1. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: równoważenie względem adresu źródłowego,    2. równoważenie względem połączenia.    3. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.    4. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).    5. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.    6. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).    7. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.   **ROUTING (TRASOWANIE)**   1. Urządzenie ma umożliwiać statyczne trasowanie pakietów. 2. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 3. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing). 4. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP. 5. Rozwiązanie musi dawać możliwość wybrania predefiniowalnego obiektu typu blackhole.   **ADMINISTRACJA URZĄDZENIEM**   1. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego. 2. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS. 3. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP. 4. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami 5. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. 6. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH) 7. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania. 8. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS. 9. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup. 10. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych. 11. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła. 12. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora ( script recording ). 13. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services). 14. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników. 15. Urządzenie ma umożliwiać zapisywanie logów na wbudowanym dysku. 16. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak  i szyfrowanej (TLS). 17. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.     1. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie: manualnego eksportu do pliku  w dowolnym momencie czasu,     2. automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu     3. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzącego bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.     4. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.     5. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline  z poziomu interfejsu graficznego.   **RAPORTOWANIE**   1. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. 2. System raportowania i przeglądania logów wbudowany  w system nie może wymagać dodatkowej licencji do swojego działania. 3. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego. 4. System raportowania ma umożliwiać wygenerowanie  co najmniej 25 różnych raportów. 5. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu. 6. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV. 7. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta. 8. Urządzenie ma umożliwiać monitorowanie swojego stanu  w wykorzystanie protokołu SNMP w wersji 1, 2 i 3. 9. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).   **POZOSTAŁE USŁUGI I FUNKCJE**   1. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP. 2. Urządzenie ma posiadać wbudowany serwer DHCP  z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej. 3. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay). 4. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6. 5. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny). 6. Urządzenie ma posiadać usługę DNS Proxy. 7. Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP). 8. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN. 9. Urządzenie musi mieć zaimplementowane Open API. 10. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.   **GWARANCJA I SERWIS**   1. Urządzenie ma być objęte 12-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa. 2. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.   **PARAMETRY SPRZĘTOWE**   1. Urządzenie ma być wyposażone w dysk SSD o pojemności co najmniej 200 GB. 2. Urządzenie wyposażone jest w redundantne zasilanie  z sygnalizacją pracy poszczególnych zasilaczy. 3. Liczba portów Ethernet 2,5Gbps – min. 8 z możliwością rozszerzenia do 16. 4. Liczba portów światłowodowych 1Gbps – min. 2 z możliwością rozszerzenia do 10.    1. Urządzenie ma pozwalać na instalację modułu rozszerzeń z poniższej listy: Moduł z 8 interfejsami miedzianymi 2,5Gbps    2. Moduł z 4 interfejsami miedzianymi 10Gbps.    3. Moduł z 8 interfejsami miedzianymi 1Gbps (4 pary interfejsów w trybie bypass).    4. Moduł z 8 interfejsami miedzianymi 1Gbps.    5. Moduł z 8 interfejsami światłowodowymi 1Gbps.    6. Moduł z 4 interfejsami światłowodowymi 10Gbps.    7. Moduł z 2 interfejsami światłowodowymi 25Gbps.    8. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.    9. Urządzenie ma być wyposażone w min. 2, różniące się typem, porty konsolowe. Przynajmniej jeden port konsolowy ma być typu RJ45.    10. Przepustowość Firewall (1518 bajtów UDP) – minimum 10Gbps.    11. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 5Gbps.    12. Przepustowość filtrowania Antywirusowego – minimum 1.3 Gbps.    13. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 2.5Gbps.    14. Liczba tuneli VPN IPSec – minimum 1000.    15. Liczba tuneli typu SSL VPN (tryb tunelu) – minimum 150.    16. Obsługa interfejsów 802.11q (VLAN) – minimum 256.    17. Liczba równoczesnych sesji – minimum 600 000 i nie mniej niż 30 000 nowych sesji/sekundę. 5. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive. 6. Urządzenie nie ma limitu na liczbę użytkowników. 7. Liczba reguł filtrowania – minimum 16 384. 8. Liczba tras statycznego routingu – minimum 5 120. 9. Liczba tras dynamicznego routingu – minimum 10 000. 10. Możliwość instalacji w szafie RACK 19”, wysokość urządzenia 1U. 11. Urządzenie musi być wyposażone w moduł TPM. |  |
| 3. | **Przedłużenie wsparcia w zakresie oprogramowania do skanowania podatności i zagrożeń – 1 szt.**   1. System operacyjny:    1. Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi    2. Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi    3. MacOS 12 lub nowszy. 2. Serwer administracyjny musi obsługiwać instalację na systemach:   a. Windows Server 2016 (64-bit) i nowszych. 3. Serwer administracyjny musi obsługiwać bazy danych:   a. MS SQL Server 2016 lub nowsze,   b. MS SQL Express, c. AzureSQL S3 lub nowsze. 4. Pomoc i dokumentacja programu dostępne w języku angielskim. 5. Konsola administracyjna i komunikaty klienta muszą być w języku polskim. 6. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta. 7. Serwer administracyjny musi umożliwiać instalację/dezinstalację zdalnego klienta na stacjach roboczych. 8. Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym. 9. Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia. 10. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli. 11. System musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych, usuwając najstarsze informacje, gdy rozmiar bazy osiągnie skonfigurowany limit. 12. Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania. 13. Administrator musi mieć możliwość aby tworzyć, usuwać i konta administratorów w konsoli programu. 14. Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu). 15. Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory. 16. Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą a serwerem w czasie rzeczywistym. 17. Serwer administracyjny musi umożliwiać ustawienie powiadomień dla użytkownika końcowego w przypadku złamania reguł związanych z ochroną DLP, z możliwością dostosowania grafiki, adresu e-mail i odnośnika do polityki bezpieczeństwa. 18. Administrator musi mieć możliwość wykonać audyt stacji roboczych/użytkowników w oparciu o różne czynności, takie jak uruchomione aplikacje, podłączone urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, wysyłane i odebrane wiadomości email oraz czynności na plikach. 19. Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji i typów plików. 20. Administrator musi mieć możliwość filtrowania i sortowania zebranych danych. 21. Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości email. 22. Dashboardy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu. 23. Serwer administracyjny musi posiadać wbudowany serwer SMTP dostarczony przez producenta oprogramowania. 24. Serwer administracyjny musi umożliwiać wykonywanie zadań kategoryzacji plików, zarówno istniejących na stacjach roboczych  i zasobach sieciowych, jak i nowo powstałych na bazie już   skategoryzowanych plików.   1. Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku. 2. Dla plików skategoryzowanych, wymagana jest możliwość tworzenia reguł dotyczących blokowania i zezwalania na różne operacje, takie jak zapisywanie, przenoszenie, drukowanie,   wysyłanie pocztą, wysyłanie do chmury, przesyłanie komunikatorami itp.   1. Serwer administracyjny musi umożliwiać wyszukiwanie i ochronę plików w oparciu o różne kryteria, takie jak numery kart kredytowych, numer PESEL, numer dowodu osobistego, numer paszportu, wyrażenia regularne, określone ciągi znaków i numer IBAN. 2. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym. 3. Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM. 4. Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP. 5. Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania. 6. System musi ochraniać pocztę e-mail Microsoft 365, sprawdzając każdą wiadomość e-mail wysyłaną przez użytkowników Microsoft 365. 7. System musi ochraniać pliki w Microsoft 365, kontrolując aktywność plików w Microsoft SharePoint, Microsoft OneDrive dla Firm i Microsoft Teams. 8. System musi wykorzystywać mechanizm OCR (optical character recognition), aby wykrywać poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach 9. System musi posiadać możliwość integracji z systemami do analizy danych (PowerBI, Tableau, etc.) 10. System musi zapewniać możliwość zarządzanie szyfrowaniem dysków twardych oraz urządzeń wymiennych. |  |
| 4. | **Przedłużenie wsparcia w zakresie ochrony systemów IT i rozwiązania XDR – 1 szt.**  **Oprogramowanie ma wspierać systemy operacyjne:**   1. **System Operacyjny Windows:**  * Windows 11 October 2024 Update (24H2) * Windows 11 October 2023 Update (23h2) * Windows 10 November 2022 Update (22H2) * Windows 11 September 2022 Update (22H2) * Windows 11 (initial release) * Windows 10 November 2021 Update (21H2) * Windows 10 May 2021 Update (21H1) * Windows 10 October 2020 Update (20H2) * Windows 10 May 2020 Update (20H1) * Windows 10 May 2019 Update (19H1) * Windows 10 October 2018 Update (Redstone 5) * Windows 10 April 2018 Update (Redstone 4) * Windows 10 Fall Creators Update (Redstone 3) * Windows 10 Creators Update (Redstone 2) * Windows 10 Anniversary Update (Redstone 1) * Windows 10 November Update (Threshold 2) * Windows 10 (initial release) * Windows 8.1 * Windows 8 * Windows 7 SP1   **Windows Tablet oraz systemy wbudowane**   * Windows 10 IoT Enterprise * Windows Embedded 8.1 Industry * Windows Embedded 8 Standard * Windows Embedded Standard 7 * Windows Embedded Compact 7 * Windows Embedded POSReady 7 * Windows Embedded Enterprise 7   **Windows ARM64 desktop**   * Windows 11 October 2024 Update (24H2) * Windows 10 November 2022 Update (22H2) * Windows 11 September 2022 Update (22h2) * Windows 10 November 2021 Update (21H2)   **Systemy operacyjne serwera**   * Windows Server 2025 64x * Windows Server 2022 Core * Windows Server 2022 * Windows Server 2019 Core * Windows Server 2019 * Windows Server 2016 * Windows Server 2016 Core * Windows Server 2012 R2 * Windows Server 2012 * Windows Small Business Server (SBS) 2011 * Windows Server 2008 R2  1. **Systemy Operacyjne Linux i wersja kernel**   **parte o RPM**   * RHEL 7.x - 3.10.0 (build 957) 64-bit * RHEL 8.x - 4.18.0 64-bit * RHEL 9.x - 5.14.0 64-bit * Oracle Linux 7.x (UEK) - 4.18.0 64-bit * Oracle Linux 7.x (RHCK) - 3.10.0 build 957 64-bit * Oracle Linux 8.x (UEK) - 5.4.17 / 5.15.0 64-bit * Oracle Linux 8.x (RHCK) – 4.18.0 64-bit * Oracle Linux 9.x (UEK) – 5.15.0 64-bit * Oracle Linux 9.x (RHCK) – 5.14.0 64-bit * CentOS 7.x - 3.10.0 (build 957) 32-bit/64-bit * CentOS 8 Stream - 4.18.0 64-bit * CentOS 9 Stream - 5.14.0 64-bit * Fedora 37 – 40 – wsparcie do wygaśnięcia. 64-bit * AlmaLinux 8.x - 4.18.0 64-bit * AlmaLinux 9.x - 5.14.0 64-bit * Rocky Linux 8.x - 4.18.0 64-bit * Rocky Linux 9.x - 5.14.0 64-bit * CloudLinux 7.x - 3.10 (build 957) 64-bit * CloudLinux 8.x - 4.18.0 64-bit * Miracle Linux 8.x - 4.18.0 64-bit * Kylinv10 RHEL - 4.19.90 64-bit   **Oparte o Debian**   * Debian 9 - 4.9.0 32-bit/64-bit * Debian 10 - 4.19 32-bit/64-bit * Debian 11 - 5.10 32-bit/64-bit * Debian 12 – 6.1.0 64-bit * Ubuntu 16.04.x - 4.8 / 4.10 / 4.13 / 4.15 32-bit/64-bit * Ubuntu 18.04.x - 5.0 / 5.3 / 5.4 64-bit * Ubuntu 20.04.x - 5.4 / 5.8 / 5.11 / 5.13 / 5.15 64-bit * Ubuntu 22.04.x - 5.15 / 5.19 64-bit * Ubuntu 23.04.x – 6.2.0 64-bit * Ubuntu 24.04.x – 6.8.0 64- bit * PopOS 22.04.x – 6.2.6 64-bit * Pardus 21 – 5.10.0 64-bit * Mint 20.x – 5.4.0 64-bit * Mint 21.x – 5.15.0 64-bit * Mint 22.x – 6.8.0.x 64-bit * Zorin OS – 6.5.x 64-bit * Linux Mint Debian Edition 6 – 6.1.x 64-bit   **Oparte o SUSE**   * SLES 12 SP4 - 4.12.14-x 64-bit * SLES 12 SP5 - 4.12.14-x 64-bit * SLES 15 SP1 - 4.12.14-x 64-bit * SLES 15 SP2 - 5.3.18-x 64-bit * SLES 15 SP3 - 5.3.18-x 64-bit * SLES 15 SP4 – 5.14.21 64-bit * SLES 15 SP5 – 5.14.21 64-bit * SLES 15 SP6 – 6.4.x 64-bit * SLED 15 SP4 – 5.14.21 64-bit * openSUSE Leap 15.4 - 15.5 - 5.14.21 64-bit   **Cloud based Linux**   * AWS Bottlerocket 2020.03 - 5.4.x, 5.10.x 64-bit * Amazon Linux v2 - 4.14.x / 4.19.x / 5.10 64-bit * Amazon Linux 2023 – 6.1.x 64-bit * Google COS Milestones 77, 81, 85 - 4.19.112 / 5.4.49 64-bit * Azure Mariner 2 - 5.15 64-bit   **Linux dla ARM**  Oparte o RPM   * RHEL 8.x – 4.18.0-x * RHEL 9.x – 5.14 * AlmaLinux 9.x – 5.14 * Rocky Linux 9.x – 5.14   **Oparte o Debian**   * Debian 11 – 5.10 / 6.1 * Debian 12 – 6.1.0.x * Ubuntu 20.04.x – 5.15 * Ubuntu 22.04.x – 5.15 / 5.19 * Ubuntu 24.04.x – 6.8.0.x   **Oparte o SUSE**   * SLES 15 SP4 – 5.14.21-x * openSUSE Leap 15.4-15.5 – 5.14.21-x   **Oparte o chmurę**   * Amazon Linux v2 – 5.10 * Amazon Linux 2023 - 6.1  1. **Systemy Operacyjne Mac OS X**  * macOS Sequoia (15.x) * macOS Sonoma (14.x) * macOS Ventura (13.x) * macOS Monterey (12.x) * macOS Big Sur (11.x)  1. **Obsługiwane Środowiska Microsoft Exchange**   Security for Exchange ma wspierać następujące wersje i role Microsoft Exchange:   * Exchange Server 2019 z rolą Edge Transport lub Mailbox * Exchange Server 2016 z rolą Edge Transport lub Mailbox * Exchange Server 2013 z rolą Edge Transport lub Mailbox * Exchange Server 2010 z rolą Edge Transport, Hub Transport lub Mailbox   Security for Exchange ma być kompatybilny z Microsoft Exchange Database Availability Groups (DAG).  **Ochrona środowisk wirtualnych (SVE)**   1. Możliwość zastosowania zewnętrznego silnika skanującego w postaci maszyny wirtualnej. 2. Maszyna wirtualna pełniąca rolę silnika skanującego może być pobrana w formacie:    1. OVA    2. XVA    3. VHD    4. VHDX    5. VMDK   **Środowiska wspierane:**   * VMware vSphere and vCenter Server:   + version 6.5   + version 6.7, including update 1, update 2a and update 3   + version 7.0, including update 1, update 2, update 2b, update 2c and update 2d   + version 8.0, including update 1, update 2 * VMware Horizon/View 7.8, 7.7, 7.6, 7.5, 7.1, 6.x, 5.x * VMware Workstation 11.x, 10.x, 9.x, 8.0.6 * VMware Player 7.x, 6.x, 5.x * Citrix Xen Hypervisor: 7.1 (with the XS71ECU2060 hotfix), 8.2. * Citrix Virtual Apps and Desktops 7 1808, 7 1811, 7 1903, 7 1906 * Citrix XenApp and XenDesktop 7.18, 7.17, 7.16, 7.15 LTSR, 7.6 LTSR * Citrix VDI-in-a-Box 5.x * Microsoft Hyper-V Server 2008 R2, 2012, 2012 R2, 2016, 2019 or Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019 (including Hyper-V Hypervisor) * Red Hat Enterprise Virtualization 3.0 (including KVM Hypervisor) * Oracle VM 3.0 * Oracle VM VirtualBox 5.2, 5.1 * Nutanix Prism with AOS 5.6, 5.5, 5.20 LTS, 5.18 STS, 5.15 LTS, 5.11, 5.10 (Enterprise Edition) * Nutanix Prism with AHV 20170830.115, 20170830.301, 20170830.395 and 20190916.294 (Community Edition)   **Ochrona antywirusowa i antyspyware ma być wyposażona w:**   1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 2. Interfejs oraz pomoc techniczna świadczona w języku polskim. 3. Wykrywanie zagrożeń i analiza procesów technikami heurystycznymi. 4. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. 5. Wbudowana technologia do ochrony przed rootkitami. 6. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych  i wykonywanych plików. 7. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie". 8. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 9. Możliwość ustawienia zadania skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu. 10. Możliwość skanowania dysków sieciowych i dysków przenośnych. 11. Skanowanie plików spakowanych i skompresowanych. 12. Ochrona krytycznych kluczy rejestru przed ich wykorzystaniem lub nieautoryzowanym dostępem do nich. 13. Możliwość dodawania wykluczeń na podstawie:     1. Plik     2. Folder     3. Rozszerzenie     4. Proces     5. Hash pliku     6. Hash certyfikatu     7. Nazwa zagrożenia     8. Wiersz poleceń     9. IP/maska 14. Skanowanie poczty opartej o protokoły POP3 i SMTP w czasie rzeczywistym. 15. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie w przeglądarce. 16. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Dodatkowo zdefiniowane są grupy stron przez producenta. 17. Wsparcie przeglądarek Internet Explorer 8+, Mozilla Firefox 30+, Google Chrome 34+, Safari 4+, Microsoft Edge 20+ i Opera 21+ bez konieczności zmian w konfiguracji. 18. Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, RDP, FTPS, SCP/SSH. 19. Program powinien skanować ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe. 20. W GUI programu na punkcie końcowym z systemem Windows oraz macOS możliwość wyświetlenia aktualnej wersji produktu i aktualnej wersji silników. 21. W GUI programu na punkcie końcowym z systemem Windows oraz macOS możliwość wyświetlenia, kiedy była przeprowadzana ostatnia aktualizacja z dokładnością co do dnia i godziny. 22. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń. 23. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy. 24. Administrator musi mieć możliwość ukrycia ikony oprogramowania  w obszarze powiadomień systemu Windows. 25. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na punkcie końcowym Windows  i macOS. 26. Stacje robocze mogą łączyć się do serwera administracyjnego  za pośrednictwem sieci Internet. 27. Oprogramowanie klienckie ma posiadać wbudowaną funkcję do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej. 28. System musi umożliwiać kontrolę dostępu do urządzeń na podstawie interfejsów, do których zostały one podłączone. 29. Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej na podstawie ich wykrycia lub wpisanych ręcznie ID urządzenia lub ID produktu. 30. Funkcja blokowania informacji wysyłanych przez HTTP lub SMTP jak: (adresy e-mail, Piny, Konta bankowe, hasła itp.). 31. Funkcja blokowania wysyłanych informacji konfigurowana zdalnie przez administratora. 32. Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego. 33. Wbudowany IDS. 34. Możliwość wykorzystania funkcji skanowania lokalnego lub hybrydowego ze sprawdzaniem reputacji plików w chmurze. 35. Możliwość tworzenia list sieci zaufanych. 36. Możliwość dezaktywacji funkcji zapory sieciowej. 37. Dodatkowa funkcja ochrony przeciwko znanym zagrożeniom typu ransomware. 38. Użytkownik na punkcie końcowym ma możliwość opóźnienia restartu potrzebnego do zakończenia jednego lub wielu zadań (konfigurowalne w politykach bezpieczeństwa). 39. Komunikacja między konsolą zarządzającą, a punktami końcowymi jest szyfrowana. 40. Wbudowana ochrona przed exploitami wyposażona w minimum 15 różnych technik wykrycia exploitów z możliwością włączenia lub wyłączenia każdej z nich oraz dająca możliwość dodania własnych procesów. Funkcja umożliwia również: 41. Możliwość wymuszenia funkcji DEP systemu Windows. 42. Możliwość wymuszenia relokacji modułów (ASLR) dla Windows. 43. Ochrona przed atakami sieciowymi – Mechanizm obronny przed atakującymi próbującymi uzyskać dostęp do systemu poprzez wykorzystanie luk w sieci. Funkcja ta musi obejmować ochronę przed technikami takimi jak:     1. Pierwszy dostęp.     2. ostęp do poświadczeń.     3. Wykrycie.     4. Crimeware.     5. Ruch boczny. 44. Ochrona przed ransomware - możliwość wykrywania i blokowania ataków typu ransomware niezależnie od tego czy atak został przeprowadzony lokalnie lub zdalnie na punkcie końcowym oraz utworzenie kopii zapasowej plików w momencie szyfrowania,  a w przypadku ataku odzyskanie i przywrócenie ich do pierwotnej lokalizacji. Oprogramowanie musi dać możliwość odzyskania plików na żądanie lub automatycznie, o następujących rozszerzeniach:     1. 3fr, ai, arw, bay, cdr, cer, cr2, crt, crw, dcr, der, dll, dng, doc, docm, docx, dwg, dxf, dxg, eps, erf, exe, indd, jpe, jpeg, jpg, mdf, mef, mrw, nef, nrw, odb, odc, odm, odp, ods, odt, orf, p12, p7b, p7c, pdd, pdf, pef, pem, pfx, ppt, pptm, pptx, psd, pst, ptx, png, r3d, raf, rtf, rw2, rwl, sr2, srf, srw, wb2, wpd, wps, x3f, xlk, xls, xlsb, xlsm, xlsx, msg, py, ini, xml, msi, cab, tsf, dgn, log, gif, csv, avi, mov, mp4 45. System musi wykrywać podatne sterowniki zainstalowane na punkcie końcowym z Windows i Linux. 46. Agent i usługi oprogramowania antywirusowego zainstalowanego na punkcie końcowym muszą być chronione przed próbami manipulacji i naruszenia ich integralności w systemie Windows. 47. Oprogramowanie musi skanować nośniki USB zanim użytkownik zaloguje się do systemu Windows. 48. System musi umożliwiać skanowanie oprogramowania układowego UEFI. 49. System ma umożliwiać przechwytywanie TLS handshake pozwalając na skanowanie ruchu sieciowego bez konieczności deszyfracji. 50. Telemetria - Możliwość przesyłania nieprzetworzonych danych bezpieczeństwa z punktów końcowych z systemem operacyjnym Windows i macOS do SIEM Splunk (wymaga TLS 1.2 lub wyższy) lub z systemem Windows i Linux do serwera Syslog (JSON). 51. Oprogramowanie ma pozwalać na skanowanie punktów końcowych pod kątem wyszukiwania wskaźników naruszeń bezpieczeństwa (IOC).   **Stacje robocze i serwery**   1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. 3. Jedna wersja instalacyjna na stacje robocze i serwery plików Windows. 4. Oprogramowanie musi zawierać monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego. 5. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program powinien pytać o hasło. 6. Produkt i zawartość zabezpieczeń powinny być aktualizowane nie rzadziej niż raz na godzinę. 7. Oprogramowanie ma posiadać możliwość raportowania zdarzeń informacyjnych. 8. Oprogramowanie musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju. 9. Oprogramowanie musi posiadać możliwość skanowania jedynie nowych i zmienionych plików. 10. Oprogramowanie ma posiadać możliwość odblokowania ustawień lokalnych konfiguracji na systemach Windows po doinstalowaniu odpowiedniego modułu. Zmiana ustawień zabezpieczona jest hasłem. 11. Po kliknięciu prawym klawiszem myszy na ikonie programu i wybraniu opcji „O programie”, ma dać możliwość wyświetlenia danych do pomocy technicznej tj: adres strony pomocy, adres e-mail do administratora ochrony, numer telefonu do administratora ochrony z wyłączeniem systemów Linux. 12. Dla maszyn z systemem Linux możliwość wskazania katalogów, które mogą być chronione w czasie rzeczywistym.   **Ochrona Exchange**   1. Rozwiązanie musi zapewniać filtrowanie antymalware dla przychodzącego, wewnętrznego i wychodzącego ruchu mailowego. 2. Rozwiązanie musi wspierać skanowanie "na życzenie" oraz skanowanie według harmonogramu dla skrzynek pocztowych i folderów publicznych, w tym możliwość zarówno wykluczenia konkretnych skrzynek bądź folderów publicznych, jak i skanowania tylko emaili z załącznikami bądź emaili otrzymanych w ciągu określonego czasu. 3. Zdolność konfigurowania różnych akcji wykonywanych na plikach zainfekowanych, podejrzanych oraz niemożliwych do przeskanowania. 4. Możliwość skanowania w poszukiwaniu potencjalnie niechcianych aplikacji (PUA). 5. Możliwość skanowania malware wewnątrz archiwów. 6. Rozwiązanie musi zapewniać filtr antyspamowy dla ruchu mailowego, z możliwością dodania do białej listy konkretnych adresów email  i domen. 7. Możliwość odpytania serwerów Realtime Blackhole List (RBL) zdefiniowanych przez administratorów i odfiltrowania wiadomości zaklasyfikowanych jako spam bazując na reputacji wysyłającego serwera. 8. Zdolność automatycznego oznaczenia jako spam wiadomości mailowych napisanych przy użyciu alfabetów azjatyckich bądź cyrylicy. 9. Zdolność do wykonania zapytań bazujących na chmurze dla udoskonalonej ochrony przeciw nowemu spamowi. 10. Zdolność do podjęcia różnych akcji na wykrytych mailach ze spamem, takich jak poprzedzanie tematu maila konkretną etykietą, usunięcie, przeniesienie do kwarantanny bądź przekierowanie maila  do konkretnej skrzynki pocztowej. 11. Rozwiązanie musi zapewniać funkcjonalności filtrowania zawartości dla przychodzącego, wewnętrznego i wychodzącego ruchu mailowego, bazujące na konkretnym tekście bądź wyrażeniach regularnych zgodnych z tematem maila i/lub jego zawartością. 12. Zdolność do podejmowania różnych akcji na emailach, pasujących do reguł filtrowania treści, takich jak dodawanie prefiksu w postaci taga do tematu maila, usuwanie, wysyłanie do kwarantanny bądź przekierowywanie emaila do konkretnej skrzynki.   **Konsola zdalnej administracji**   1. System musi umożliwiać centralne zarządzanie i konfigurację ochrony wspieranych stacji roboczych i serwerów. 2. Możliwość integracji wielu domen Active Directory. 3. Możliwość uruchomienia zdalnego skanowania wybranych punktów końcowych. 4. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony punktu końcowego (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania na żądanie, zainstalowanych modułów, ostatniej aktualizacji oraz przypisanej polityki). 5. Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci, analityk bezpieczeństwa lub z ustawieniami niestandardowymi. 6. Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, systemu operacyjnego. 7. Możliwość centralnej aktualizacji punktów końcowych z serwera w sieci lokalnej lub z Internetu. 8. Możliwość wysłania linku instalacyjnego bezpośrednio z poziomu konsoli administracyjnej. 9. Możliwość uruchomienia centralnej konsoli jedynie z poziomu przeglądarki internetowej. 10. Możliwość ręcznego (na żądanie) i automatycznego generowania raportów (według ustalonego harmonogramu) oraz wyeksportowanie ich do formatu: pdf i csv. Również zbiorczo w formie archiwum zip. 11. Raport generowany według harmonogramu z możliwością automatycznego wysłania go do osób zdefiniowanych w tym raporcie. 12. Możliwość generowania raportu co godzinę. 13. Pierwsza aktywacja modułu kontroli urządzeń nie wymaga restartu stacji docelowej. 14. Możliwość dodania etykiety do stacji roboczej. 15. Możliwość dezinstalacji oprogramowania antywirusowego innych firm w trakcie instalacji zdalnej. 16. Możliwość przechowywania kwarantanny maksymalnie 180 dni. 17. Możliwość definiowania, czy pliki z kwarantanny mają być przesyłane do producenta i co ile godzin ma się ta czynność odbywać. 18. Po aktualizacji zawartości bezpieczeństwa opcja automatycznego przeskanowania kwarantanny. 19. Wsparcie techniczne mailowe i telefoniczne w j. polskim od poniedziałku do piątku w godzinach 8:00-16:00. W pozostałych godzinach możliwość bezpośredniego kontaktu z producentem (24/7) w j. angielskim. 20. Po integracji z lokalnym Active Directory możliwość przypisywania polityk automatycznie po zalogowaniu do systemu operacyjnego w zależności od tego jaki użytkownik domenowy się zalogował lub do jakiej grupy domenowej on należy. 21. Możliwość automatycznego przypisywania polityk na podstawie reguły lokalizacji. Określenie lokalizacji na podstawie:     1. Zakres adresów IP/IP.     2. Adres bramy.     3. Adres serwera WINS.     4. Adres serwera DNS.     5. Połączenie DHCP sufiksów DNS.     6. Punkt końcowy może rozwiązać hosta.     7. Typ sieci.     8. Nazwa hosta. 22. Uwierzytelnienie dwuskładnikowe realizowane przy pomocy aplikacji kompatybilnej ze standardem RFC6238. 23. Możliwość naprawy instalacji agenta z poziomu konsoli. 24. Możliwość utworzenia reguły, która będzie usuwała punkty końcowe z konsoli zarządzającej, jeżeli punkt końcowy nie połączył się z konsolą przez określoną liczbę dni. Funkcja ta pozwala również na określenie wzoru nazw maszyn, które automatycznie będą usuwane oraz na określenie godziny, o której te maszyny będą usuwane. 25. Możliwość wyświetlania adresu MAC dołączonego do nazwy hosta. 26. Możliwość wyświetlenia czy punkt końcowy jest serwerem czy stacją roboczą. 27. Możliwość wyświetlenia informacji czy zainstalowany na punkcie końcowym system operacyjny to Windows, Linux lub MacOS. 28. Możliwość filtrowania punktów końcowych, które były online w ciągu ostatnich 24 godzin, 7 lub 30 dni. 29. Menu tworzenia paczek instalacyjnych musi określać czy dany moduł jest dostępny dla stacji roboczych Windows, Serwerów Windows, Linux, MacOS. 30. Oprogramowanie umożliwia pobranie oddzielnego pakietu instalacyjnego dla systemów MacOS z Intel x86 oraz oddzielnego dla Apple M oraz osobnego pakietu dla systemów Windows z Intel x86 oraz oddzielnego dla architektury ARM. 31. System umożliwia pobieranie plików poddanych kwarantannie z poziomu centralnej konsoli administracyjnej. 32. Możliwość wygenerowania i zapisania logów na stacji roboczej z poziomu konsoli zarządzającej. 33. Możliwość zarządzania ochroną na serwerach Exchange, tworzenie polityk i konfiguracji zdalnej ochrony. 34. Znaczniki punktów końcowych – oprogramowanie musi umożliwiać przypisywanie znaczników (tagów) do punktów końcowych. Przypisywanie musi odbywać się ręcznie lub automatycznie. Musi istnieć możliwość filtrowania punktów końcowych na podstawie kilku wybranych znaczników w jednym czasie. 35. Ochrona proaktywna oparta o maszynowe uczenie, która działa w fazie poprzedzającej wykonanie. Ochrona ta musi wykrywać zagrożenia takie jak:     1. Ukierunkowane ataki.     2. Podejrzane pliki i ruch w sieci.     3. Exploity.     4. Ransomware.     5. Grayware. 36. Moduł ochrony proaktywnej musi posiadać oddzielne działania jakie będzie podejmował dla plików i oddzielne dla ruchu sieciowego. 37. Moduł ochrony proaktywnej musi działać w trybach, które administrator może dowolnie zmieniać na:     1. Tolerancyjny.     2. Normalny.     3. Agresywny. 38. Zintegrowany sandbox po stronie producenta, który pozwala na analizę pliku:  * Plik może zostać wysłany automatycznie ze stacji roboczej, jeżeli oprogramowanie uzna go za podejrzany lub ręcznie z poziomu konsoli przez administratora. * Możliwość ręcznego przesłania archiwum zabezpieczonego hasłem. * Możliwość ręcznego przesłania adresu URL. * W przypadku ręcznego przesłania wielu plików jednorazowo, możliwość detonacji próbek pojedynczo. * Wbudowany sandbox musi działać w trybie monitorowania i blokowania. * Wbudowany sandbox musi oferować działania naprawcze takie jak dezynfekcja, przeniesienie do kwarantanny lub tylko raportowanie. * Wbudowany sandbox musi oferować opcję wstępnego filtrowania plików z kategorii aplikacje, dokumenty, skrypty, archiwa, maile zapisane do pliku, pod kątem podejrzanego zachowania. * Wbudowany sandbox musi posiadać opcję, która pozwala na dodanie określonych rozszerzeń do wyjątków, pliki z tym rozszerzeniem nie zostaną przesłane do sandboxa. * Minimalny rozmiar pliku jaki może zostać automatycznie przesłany do sandboxa to 1KB. * Maksymalny rozmiar pliku jaki może zostać automatycznie przesłany do sandboxa to 50MB.  1. System zarządzania ryzykiem – Zintegrowany z konsolą zarządzającą system, który pozwala oszacować podatność środowiska na atak na podstawie punktów ryzyka. Punkty ryzyka powinny być przydzielane od 0 do 100, gdzie liczba mniejsza stanowi mniejsze ryzyko, a liczba większa większe ryzyko. System ponadto musi posiadać: 2. Funkcję, która pozwala wyszukiwać podatności ustawień punktów końcowych oraz naprawiać je lub ignorować z podziałem na typ wykrytej konfiguracji:    1. Przeglądarka    2. Sieć    3. System operacyjny    4. Luki 3. System ponadto musi określać nasilenie zagrożenia wynikłego z wykrytej podatności w oparciu o punkty procentowe oraz posiadać funkcję cofnięcia wprowadzonych zmian w ustawieniach systemów. 4. System zarządzania ryzykiem powinien określać luki w wykrytym zainstalowanym oprogramowaniu podając przy tym numer CVE tych luk. 5. System ma pozwalać na śledzenie i wykrywanie ryzykownych działań jakie podejmuje użytkownik na punkcie końcowym wraz z poinformowaniem o liczbie użytkowników, których takie działanie dotyczy oraz jaka jest jego szkodliwość. 6. System ma pozwalać na skanowanie punktów końcowych pod kątem wykrywania ryzyka na podstawie harmonogramu lub pojedynczo utworzonego zadania. 7. System ma pozwalać na raportowanie na ilu urządzeniach wykryto błędną konfigurację i luki w aplikacjach oraz jaka jest ilość takich podatności i ich szkodliwość wyrażona w procentach. 8. System ma pozwalać na wykrywanie podatności w oparciu o standardy bezpieczeństwa zgodne z: CISv8, SOC 2, ISO/IEC 27001:2022, GDPR (EU), NIS2 (EU) oraz DORA (EU). 9. System musi mieć możliwość określenia, które konkretnie zapisy standardów bezpieczeństwa: CISv8, SOC 2, ISO/IEC 27001:2022, GDPR (EU), NIS2 (EU) oraz DORA (EU) nie są spełnione w wyniku wykrytej błędnej konfiguracji. 10. Możliwość scentralizowanego podglądu wykrytych zagrożeń z wszystkich modułów ochrony w jednym miejscu i odfiltrowania ich według daty, kategorii, typu zagrożenia, działań naprawczych i innych. 11. Możliwość ustawienia wymagania zmiany hasła logowania do konsoli co 90 dni. 12. Możliwość zablokowania konta w konsoli, jeżeli użytkownik tego konta podejmował pięć kolejnych prób logowania nieprawidłowym hasłem. 13. Funkcja pojedynczego logowania – Single Sign-on (SSO) przy integracji z Microsoft Azure. 14. Raport podsumowujący - Możliwość podglądu raportu, który streszcza stan środowiska firmowego w ciągu ostatnich 24h, 7 dni lub 30 dni.  Z rozróżnieniem na takie sekcje jak: 15. Zarządzane punkty końcowe. 16. Ilość zajętych miejsc w licencji z rozróżnieniem na stacje robocze Windows, serwery Windows, macOS, Linux oraz fizyczne punkty końcowe i maszyny wirtualne. 17. Pięć rodzajów najczęściej blokowanych zagrożeń. 18. Podział zagrożeń na urządzenia takie jak stacje robocze i serwery. 19. Status incydentów bezpieczeństwa, które wystąpiły. 20. Stan modułów punktów końcowych. 21. Ocena ryzyka firmy. 22. Zablokowane strony WWW w oparciu o wykryte tam szkodliwe oprogramowanie, phishing, oszustwa. 23. Zablokowane techniki ataku sieciowego z podziałem na takie jak wczesny dostęp, dostęp do poświadczeń, wykrycie, ruch boczny, crimeware. 24. Możliwość integracji z innymi systemami poprzez API takich elementów bądź sekcji jak:     1. Firmy     2. Raporty     3. Licencjonowanie     4. Konta     5. Pakiety     6. Incydenty     7. Sieć     8. Kwarantanna     9. Integracje     10. Event Push Service     11. Polityki 25. Early access – Oprogramowanie musi umożliwiać dobrowolne przystąpienie do darmowych testowych programów wczesnego dostępu. Programy wczesnego dostępu powinny umożliwiać testowanie najnowszych funkcji oprogramowania, których nie ma jeszcze w wersji końcowej produktu. Uzyskanie dostępu do programu testowego musi być natychmiastowe. 26. Możliwość utworzenia konsoli typu Partner, która pozwala na zarządzanie wieloma firmami z poziomu jednej scentralizowanej konsoli zarządzającej, konsola partnerska musi umożliwiać: 27. Pobieranie przez partnera plików z kwarantanny podległych firm. 28. Zarządzanie systemem ochrony firm podrzędnych przez Partnera z jednej konsoli lub tworzenie bezpośrednich dostępów użytkowników dla tych firm. 29. Odseparowanie przez administratora konsoli podrzędnej od konsoli partnera nadrzędnego. 30. Profil firmy - Możliwość określenia profilu przedsiębiorstwa w konsoli webowej. Dostępne są kategorie m.in: Lotnictwo, Budownictwo, Edukacja, Służba zdrowia, Handel i inne. 31. System musi umożliwiać wybór trzech poziomów obciążenia procesora dla zadań określonych w harmonogramie skanowania na systemach Linux i macOS. 32. System musi posiadać funkcję wstrzymywania skanowania podczas pracy na baterii. 33. Wbudowany sandbox musi posiadać możliwość przesyłania pliku do analizy z komputera zdalnego za pomocą podanej ścieżki. Wielkość pliku nie może przekraczać 100MB. 34. Filtrowanie wykrytych incydentów bezpieczeństwa m.in. na podstawie:     1. ID.     2. Ostatnia aktualizacja.     3. Status.     4. Osoba przydzielająca.     5. Data utworzenia.     6. Priorytet.     7. Ocena szkodliwości w skali 0-100.     8. Podmioty.     9. Zasoby.     10. Ostatnia faza killchain.     11. Wykonane czynności.     12. Skorelowane incydenty.     13. Typ incydentu. 35. System umożliwia wygenerowanie i pobranie zestawu informacji  z chronionych punktów końcowych w formie archiwum. Funkcja powinna być dostępna dla systemów Windows, Linux oraz macOS. Archiwum musi zawierać co najmniej informacje:     1. Windows        * Logi zainstalowanego agenta.        * Dziennik zdarzeń Windows.        * Informacje o systemie.        * DnsCache.        * Webcache.        * Informacje z głównych katalogów rejestru (SYSTEM, SOFTWARE, DEFAULT, DRIVERS, SAM, SECURITY).        * Harmonogram zadań.        * Historia Powershell (jeśli włączono).        * Linux        * Podstawowy log pomocy technicznej zainstalowanego agenta.        * Certyfikaty.        * Autorun i usługi.        * Informacje sieciowe.        * Informacje systemowe.        * Zainstalowane pakiety.     2. macOS     * - Podstawowy log pomocy technicznej zainstalowanego agenta.     * - Autorun.     * - Lista procesów.     * - Informacje sieciowe.     * - Informacje o systemie. 36. Oprogramowanie musi umożliwiać przegląd konfiguracji punktów końcowych w czasie rzeczywistym poprzez tworzenie zapytań pod kątem wykrywania:     1. historia powłoki.     2. wczytywanie bibliotek .dll z podejrzanej lokalizacji.     3. Sesje logowania z użyciem jawnych danych uwierzytelniających.     4. Arp cache.     5. Ip forwarding.     6. Lista zamontowanych nośników.     7. Konfiguracja ip tables.     8. Połączenia TLS które używają certyfikatów self-signed.     9. Używane rozszerzenia w przeglądarce Chrome.     10. Używane rozszerzenia w przeglądarce Firefox.     11. Używane rozszerzenia w przeglądarce Safari.     12. Źródła apt w systemach Linux.     13. Wyświetlanie zainstalowanych pakietów DEB.     14. Wyświetlanie zainstalowanych pakietów RPM.     15. Pakiety Python zainstalowane w systemie.     16. Lista użytkowników, którzy zostali utworzeni w ciągu ostatnich 30 dni (Linux).     17. Wykrywanie czy aplikacje zdalnego dostępu są zainstalowane w systemie MacOS.     18. Wykrywanie czy Kontrola Kont Użytkowników (UAC) jest wyłączona.     19. Wykrywanie czy SecureBoot jest włączony.     20. Lista zapamiętanych sieci bezprzewodowych.     21. Wykrywa, czy zmienił się domyślny folder startowy użytkownika.     22. Wykrywa, czy zmienił się domyślny folder startowy maszyny. 37. Oprogramowanie musi umożliwiać tworzenie konfigurowalnych reguł, po spełnieniu których może zostać wygenerowany incydent bezpieczeństwa. Funkcja ta powinna:     1. Oferować opcję podjęcia automatycznych działań po spełnieniu warunków tj.: izolacja punktu końcowego, wygenerowanie archiwum diagnostycznego, przesłanie pliku do analizy sandbox, zakończenie procesu i innych.     2. Automatyczne działania zapobiegawcze są zależne od wyboru kategorii.     3. Tworzenie reguł musi być określone poprzez wybór operatora np. „to”, „zawiera”, „jest jednym z” itp. 38. Dotyczyć określonych kryteriów tj. proces, plik, rejestr, połączenia. 39. Zapewniać możliwość tworzenia zapytań YARA. 40. Umożliwiać określenie priorytetu kolejności automatyzacji. 41. Administrator powinien mieć możliwość wyboru poziomu szkodliwości potencjalnie wygenerowanych incydentów (wysokie, średnie i niskie).   **EDR-Endpoint Detection and Response**  Produkt zapewnia szczegółowe informacje o wykrytych incydentach, interaktywną mapę incydentów i działania naprawcze.  **Wspierane systemy operacyjne**  **Systemy desktopowe**   * Windows 11 October 2024 Update (24H2) * Windows 11 October 2023 Update (23H2) * Windows 10 November 2022 Update (22H2) * Windows 11 September 2022 Update (22H2) * Windows 11 (initial release) * Windows 10 November 2021 Update (21H2) * Windows 10 May 2021 Update (21H1) * Windows 10 October 2020 Update (20H2) * Windows 10 May 2020 Update (20H1) * Windows 10 May 2019 Update (19H1) * Windows 10 October 2018 Update (Redstone 5) * Windows 10 April 2018 Update (Redstone 4) * Windows 10 Fall Creators Update (Redstone 3) * Windows 10 Creators Update (Redstone 2) * Windows 10 Anniversary Update (Redstone 1) * Windows 10 November Update (Threshold 2) * Windows 10 (initial release) * Windows 8.1 * Windows 8 * Windows 7 SP1   **Systemy operacyjne dla serwerów:**   * Windows Server 2025 64x * Windows Server 2022 Core * Windows Server 2022 * Windows Server 2019 Core * Windows Server 2019 * Windows Server 2016 * Windows Server 2016 Core * Windows Server 2012 R2 * Windows Server 2012 * Windows Small Business Server (SBS) 2011 * Windows Server 2008 R2   **MacOS:**   * macOS Sequoia (15.x) * macOS Sonoma (14.x) * macOS Ventura (13.x) * macOS Monterey (12.x) * macOS Big Sur (11.x)   **Linux**  **Oparte o RPM**   * RHEL 7.x - 3.10.0 (build 957) 64-bit * RHEL 8.x - 4.18.0 64-bit * RHEL 9x - 5.14.0 64-bit * Oracle Linux 7.x (UEK) - 4.18.0 64-bit * Oracle Linux 7.x (RHCK) - 3.10.0 build 957 64-bit * Oracle Linux 8.x (UEK) - 5.4.17 / 5.15.0 64-bit * Oracle Linux 8.x (RHCK) – 4.18.0 64-bit * Oracle Linux 9.x (UEK) – 5.15.0 64-bit * Oracle Linux 9.x (RHCK) – 5.14.0 64-bit * CentOS 7.x - 3.10.0 (build 957) 32-bit/64-bit * CentOS 8 Stream - 4.18.0 64-bit * CentOS 9 Stream - 5.14.0 64-bit * Fedora 37 – 40 – wsparcie do wygaśnięcia. 64-bit * AlmaLinux 8.x - 4.18.0 64-bit * AlmaLinux 9.x - 5.14.0 64-bit * Rocky Linux 8.x - 4.18.0 64-bit * Rocky Linux 9.x - 5.14.0 64-bit * CloudLinux 7.x - 3.10 (build 957) 64-bit * CloudLinux 8.x - 4.18.0 64-bit * Miracle Linux 8.x - 4.18.0 64-bit * Kylin v10 RHEL - 4.19.90 64-bit   **Oparte o Debian**   * Debian 9 - 4.9.0 32-bit/64-bit * Debian 10 - 4.19 32-bit/64-bit * Debian 11 - 5.10 32-bit/64-bit * Debian 12 – 6.1.0 64-bit * Ubuntu 16.04.x - 4.8 / 4.10 / 4.13 / 4.15 32-bit/64-bit * Ubuntu 18.04.x - 5.0 / 5.3 / 5.4 64-bit * Ubuntu 20.04.x - 5.4 / 5.8 / 5.11 / 5.13 / 5.15 64-bit * Ubuntu 22.04.x - 5.15 / 5.19 64-bit * Ubuntu 23.04.x – 6.2.0 64-bit * Ubuntu 24.04.x – 6.8.0 64- bit * PopOS 22.04.x – 6.2.6 64-bit * Pardus 21 – 5.10.0 64-bit * Mint 20.x – 5.4.0 64-bit * Mint 21.x – 5.15.0 64-bit * Mint 22.x – 6.8.0.x 64-bit * Zorin OS – 6.5.x 64-bit * Linux Mint Debian Edition 6 – 6.1.x 64-bit   **Oparte o SUSE**   * SLES 12 SP4 - 4.12.14-x 64-bit * SLES 12 SP5 - 4.12.14-x 64-bit * SLES 15 SP1 - 4.12.14-x 64-bit * SLES 15 SP2 - 5.3.18-x 64-bit * SLES 15 SP3 - 5.3.18-x 64-bit * SLES 15 SP4 – 5.14.21 64-bit * SLES 15 SP5 – 5.14.21 64-bit * SLES 15 SP6 – 6.4.x 64-bit * SLED 15 SP4 – 5.14.21 64-bit * openSUSE Leap 15.4 - 15.5 - 5.14.21 64-bit   **Cloud based Linux**   * AWS Bottlerocket 2020.03 - 5.4.x, 5.10.x 64-bit * Amazon Linux v2 - 4.14.x / 4.19.x / 5.10 64-bit * Amazon Linux 2023 – 6.1.x 64-bit * Google COS Milestones 77, 81, 85 - 4.19.112 / 5.4.49 64-bit * Azure Mariner 2 - 5.15 64-bit  **Komponenty EDR**   **Główne elementy**   * Sensor EDR, który gromadzi i przetwarza dane dotyczące punktu końcowego i zachowania aplikacji w celu ich raportowania. * Analityka Bezpieczeństwa, komponent służący do interpretacji metadanych gromadzonych przez sensor EDR. * Możliwość instalacji dodatkowego, dedykowanego agenta z sensorem EDR dla urządzeń z systemem Windows, aby rozszerzyć już zainstalowaną równolegle ochronę świadczoną przez innego producenta oprogramowania antywirusowego.   **Wykrywanie podejrzanej aktywności**  Monitorowanie zdarzeń na punktach końcowych w poszukiwaniu oznak ataku i wywoływanie incydentów po wykryciu takiej aktywności.   * Bazowanie na systemach opartych o techniki MITRE ATT&CK i własnej inteligencji. * Zgłaszanie naruszeń jako incydent w module EDR.   **Badanie incydentów i wizualizacja**   1. Produkt zapewnia wsparcie analizy incydentów poprzez dostarczenie narzędzi, które pomagają filtrować, badać i podejmować działania dotyczące wszystkich zdarzeń bezpieczeństwa wykrytych przez czujnik EDR w określonym czasie. 2. Produkt integruje się z bazą wiedzy MITRE ATT&CK i odpowiednio oznacza zdarzenia bezpieczeństwa. 3. Produkt zapewnia zaawansowaną wizualizację zdarzeń bezpieczeństwa z określonymi danymi lub działaniami z następującymi informacjami: 4. Karta podsumowująca zawiera przegląd wpływu zdarzenia i szczegółowe informacje o każdym węźle zdarzenia. 5. Funkcja osi czasu zbiera informacje o rozwoju zdarzenia bezpieczeństwa w kolejności chronologicznej. 6. System gromadzi informacje o działaniach podejmowanych przez produkt w związku ze zdarzeniem bezpieczeństwa.   **Incydenty**   1. Oprogramowanie pozwala na informowanie o zagrożeniach wykrytych i zablokowanych w formie grafu i chronologicznej linii zdarzeń oraz daje możliwość: 2. Filtrowania zdarzeń. 3. Zakończenia procesów. 4. Dodania procesów do czarnej listy. 5. Dodania procesów do białej listy. 6. Izolacji hosta. 7. Przesłania pliku do Sandbox. 8. Sprawdzenia informacji o pliku w Google. 9. Sprawdzenia informacji o pliku w VirusTotal. 10. Możliwość szybkiego podglądu incydentów za pomocą spersonalizowanych widoków list lub widoku domyślnego. 11. Możliwość wyświetlenia 10,20,30,50,100 zdarzeń na jednej stronie. 12. System umożliwia blokowanie na podstawie utworzonych reguł czarnej listy przy pomocy kategorii:     1. Hash MD5 lub SHA256. 13. Pełna ścieżka do aplikacji. 14. Reguła połączenia. 15. Możliwość importu reguł czarnej listy dla hash, ścieżek do aplikacji oraz reguł połączeń z pliku CSV. 16. System musi oferować szeroki zakres filtrowania dodanych reguł blokowania minimum po nazwie pliku, hash pliku, typu hash, ścieżce, protokole porcie/zakresie portów, daty dodania.   **Komponent XDR**   * **Sensor Tożsamości (Identity Sensor),** * **Sensor Sieciowy (Network Sensor),**   **Wymagania funkcjonalne**  **Sensor Tożsamości (Bitdefender XDR Identity Sensor)**  Sensor tożsamości musi spełniać następujące funkcje:   * Integracja z usługą **Active Directory**. * Wykrywanie aktywności związanej z próbami wykorzystania:   + skompromitowanych kont użytkowników,   + kont systemowych oraz kont API,   + tokenów i obiektów uwierzytelniających. * Identyfikacja i sygnalizacja zagrożeń dotyczących protokołu **Kerberos**, w tym:   + ataków typu brute-force z użyciem loginów Kerberos,   + użycia skradzionych biletów Kerberos (ang. ticket),   + żądań biletów z niezalecanym (słabym) szyfrowaniem,   + ataków typu **replay attack**. * Rozpoznawanie rejestracji fałszywego kontrolera domeny AD (ang. rogue domain controller) i prób wstrzyknięcia złośliwego kodu. * Identyfikacja nieautoryzowanego uwierzytelnienia w systemach zdalnych przy użyciu przejętych poświadczeń. * Możliwość automatycznego podjęcia działań zaradczych, takich jak:   + wyłączenie konta użytkownika w AD,   + wymuszenie zmiany hasła – bezpośrednio z poziomu konsoli GravityZone XDR.   **Sensor Sieciowy (Bitdefender XDR Network Sensor)**  Sensor sieciowy powinien działać jako wirtualne urządzenie/appliance, którego funkcje obejmują:   * Stały monitoring ruchu sieciowego wewnętrznego i wychodzącego. * Wykrywanie prób poruszania się lateralnego atakującego (lateral movement). * Wykrywanie prób wyprowadzania danych poza organizację (data exfiltration). * Wykrywanie aktywności sieciowej typowej dla ataków:   + skanowania portów,   + brute-force,   + innych działań mających na celu enumerację i infiltrację sieci. * Zapewnienie pełnego wglądu w działania wykryte przez sensor oraz udostępnianie ich do centralnej konsoli zarządzającej.   **Konsola zarządzania i integracja**   * Wszystkie komponenty muszą być zarządzane centralnie z poziomu platformy. * Platforma powinna umożliwiać:   + podgląd alertów i raportów w czasie rzeczywistym,   + konfigurację reakcji automatycznych (np. blokad, resetów haseł),   + integrację z SIEM/SOAR (opcjonalnie),   + analizę incydentów i powiązanych artefaktów.   **Wymagania techniczne i organizacyjne**   * Rozwiązanie musi działać zgodnie z obowiązującymi standardami bezpieczeństwa (np. ISO/IEC 27001, NIST, RODO). * Wsparcie techniczne min. 12 miesięcy (serwis, aktualizacje, wsparcie producenta).   **Wymagania dotyczące licencjonowania**   * Licencja dla min. [X] użytkowników / punktów końcowych (do określenia przez Zamawiającego). * Licencja powinna obejmować wszystkie funkcjonalności opisane powyżej. * Czas trwania licencji: minimum 12 miesięcy. |  |
| 5. | **Zakup rozwiązania w zakresie kopii zapasowych – 1 szt.**  **Oprogramowania do zabezpieczania danych poprzez mechanizm kopii zapasowych dedykowane dla środowisk serwerowych.**  1. Oprogramowanie musi wspierać co najmniej systemy operacyjne:  • Windows XP i nowsze.  • Windows Server 2003 i nowsze.  • Windows SBS 2011/2008, 2003/2003R2.  • Windows Storage Server 2012/2012R2, 2008R2/2008/2003.  • Windows MultiPoint Server 2012/2011/2010.  • Linux.  2. Zarządzanie systemem kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności:  • Interfejs zarządzania oparty na przeglądarce WWW. Zgodność interfejsu z  większością popularnych przeglądarek www.  • Interfejs musi być zgodny z platformami mobilnymi (możliwość zarządzania  systemem z poziomu urządzenia mobilnego).  • Interfejs musi oferować możliwość prezentacji najważniejszych danych  dotyczących stanu systemu i zadań przez niego realizowanych  w przejrzystej formie graficznej z możliwością dostosowania zawartości, treści i formy prezentacji poszczególnych danych.  • Moduł raportujący z możliwością zdefiniowania zawartości, formy i częstotliwości generowania raportów oraz metody ich dostarczania(wysyłanie na podany adres email lub zapisywanie do wskazanego folderu).  • Możliwość definiowania uprawnień dla administratorów system kopi zapasowych na poziomie dostępu do poszczególnych obiektów (maszyn, hostów, lokalizacji, modułów, itp.).  • Integracja z MS Active Directory na poziomie zarządzania dostępem i administratorami.  • Wsparcie dla Single Sign On dla logowania do systemu.  • Możliwość zarządzania procesem tworzenia kopi zapasowych dla wielu różnych podsieci, również w przypadku stosowania NAT.  • Możliwość definiowania planów wykonywania kopii zapasowych, ich replikacji i zarządzaniem ich retencją (kasowaniem).  • Możliwość tworzenia zcentralizowanych (obejmujących swym zasięgiem wiele maszyn lub ich grupy) planów wykonywania kopii zapasowych.  • Możliwość zdalnej instalacji agentów kopi zapasowych z poziomu konsoli cyberochrony na maszynach z systemem operacyjnym Windows.  • Możliwość zdalnego uaktualniania agentów kopi zapasowych.  • Możliwość zdalnego zarządzania procesem wykonywania kopii zapasowej i odzyskiwania danych.  • Możliwość zdefiniowania dedykowanej maszyny, której agent kopi zapasowej wykonywał będzie czynności zarządzania i replikacji kopii zapasowych z wielu innych maszyn (zadania kopiowania, przenoszenia, konsolidacji plików kopi zapasowej).  • Możliwość zastosowania zcentralizowanych modułów do zarządzania przechowywaniem plików kopii zapasowych.  • Centralny katalog wszystkich danych zapisanych w kopiach zapasowych.  • Wbudowany serwer PXE umożliwiający bootowanie maszyn przez sieć LAN z przygotowanego nośnika startowego.  3. Wykonywanie kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności:  • Kopie zapasowe całych dysków i partycji.  • Kopie zapasowe wybranych plików i folderów.  • Kopia zapasowa udziałów sieciowych.  • Kopie zapasowe aplikacji (Exchange, SQL, SharePoint, Active Directory)  • Kopie zapasowe baz danych Oracle.  • Zapis kopi zapasowych (plikowych i dyskowych) w magazynie chmurowym dostarczanym przez producenta systemu kopi zapasowych.  • Zapis kopi zapasowych na udziały sieciowe.  • Zapis kopi zapasowych na serwer SFTP.  • Zapis kopi zapasowych na dedykowaną ukrytą partycję na maszynie, której  kopia zapasowa jest wykonywana.  • Zapis kopi zapasowych na urządzenia taśmowe (pojedyncze napędy, biblioteki taśmowe, autoloadery), wraz z wsparciem LTO-9.  • Możliwość wyszukiwania plików w kopiach zapasowych.  • Możliwość szyfrowania plików kopi zapasowych.  • Wsparcia dla technologii VSS.  • Deduplikacja kopii zapasowych na poziomie bloków danych. Deduplikacja wykonywana na źródle w celu ograniczenia ilości danych przesyłanych przez sieć.  • Kompresja plików kopi zapasowych.  • Możliwość replikacji kopi zapasowych na kolejne nośniki (dyski, napędy taśmowe, magazyn chmurowy).  • Możliwość zaplanowania zadań związanych weryfikacją, replikacją i retencją plików kopi zapasowych.  4. Oprogramowanie musi umożliwiać odtwarzanie kopii zapasowych w oparciu o co najmniej:  • Odtworzenie całej maszyny (Windows, Linux, Mac) – tzw. Bare Metal Restore.  • Odtworzenie całej maszyny (Windows, Linux, Mac) na innej platformie  sprzętowej niż ta, z której wykonano kopię zapasową.  • Odtworzenie poszczególnych plików i folderów.  • Automatyzacja procesu odtwarzania całych maszyn – np.:  po zbootowaniu maszyny z przygotowanego wcześniej nośnika, powinna zostać odtworzona ostatnia wykonany kopia zapasowa automatycznie, bez konieczności jej wyszukiwania i wskazywania).  • Granularne odtwarzanie baz danych Microsoft Exchange.  • Granularne odtwarzanie skrzynek pocztowych i poszczególnych wiadomości email z Microsoft Exchange.  • Wyszukiwanie i podgląd odtwarzanych wiadomości email.  • Granularne odtwarzanie baz danych Microsoft SQL.  • Możliwość granularnego odtwarzania witryn i plików Microsoft SharePoint.  • Odtwarzanie kontrolerów domeny Microsoft Active Directory.  • Granularne odtwarzanie baz danych Oracle.  • Przywracanie przyrostu względem danych, które już się znajdują na dysku na który przywracana jest kopia zapasowa.  5. Dodatkowe (obowiązkowe) wymagania związane ochroną danych dla systemów Windows 7 i nowszych:  • Ochrona systemów operacyjnych Windows przed złośliwym oprogramowaniem typu ransomware w oparciu o heurystyczne algorytmy identyfikacji i eliminacji zagrożeń.  • Skanowanie oprogramowania celem poszukiwania podatności.  Podatności wypisane muszą być z minimum informacjami takimi jak nazwa produktu który zawiera podatność, maszyny na których znaleziono takie oprogramowanie, stopień ważności w skali CVSS.  6. Przestrzeń chmurowa dostarczana wraz z oprogramowaniem musi spełniać poniższe wymagania:  • W przypadku uzyskania uzasadnionej pewności, że doszło do naruszenia bezpieczeństwa, producent oprogramowania bez zbędnej zwłoki dostarczy informacje o takowym naruszeniu na adres e-mail podany podczas rejestracji konta.  • W przypadku wyżej wymienionego naruszenia, producent podejmie kroki, aby udokumentować, naprawić i zminimalizować skutki naruszenia bezpieczeństwa w odniesieniu do danych osobowych oraz aby zapobiec jego powtórzeniu  • Kopie zapasowe wykonywane do dostarczonej przestrzeni chmurowej oraz ich repliki muszą być przechowywane na terenie Polski.  • Producent przechowuje dane osobowe klienta (dane osobowe oraz kopie zapasowe) przy użyciu technik szyfrowania, minimum AES-256.  • Producent nie wykorzystuje danych osobowych klienta bez anonimizacji w środowiskach programistycznych lub testowych.  • Producent oprogramowania przeprowadza okresowe oceny ryzyka i przeglądy co najmniej raz w roku.  • Infrastruktura (chmurowy magazyn kopii zapasowych) jest zaprojektowana zgodnie z podejściem N+1 (to, co niezbędne +1).  • Producent oprogramowania jest zgodny z standardem bezpieczeństwa ISO 27001 lub SOC 2, a magazyn kopii zapasowych musi być zgodny z certyfikatami ISO 9001, ISO 27001 oraz certyfikację DCOS na minimum 4 poziomie.  • Przestrzeń chmurowa dostarczana wraz z oprogramowaniem to minimum 250GB w ramach jednej licencji, na cały okres jej trwania.  7. Wymagania co do modelu licencjonowania rozwiązania:  • Możliwość zakupu licencji subskrypcyjnych w okresie 1/3/5 lat  • Model licencjonowania oparty na maszynach fizycznych – brak limitów na chronioną ilość danych i aplikacji.  **Oprogramowania do zabezpieczania danych poprzez mechanizm kopi zapasowych dedykowane dla środowisk wirtualizacyjnych.**  1. Oprogramowanie musi wspierać co najmniej systemy operacyjne:  • Dla hosta:  • VMware ESX/ESX(i) 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0.  • Hyper-V.  • Citrix XenServer 4.1.5, 5.5, 5.6, 6.0, 6.1, 6.2, 6.5, 7.0, 7.1, 7.2, 7.3,  7.4, 7.5, 7.6.  • Red Hat Virtualization 4.0, 4.1.  • Linux KVM.  • Oracle VM Server 3.0, 3.3, 3.4.  • Scale Computing Hypercore 8.8, 8.9, 9.0, 9.1, 9.2, 9.3  • Dla maszyn wirtualnych:  • Windows XP (SP3) i nowsze.  • Windows Server 2003 i nowsze.  • Windows SBS 2011/2008, 2003/2003R2.  • Windows Storage Server 2012/2012R2, 2008R2/2008/2003.  • Windows MultiPoint Server 2012/2011/2010.  • Linux OS.  • macOS.  2. Zarządzanie systemem kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności:  • Interfejs zarządzania oparty na przeglądarce WWW. Zgodność interfejsu z większością popularnych przeglądarek www.  • Interfejs musi być zgodny z platformami mobilnymi (możliwość zarządzania systemem z poziomu urządzenia mobilnego).  • Interfejs musi oferować możliwość prezentacji najważniejszych danych dotyczących stanu systemu i zadań przez niego realizowanych  w przejrzystej formie graficznej z możliwością dostosowania zawartości, treści i formy prezentacji poszczególnych danych.  • Moduł raportujący z możliwością zdefiniowania zawartości, formy i częstotliwości generowania raportów oraz metody ich dostarczania (wysyłanie na podany adres email lub zapisywanie do wskazanego folderu).  • Definiowanie uprawnień dla administratorów system kopi zapasowych na poziomie dostępu do poszczególnych obiektów (maszyn, hostów, lokalizacji, modułów, itp.).  • Integracja z MS Active Directory na poziomie zarządzania dostępem i administratorami.  • Wsparcie dla Single Sign On dla logowania do systemu.  • Zarządzanie procesem tworzenia kopi zapasowych dla wielu różnych podsieci, również w przypadku stosowania NAT.  • Definiowanie planów wykonywania kopii zapasowych, ich replikacji i zarządzaniem ich retencją (kasowaniem).  • Tworzenie zcentralizowanych (obejmujących swym zasięgiem wiele maszyn lub ich grupy) planów wykonywania kopi zapasowych.  • Możliwość zdalnej instalacji agentów kopi zapasowych  z poziomu konsoli cyberochrony na maszynach z systemem operacyjnym Windows.  • Zdalne uaktualniania agentów kopi zapasowych.  • Zdalne zarządzanie procesem wykonywania kopii zapasowej i odzyskiwania danych.  • Możliwość zdefiniowania dedykowanej maszyny, której agent kopi zapasowej wykonywał będzie czynności zarządzania  i replikacji kopii zapasowych z wielu innych maszyn (zadania kopiowania, przenoszenia, konsolidacji plików kopi zapasowej).  • Możliwość zastosowania zcentralizowanych modułów do zarządzania przechowywaniem plików kopii zapasowych.  • Centralny katalog wszystkich danych zapisanych w kopiach zapasowych  • Wbudowany serwer PXE umożliwiający bootowanie maszyn przez sieć LAN z przygotowanego nośnika startowego.  3. Wykonywanie kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności:  • Kopie zapasowe całych dysków i partycji.  • Kopie zapasowe wybranych plików i folderów.  • Kopia zapasowa udziałów sieciowych.  • Technologia bezagentowego wykonywania kopii zapasowej dla maszyn wirtualnych (dotyczy Hyper-V i VMWare ESXi).  • Kopie zapasowe aplikacji (Exchange, SQL, SharePoint, Active Directory)  • Kopie zapasowe baz danych Oracle.  • Kopie zapasowe hostów Hyper-V i VMWare ESXi.  • Zapis kopi zapasowych (plikowych i dyskowych)  w magazynie chmurowym dostarczanym przez producenta systemu kopi zapasowych.  • Zapis kopi zapasowych na udziały sieciowe.  • Zapis kopi zapasowych na serwer SFTP.  • Zapis kopi zapasowych na dedykowaną ukrytą partycję na maszynie, której kopia zapasowa jest wykonywana.  • Zapis kopi zapasowych na urządzenia taśmowe (pojedyncze napędy, biblioteki taśmowe, autoloadery).  • Możliwość wyszukiwania plików w kopiach zapasowych.  • Szyfrowanie plików kopi zapasowych.  • Wsparcie dla technologii VSS.  • Deduplikacjia kopi zapasowych na poziomie bloków danych. Deduplikacja wykonywana na źródle w celu ograniczenia ilości danych przesyłanych przez sieć.  • Kompresja plików kopi zapasowych.  • Replikacja kopi zapasowych na kolejne nośniki (dyski, napędy taśmowe, magazyn chmurowy).  • Możliwość zaplanowania zadań związanych weryfikacją, replikacją i retencją plików kopi zapasowych.  4. Oprogramowanie musi umożliwiać odtwarzanie kopii zapasowych w oparciu o co najmniej:  • Odtworzenie całej maszyny (Windows, Linux, Mac) – tzw. Bare Metal Restore  • Odtworzenie całej maszyny (Windows, Linux, Mac) na innej platformie  sprzętowej niż ta, z której wykonano kopię zapasową.  • Odtworzenie całego hosta (Hyper-V i VMWare ESXi) na takiej samej lub innej platformie sprzętowej.  • Odtworzenie poszczególnych plików i folderów.  • Automatyzacja procesu odtwarzania całych maszyn – np.: po zabootowaniu maszyny z przygotowanego wcześniej nośnika, powinna zostać odtworzona ostatnia wykonany kopia zapasowa automatycznie, bez konieczności jej wyszukiwania i wskazywania).  • Granularne odtwarzanie baz danych Microsoft Exchange.  • Granularne odtwarzanie skrzynek pocztowych i poszczególnych wiadomości  email z Microsoft Exchange.  • Wyszukiwanie i podgląd odtwarzanych wiadomości email.  • Granularne odtwarzanie baz danych Microsoft SQL.  • Granularne odtwarzanie witryn i plików Microsoft SharePoint.  • Odtwarzanie kontrolerów domeny Microsoft Active Directory.  • Granularne odtwarzanie baz danych Oracle.  • Przywracanie przyrostu względem danych, które już się znajdują na dysku na który przywracana jest kopia zapasowa.  • Dla hostów VMware ESXi i Hyper-V – uruchomienie maszyny wirtualnej  bezpośrednio z pliku kopii zapasowej bez konieczności odtwarzania całej maszyny na hoście. Możliwość docelowego odtworzenia uruchomionej maszyny z pliku kopii zapasowej na wybranym hoście bez przerywania jej pracy.  5. Dodatkowe (obowiązkowe) wymagania związane ochroną danych dla systemów  Windows 7 i nowszych:  • Ochrona systemów operacyjnych Windows przed złośliwym oprogramowaniem typu ransomware w oparciu  o heurystyczne algorytmy identyfikacji i eliminacji zagrożeń.  • Skanowanie oprogramowania celem poszukiwania podatności.  Podatności wypisane muszą być z minimum informacjami takimi jak nazwa produktu który zawiera podatność, maszyny na których znaleziono takie oprogramowanie, stopień ważności w skali CVSS.  6. Przestrzeń chmurowa dostarczana wraz z oprogramowaniem musi spełniać poniższe  wymagania:  • W przypadku uzyskania uzasadnionej pewności, że doszło do naruszenia bezpieczeństwa, producent oprogramowania bez zbędnej zwłoki dostarczy informacje  o takowym naruszeniu na adres e-mail podany podczas rejestracji konta.  • W przypadku wyżej wymienionego naruszenia, producent podejmie kroki, aby  udokumentować, naprawić i zminimalizować skutki naruszenia bezpieczeństwa w  odniesieniu do danych osobowych oraz aby zapobiec jego powtórzeniu.  • Kopie zapasowe wykonywane do dostarczonej przestrzeni chmurowej oraz ich repliki muszą być przechowywane na terenie Polski.  • Producent przechowuje dane osobowe klienta (dane osobowe oraz kopie zapasowe) przy użyciu technik szyfrowania, minimum AES-256.  • Producent nie wykorzystuje danych osobowych klienta bez anonimizacji w środowiskach programistycznych lub testowych.  • Producent oprogramowania przeprowadza okresowe oceny ryzyka i przeglądy co najmniej raz w roku.  • Infrastruktura (chmurowy magazyn kopii zapasowych) jest zaprojektowana zgodnie z podejściem N+1 (to, co niezbędne +1).  • Producent oprogramowania jest zgodny z standardem bezpieczeństwa ISO 27001 lub SOC 2, a magazyn kopii zapasowych musi być zgodny z certyfikatami ISO 9001, ISO 27001 oraz certyfikację DCOS na minimum 4 poziomie.  • Przestrzeń chmurowa dostarczana wraz z oprogramowaniem to minimum 250GB w ramach jednej licencji, na cały okres jej trwania.  7. Wymagania co do modelu licencjonowania rozwiązania:  • Możliwość zakupu licencji subskrypcyjnych w okresie 1/3/5 lat  • Model licencjonowania oparty na maszynach fizycznych i hostach – brak  limitów na chronioną ilość danych, maszyn wirtualnych i aplikacji) |  |
| 6. | **Zakup rozwiązania w zakresie monitorowania sieci i inwentaryzacji zasobów IT oraz kontroli użytkowników – 1 szt.**   * + - 1. Wymagania ogólne:   Monitorowanie infrastruktury (bezagentowo), ma obejmować serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:   * wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping * wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU) * wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci * wizualizacji urządzeń na mapach z funkcją siatki umożliwiającej korygowanie pozycji ikon na mapie do najbliższej linii siatki * wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła. * wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku * wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach o dowolnym rozmiarze i kolorze * wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie * wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny * zablokowania mapy urządzeń przed przypadkową edycją * serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz  z możliwością definiowania własnych serwisów. * serwerów pocztowych: monitoruje czas logowania do serwisu odbierającego oraz czas wysyłania poczty - program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem) - program ma możliwość wykonywania operacji testowych - program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa * monitorowania serwerów WWW i adresów URL * cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS * obsługi szyfrowania SSL/TLS w powiadomieniach e-mail * obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID * obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych * monitoringu routerów i przełączników wg: - zmian stanu interfejsów sieciowych - ruchu sieciowego - podłączonych stacji roboczych – graficzna prezentacja panelu switcha - ruchu generowanego przez podłączone do portów stacje robocze * serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie * wyświetlania statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu * monitorowania stanu maszyn wirtualnych Vmware: działa, nie działa, wstrzymano * zarządzania stanem maszyn wirtualnych Vmware: wysyłanie poleceń włączenia, wstrzymania i wyłączenia zasilania do każdej maszyny * wydajności systemów Windows: - obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy   + - 1. Dodatkowe wymagana w zakresie modułu inwentaryzacji, ma mieć możliwość: * przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji, * przydzielania dostępu administratorów do zasobów na podstawie praw do oddziałów, * tworzenia powiązań między zasobami a urządzeniami, * tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych, * tworzenia relacji pomiędzy zasobami, * wskazania osób uprawnionych do użycia zasobów poprzez rozbudowane mechanizmy, * definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz, * określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów, * określenia atrybutów dodatkowych tylko dla wybranych typów zasobów, * masową edycję atrybutów zasobów, * definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie, * importu danych z zewnętrznego źródła (.CSV), * przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp., * tworzenia powiązań między zasobami a dokumentami w relacji 1:N, * oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp., * ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności, * generowania zestawienia wszystkich zasobów, w tym urządzeń  i zainstalowanego na nich oprogramowania, * przygotowanie wielu szablonów generowanych dokumentów  i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji, * konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca, * konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca, * archiwizacji i porównywania audytów zasobów, * tworzenia kodów kreskowych dla zasobów, * drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy, * inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet, * możliwość zmiany portu komunikacyjnego wykorzystywanego przez aplikację mobilną dla systemu Android, * inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline), * definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja”).   + - 1. Inwentaryzacja oprogramowania ma zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez: * Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP. * Informacje o aplikacjach używanych w organizacji. * Tworzenie własnych wzorców aplikacji. * Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp. * Informacje o komputerach, na których aplikacja została wykryta. * Zarządzanie posiadanymi licencjami. * Wskazywanie osób odpowiedzialnych za licencję. Wskazanie użytkowników licencji. * Tworzenia powiązań między licencjami a dokumentami w relacji 1:N. * Rozbudowane i konfigurowalne scenariusze zarządzania licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu. * Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych. * Zarządzanie posiadanymi licencjami: raport zgodności licencji. * Możliwość przypisania do programów numerów seryjnych, wartości itp. * Okna audytowe posiadają możliwość filtrowania elementów per oddział.   + - 1. W zakresie obsługi użytkowników program ma umożliwiać monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie: * Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy), * Procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach, * Rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania  w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność, * Informacji o edytowanych przez użytkownika dokumentach, * Historii pracy (cykliczne zrzuty ekranowe), * Listy odwiedzanych stron WWW (tytuły, adresy, liczba i czas wizyt), * Transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika), * Wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program ma możliwość monitorowania kosztów wydruków, * Nagłówków przesyłanej w aplikacjach klienckich poczty e-mail.   + - 1. Program ponadto ma posiadać możliwość: * wykrywania podejrzanej aktywności przez popularne „jigglery”, mającej na celu symulowanie faktycznej pracy. * zdefiniowania czasu (min. 15 minut) gdy wykrywana będzie symulowana aktywność wyłącznie przez ruch myszą bez kliknięcia lub wprowadzanie tego samego znaku z klawiatury. * wyszczególnienia podejrzanej aktywności w raportach. * wygenerowania alarmu i wykonania akcji po wykryciu podejrzanej aktywności. * automatycznego włączenia zapisywania zrzutów ekranowych po wykryciu podejrzanej aktywności. * blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych  sub-domen (np. \*.domena.pl). Reguły w postaci listy domen tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane lub współdzielone pomiędzy grupami lub kontami. * integracji list stron w formie plików .TXT z dowolnego adresu zewnętrznego np. CERT. * skorzystania z wbudowanej listy stron sklasyfikowanych jako zagrożenia. * automatycznego odświeżania list stron zintegrowanych z adresów zewnętrznych. * blokowania ruchu na wskazanych portach TCP/IP, * blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem, * prowadzenia rejestru naruszeń blokad * wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia, naruszy skonfigurowane blokady, * przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika), * definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone. * Możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie. * Mechanizm blokowania uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku. * Reguły w postaci listy blokowanych plików lub lokalizacji tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami. * Program posiada Grupy użytkowników oraz Grupy Inteligentne, które służą do lepszego zarządzania użytkownikami, polityką monitorowania oraz blokowania aplikacji i stron internetowych.   + - 1. **Program, który umożliwia pomoc zdalną dla użytkowników.**     W ramach kontroli stacji użytkownika ma być dostępny podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połącznie i opcją odrzucenia takiego połącznia przez użytkownika (np.  w przypadku pracowników wysokiego szczebla).   * Podczas dostępu zdalnego, zarówno użytkownik jak i administrator widzą ten sam ekran. * Administrator w trakcie zdalnego dostępu ma możliwość wyboru dowolnego ekranu (monitora) oraz zablokowania działania myszy oraz klawiatury dla użytkownika. Funkcja zdalnego dostępu umożliwia równoczesne podłączenie do tego samego komputera kilku administratorom.   W niniejszym module znajduje się baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych poprzez dedykowany portal oraz przetwarzanie wiadomości e-mail, które są przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie.   * Oprogramowanie pozwala na integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0. Moduł umożliwia również przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o sygnalistach”) oraz zawiera dokumenty prawne dot. ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę. * Ma umożliwiać użytkownikom monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron. System umożliwia użycie pośredniego statusu „zgłoszenie rozwiązane” przed ostatecznym zamknięciem zgłoszenia.   Moduł ten musi zawierać również komunikator (czat), który umożliwia prowadzenie rozmów w czasie rzeczywistym oraz archiwizację historii wiadomości pomiędzy zalogowanymi użytkownikami, pracownikami pomocy technicznej i administratorami (wraz z wyszukiwarką rozmów i wiadomości wg słów kluczowych oraz automatycznym oczyszczaniem historii rozmów).  Ponadto czat ma pozwalać na:   * Dostęp do systemu zgłoszeń oraz bazy wiedzy realizowany jest przez dedykowany portal dostępny przez przeglądarkę internetową, który może być wyświetlany w trybie jasnym lub ciemnym. * zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej * rozmowy również między „zwykłymi” użytkownikami * osadzanie załączników w treści wiadomości, * osadzanie obrazków w treści wiadomości, * formatowanie tekstu, * tworzenie pokojów tematycznych, rozmów grupowych * oznaczanie kontaktów jako „ulubionych” na liście kontaktów * uruchomienie z poziomu ikony dostępowej Agenta oraz bezpośrednio w interfejsie WWW heldpesku * może być wyświetlany w trybie jasnym lub ciemnym W module zawarta jest również baza wiedzy pomagająca użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy wraz z możliwością nadawania artykułom 1 z 3 statusów (opublikowany, wewnętrzny, szkic). * Program ma umożliwiać informowanie pracowników o zdarzeniach, np. planowanych przestojach w dostępie do usług, przez komunikaty z graficznym formatowaniem treści oraz łączami do artykułów w bazie wiedzy. * Użytkownik ma możliwość przeglądnięcia historii odczytanych komunikatów bezpośrednio z poziomu ikony Agenta. * Administrator ma możliwość tworzenia szkiców i archiwizowania komunikatów.   Funkcjonalność modułu musi umożliwiać również uzyskanie dostępu  z prywatnego komputera tylko do swojego komputera firmowego, który pozostał w organizacji, za pomocą funkcji zdalnego dostępu przez każdego pracownika. Moduł pomocy zdalnej umożliwia również:  pobieranie listy użytkowników z Active Directory wraz z awatarami,   * wyświetlanie w systemie zgłoszeń wizytówki użytkownika wraz  z jego numerem telefonu, adresem e-mail oraz informacją  o przełożonym, ⎫ zarządzanie lokalnymi kontami Windows  w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont, ⎫ zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez rozbudowany system zarządzania regułami widoczności zgłoszeń, ⎫ zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii zgłoszeń, * zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii artykułów bazy wiedzy, * tworzenie własnego drzewa kategorii zgłoszeń wraz  z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO, * automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników, * definiowanie ścieżek akceptacji zgłoszeń – procesu, w którym użytkownik uzyskuje akceptację na realizację zgłoszenia od wyznaczonych osób w organizacji, * przypisywanie ścieżek akceptacji zgłoszeń do określonych kategorii, * procesowanie zgłoszeń użytkowników z wiadomości e-mail * dostęp do plików źródłowych wiadomości e-mail przetworzonych na zgłoszenia, * obsługę wielu adresów e-mail jednego użytkownika w celu przetwarzania jako zgłoszeń pochodzących od tej samej osoby, * eksportowania listy zgłoszeń do plików CSV i XLSX, * integrację ze wieloma skrzynkami e-mail w celu obsługi różnych kanałów zgłoszeń wraz z automatyzacjami, * integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0, * tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń, * wykonywanie operacji na wielu zgłoszeniach równocześnie, * dołączanie załączników do zgłoszeń, * usuwanie zamkniętych zgłoszeń, * rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy, * szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy  i załączników, * wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia, * zrzuty ekranowe (podgląd pulpitu), * zdalną modyfikację rejestrów, dystrybucję oprogramowania przez Agenty, * definiowanie aplikacji dozwolonych do samodzielnej instalacji przez użytkowników z pakietów MSI w postaci Kiosku  z Aplikacjami, * przypisywanie dostępnych w Kiosku instalatorów do grup użytkowników, * dystrybucję oraz uruchamianie plików za pomocą Agentów  (w tym plików MSI), * zadania dystrybucji plików, jeśli komputer jest wyłączony  w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku, * możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu, * możliwość skonfigurowania automatyzacji dodających komentarze publiczne wraz z załącznikami i odnośnikami  do artykułów w Bazie Wiedzy, * planowanie nieobecności pracowników helpdesk, * obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem, * generowanie raportów obsługi helpdesk, * zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu), * zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami), * wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików bez blokowania interfejsu programu podczas przesyłania plików. Kolejną funkcją oprogramowania jest   + - 1. MOŻLIWOŚĆ OCHRONY DANYCH PRZED WYCIEKIEM poprzez blokowanie urządzeń. * Blokowanie urządzeń i nośników danych. * Program ma możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny. * Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek. * Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA. * Blokownie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane. * Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych. * Funkcje wspierające bezpieczeństwo systemu: integracja  i zarządzanie ustawieniami Windows Defender. * Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker. * Funkcje wspierające bezpieczeństwo systemu: zdalne szyfrowanie dysków za pomocą BitLocker. * Funkcje wspierające bezpieczeństwo systemu: zapisywanie klucza odzyskiwania do pliku oraz jako zasób w bazie danych programu. * Funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu. * Funkcje wspierające bezpieczeństwo systemu: odczytanie informacji o aktywnym oprogramowaniu antywirusowym firm trzecich, innym niż Windows Defender. * Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM.   + - 1. Zarządzanie prawami dostępu do urządzeń: * Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików. 2. 3. 4. 5. * Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive’ów, dysków itp. - urządzenia prywatne są blokowane. * Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników. * Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci. Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. * Przydzielanie uprawnień również do kont użytkowników lokalnych. Program umożliwia prowadzenie rejestru naruszeń blokad podłączanych nośników.   + - 1. Program ma spierać zarządzanie czasem i analizowanie aktywności użytkowników, poprzez dostarczenie informacji  o czasie poświęconym na pracę w poszczególnych aplikacjach i na stronach WWW z dowolnie wybranego okresu. Każdy pracownik organizacji może oznaczyć sesję aktywności jako czas prywatny gdy wykonuje czynności prywatne na sprzęcie firmowym. Może również uzyskać dostęp do własnych wskaźników aktywności w czasie pracy. Menedżerowie oraz przełożeni mogą uzyskać automatyczny dostęp do aktywności podwładnych w zespołach i indywidualnie oraz mogą przeanalizować aktywności w danym okresie i zyskać pełny obraz obszarów wymagających największego zaangażowania. Pracownik może przeglądać swoje historyczne dane, wybierając okres aktywności, który go interesuje. Zastosowane reguły pozwalają zidentyfikować różnego rodzaju rozpraszacze i nieefektywne działania. * Dostęp realizowany jest przez przeglądarkę internetową a strona może być wyświetlana w trybie jasnym lub ciemnym. * Statystyki czasu pracy i osobistej aktywności w wybranym przedziale czasu. * Statystyki aktywności grupy i jej członków widoczne dla menedżera grupy. * Statystyki aktywności podwładnych widoczne dla przełożonego. * Lista odwiedzanych stron internetowych i aplikacji wraz  ze spędzonym na nich czasem. * Podgląd listy użytkowników korzystających z wybranej aplikacji we wskazanym zakresie czasu. * Statystyki popularności stron i aplikacji w organizacji, grupie  i u poszczególnych użytkowników. * Ocena produktywności użytkownika na podstawie czasu spędzonego w aplikacjach i na stronach internetowych. * Grupowanie stron internetowych i aplikacji z podziałem na: produktywne, neutralne i nieproduktywne. * Możliwość przypisywania wyjątków produktywności dla określonych grup użytkowników w przypadku aplikacji globalnie sklasyfikowanych jako nieproduktywne co pozwala na sklasyfikowanie aktywności użytkowników będących członkami takiej grupy jako produktywnej przy ocenie ich pracy. * Jednoczesna edycja klasyfikacji aplikacji pod kątem oceny produktywności oraz przeznaczenia (kategoryzowanie). * Wskaźnik czasu poświęconego na aktywność produktywną. * Definiowanie wymaganego progu produktywności i limitu nieproduktywności, możliwość włączenia dla nich alarmów  e-mail. * Przypisywanie kategorii aplikacjom i stronom internetowym, np. Biuro, Produkcja, Rozrywka - predefiniowana lista kategorii  z możliwością edycji. * Lista kontaktów w organizacji z wbudowaną wyszukiwarką dostępna dla każdego pracownika w organizacji z możliwością ukrycia wybranych kontaktów.   + - 1. Portal informacyjny w formie platformy WWW Oprogramowanie maposiadać również obszar funkcjonalny w formie platformy WWW, który pozwala na tworzenie wielu interaktywnych paneli informacyjnych (dashboardów) z responsywnymi widgetami, których nazwy można zmieniać wg potrzeb. Na każdym  z dashboardów widgety są rozłożone na siatce o rozmiarze ustalonym przez administratora. Zawartość każdego z paneli informacyjnych jest automatycznie odświeżana oraz może być: ⎫ * Udostępniana w trybie „tylko do odczytu” z zabezpieczeniem tokenem. * Wyświetlana w trybie jasnym lub ciemnym (nocnym). Oprogramowanie umożliwia zarządzanie uprawnieniami administratorów do funkcjonalności portalu informacyjnego. Widgety prezentują dane ze wszystkich modułów funkcjonalnych oprogramowania: * Mapa sieci, * Liczniki wydajności, Alarmy (wraz z filtrowaniem) oraz odpowiedzi serwisów TCP/IP, Ostatnie urządzenia w sieci, * Zmiany w konfiguracji sprzętowej urządzeń z Agentami, Zmiany w konfiguracji aplikacyjnej urządzeń z Agentami, Alarmy dla Zasobów, * Statystyki z obszaru wydruków, Statystki użycia aplikacji, Użycie łącza, Aktywność WWW, naruszenia reguł blokad, * Statystyki z obsługi zgłoszeń, Lista najnowszych nierozwiązanych zgłoszeń, Lista najstarszych nierozwiązanych zgłoszeń, Zgłoszenia z naruszonym SLA, Zgłoszenia, których SLA wkrótce wygaśnie, * Ostatnio podłączone nośniki zewnętrzne, Ostatnie operacje na plikach (wraz z filtrowaniem), informacje o stanie Bitlocker, Windows Defender, Windows Firewall, naruszenia reguł dostępu do nośników danych, * Produktywność dla grupy, Statystyki czasu nieproduktywnego. Ochrona przed usunięciem Program jest zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora stacji roboczej, na której pracuje. * Funkcjonalność Agenta Możliwość automatycznego wyszukiwania serwera przez oprogramowanie monitorujące stacje robocze. * Zabezpieczenia Instalator programu jest zabezpieczony podpisem cyfrowym wystawionym i zweryfikowanym przez zaufany globalny urząd certyfikacji (CA). * Globalna wyszukiwarka, zwracająca wyniki obiektów różnego typu na podstawie wyszukiwanych słów kluczowych, np.: urządzenia, użytkownicy, zasoby, elementy interfejsu konsoli zarządzającej, elementy opcji. Program dostępny jest w języku polskim, angielskim, bułgarskim i litewskim, wraz z podręcznikiem Użytkownika w formie strony internetowej. Wsparcie techniczne świadczone jest telefonicznie lub mailowo w języku polskim lub angielskim. |  |
| 7. | **Zakup zarządzanych przełączników sieciowych – 6 szt.**  **Obudowa**   * Obudowa urządzenia musi być przystosowana do montażu  w standardowej szafie 19” i posiadać dwa wbudowane zasilacze * Maksymalne wymiary: * Szerokość – 44,5 cm * Głębokość – 27 cm * Wysokość – 4,5 cm. * Waga do 4 kg   **Pamięć**   * Minimum RAM: 1GB * Minimum FLASH : 64MB   **Interfejsy 1Gb**   * Porty minimum: * Rj-45 100/1000 Mbps - 24 szt. * Gigabit combo (SFP/RJ-45)- 4 szt. * 10-Gigabit SFP+ - 4 szt. * Port konsoli - RS-232c   **Wydajność**   * Potencjał przełączania nie mniejszy niż 136 Gbps * Prędkość przełączania/Przepustowość nie mniejsza niż 101,1 Mbps * Bufor pakietu nie mniejszy niż 4MB * Tabela adresów MAC nie mniejsza niż 32K * Routing table - 12k * IP interface - 256 * Jumbo frame (byte) – 9K * L3 forwarding table (8K IPv4 entries, 4K IPv6 entries)   **Zgodność ze standardami**   * IEEE 802.3 10Base-T Ethernet * IEEE 802.3u 100Base-Tx Ethernet * IEEE 802.3ab 1000Base-T Ethernet * IEEE 802.3z 1000 Base-X * IEEE 802.3az EEE support * IEEE 802.3x flow control   + IEEE 802.3ad LACP aggregation   + IEEE 802.1AB LLDP/LLDP-MED   + IEEE 802.1D Spanning Tree Protocol (STP)   + IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)   + IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)   + IEEE 802.1Q VLAN tagging   + IEEE 802.1p CoS support   + IEEE 802.1X Port authentication   **Odporność i dostępność**   * IEEE 802.1D Spanning Tree Protocol (STP) * IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) * IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) * Equal Cost Multipath Routing (ECMP) * Virtual Router Redundancy Protocol (VRRP) * CPU protection * IEEE 802.3ad LACP * Loop guard * ErrDisable recovery * MRSTP (Zyxel Proprietary) * Dual configuration files * Dual images * Physical stacking   **Kontrola ruchu**   * 802.1Q static VLANs/dynamic VLANs: 4K   + Port-based VLAN and VLAN isolation   + IP classification VLAN   + VLAN counter   + VLAN search   + VLAN translation   + VLAN MAC limit   + Rate limiting: policy-based/portbased bandwidth control with 64 kbps granularity   + CIR/PIR bandwidth control   + Port-based egress traffic shaping   + IEEE 802.1p with 8 priority queues per port   + DSCP/DSCP to 802.1p priority mapping   + Congestion control on all ports   + Selective Q-in-Q   + 802.1ad VLAN stacking (Q-in-Q)   **Bezpieczeństwo**   * 802.1X * Port security * Layer 2 MAC filtering * Layer 3 IP filtering * Layer 4 TCP/UDP socket filtering * Static MAC forwarding * Multiple RADIUS servers * Multiple TACACS+ servers * 802.1x VLAN and 802.1p assignment by RADIUS * Login authentication by RADIUS * Login authentication by TACACS+ * TACACS+ accounting * Authorization on RADIUS * Authorization on TACACS+ * SSH v2 * SSL * Intrusion lock * MAC freeze * MAC search * MAC filtering * DHCP snooping * ARP inspection * Static IP-MAC-Port binding * Policy-based security filtering * Port isolation * Limited MAC number per port * IP source guard * Guest VLAN * IEEE 802.1Q tag-based and portbased VLAN * GVRP automatic VLAN member registration * Full range 4K PVID support * Limited MAC number per port * IP filtering * TCP/UDP socket filtering * BPDU transparency * IEEE 802.1X port-based authentication * Enhanced 802.1X compensation assignment over VLAN * Layer 2 protocol tunneling * Root guard * BPDU guard * Storm control: Broadcast, multicast, unknown unicast (DLF)   **QoS**   * No. of hardware queues per port: 8 * 7802.3x flow control * 802.1p Class of Service (SPQ, WFQ, WRR, hybrid-SPQ combination capable) * DiffServ (DSCP) * Port-based rate limiting (ingress/ egress) * Rate limiting per IP/TCP/UDP per port * Policy-based rate limiting   **Layer 2 Multicast**   * L2 multicast * IGMP snooping v1, v2, v3 * IGMP throttling * IGMP snooping fast leave * IGMP snooping statistics * Multicast VLAN Registration (MVR) * IGMP filtering * IGMP snooping immediate leave * IGMP proxy mode & snooping mode selection * MLD snooping   **Zarządzanie**   * + SNMP v1, v2c, v3   + SNMP trap group   + RMON (1, 2, 3, 9)   + Custom default   + Syslog (IPv4/IPv6)   + ICMP echo/echo reply   + IEEE 802.1AB LLDP   + IEEE 802.1AB LLDP-MED   + Display port utilization   **Zarządzanie IPv6**   * + IPv6 over Ethernet (RFC 2464)   + IPv6 addressing architecture (RFC 4291)   + Dual stack (RFC 4213)   + ICMPv6 (RFC 4443)   + Path MTU (RFC 1981)   + Minimum path MTU size of 1280 (RFC 5095)   + Encapsulation for maximum PMTU of 1500   + Neighbor discovery (RFC 4861)   + DHCPv4/v6 server/relay   + Default DHCP client mode   **Zarządzanie urządzeniem**   * Web interface * Management through Console, Telnet, SNMP * Remote firmware upgrade by FTP/ Web/TFTP * Configuration saving and retrieving * Multiple logins supported * Configure clone * Multilevel CLI * CLI (Cisco-like) * CLV (Cisco-like VLAN) * DHCP relay per VLAN * DHCP client * DHCP option 82 * Daylight saving * NTP * Port mirroring: ingress/egress/both port mirroring * RS-232c local console * sFlow * Microsoft NLB * Auto configuration setup   **Link Aggregation**   * IEEE 802.3ad LACP link aggregation * Static port trunking * Up to 16 aggregation groups, 8 ports per group randomly selected * Link aggregation algorithm of source/destination IP address   **IP Routing**   * Wire-speed IP forwarding * RIP v1, v2 * OSPF * Static routing IPv4/v6 * OSPF summary address * IGMP * DVMRP * ECMP * IP port moving * VRRP * Assigned DHCP relay with specific source IP interface   **MIB**   * + Zyxel private MIB   + RFC 1066 TCP/IP-based MIB   + RFC 1213, 1157 SNMPv2c/v3 MIB   + RFC 1493 bridge MIB   + RFC 1643 Ethernet MIB   + RFC 1757 RMON group 1, 2, 3, 9   + RFC 2011, 2012, 2013 SNMPv2 MIB   + RFC 2233 SMIv2 MIB   + RFC 2358 Ethernet-like MIB   + RFC 2674 bridge MIB extension   + RFC 2819, 2925 remote management MIB   + RFC 3621 power Ethernet MIB   + RFC 4022 management information base for transmission control protocol   + RFC 4113 management information base for user datagram protocol   + RFC 4292 IP forwarding table MIB   + RFC4293 Management Information Base (MIB) for IP   + Cable diagnostic MIB   **Zakres temperaturowy pracy**   * 0°C do 50°C   **Głośność @ 25°C (dBA)**   * Nie większa niż 43,3   **Emisja cieplna (BTU/hr)**   * Nie większa niż 160.27   **Zasilanie**   * Maksymalna moc pobierana przez urządzenie nie może przekraczać 34 W.   **MTBF (hr)**   * Parametr te nie powinien być niższy niż 860,610.82   **Gwarancja**   * Urządzenie powinno posiadać ograniczoną dożywotnią gwarancję producenta   **Serwis**   * W przypadku awarii urządzenia, wysyłka zastępczego produktu ma następować w następnym dniu roboczym, po którym zgłoszona zostanie awaria. Urządzenie powinno być objęte w/w opcją serwisową w okresie nie krótszym niż 5 lat.   **Wymagane certyfikaty**   * Bezpieczeństwo: * LVD * BSMI * EMC * FCC Part 15 (Class A) * CE EMC (Class A) * BSMI EMC * RoHS Level A   **Pozostałe**   * Sprzęt musi być fabrycznie nowy i pochodzić z polskiego kanału dystrybucji |  |
| 8. | **Zakup oprogramowania do ochrony przed wyciekami informacji – 1 szt.**  1. System operacyjny:   * Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi * Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi * MacOS 12 lub nowszy.   2. Serwer administracyjny musi obsługiwać instalację na systemach:   a. Windows Server 2016 (64-bit) i nowszych.  3. Serwer administracyjny musi obsługiwać bazy danych:   * MS SQL Server 2016 lub nowsze, * MS SQL Express, * AzureSQL S3 lub nowsze.   4. Pomoc i dokumentacja programu dostępne w języku angielskim.  5. Konsola administracyjna i komunikaty klienta muszą być w języku polskim.  6. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.  7. Serwer administracyjny musi umożliwiać instalację/dezinstalację zdalnego klienta na stacjach roboczych.  8. Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym.  9. Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia.  10. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli.  11. System musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych, usuwając najstarsze informacje, gdy rozmiar bazy osiągnie skonfigurowany limit.  12. Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania.  13. Administrator musi mieć możliwość aby tworzyć, usuwać i konta administratorów w konsoli programu.  14. Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu).  15. Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory.  16. Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą a serwerem w czasie rzeczywistym.  17. Serwer administracyjny musi umożliwiać ustawienie powiadomień dla użytkownika końcowego w przypadku złamania reguł związanych z ochroną DLP, z możliwością dostosowania grafiki, adresu e-mail i odnośnika do polityki bezpieczeństwa.  18. Administrator musi mieć możliwość wykonać audyt stacji roboczych/użytkowników w oparciu o różne czynności, takie jak uruchomione aplikacje, podłączone urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, wysyłane i odebrane wiadomości email oraz czynności na plikach.  19. Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji i typów plików.  20. Administrator musi mieć możliwość filtrowania i sortowania zebranych danych.  21. Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości email.  22. Dashboardy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu.  23. Serwer administracyjny musi posiadać wbudowany serwer SMTP dostarczony przez producenta oprogramowania.  24. Serwer administracyjny musi umożliwiać wykonywanie zadań kategoryzacji plików, zarówno istniejących na stacjach roboczych i zasobach sieciowych, jak i nowo powstałych na bazie już skategoryzowanych plików.  25. Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku.  26. Dla plików skategoryzowanych, wymagana jest możliwość tworzenia reguł dotyczących blokowania i zezwalania na różne operacje, takie jak zapisywanie, przenoszenie, drukowanie, wysyłanie pocztą, wysyłanie do chmury, przesyłanie komunikatorami itp.  27. Serwer administracyjny musi umożliwiać wyszukiwanie i ochronę plików w oparciu o różne kryteria, takie jak numery kart kredytowych, numer PESEL, numer dowodu osobistego, numer paszportu, wyrażenia regularne, określone ciągi znaków i numer IBAN.  28. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.  29. Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM.  30. Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP.  31. Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania.  32. System musi ochraniać pocztę e-mail Microsoft 365, sprawdzając każdą wiadomość e-mail wysyłaną przez użytkowników Microsoft 365.  33. System musi ochraniać pliki w Microsoft 365, kontrolując aktywność plików w Microsoft SharePoint, Microsoft OneDrive dla Firm i Microsoft Teams.  34. System musi wykorzystywać mechanizm OCR (optical character recognition), aby wykrywać poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach  35. System musi posiadać możliwość integracji z systemami do analizy danych (PowerBI, Tableau, etc.)  36. System musi zapewniać możliwość zarządzanie szyfrowaniem dysków twardych oraz urządzeń wymiennych. |  |

*Dokument należy podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub elektronicznym podpisem osobistym*