Spis treści

1. Firewall UTM

Parametr	Wymagania minimalne	Parametry oferowane
Wymagania Ogólne	System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System wspiera protokoły IPv4 oraz IPv6 w zakresie: Firewall. Ochrony w warstwie aplikacji. Protokołów routingu dynamicznego.	Producent / model _____
Redundancja, monitoring i wykrywanie awarii	W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. Monitoring stanu realizowanych połączeń VPN. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.	Spełnia TAK/NIE*
Interfejsy, Dysk, Zasilanie	System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: 10 portami Gigabit Ethernet RJ-45. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. System jest wyposażony w zasilanie AC.	Spełnia TAK/NIE*
Parametry wydajnościowe	W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.3 Gbps. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum	Spełnia TAK/NIE*

Parametr	Wymagania minimalne	Parametry oferowane
	650 Mbps. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.	
Funkcje Systemu Bezpieczeństwa	W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. 13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).	Spełnia TAK/NIE*
Polityki, Firewall	1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. 5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. • Amazon Web Services (AWS).	Spełnia TAK/NIE*

Parametr	Wymagania minimalne	Parametry oferowane
	• Microsoft Azure. • Cisco ACI. • Google Cloud Platform (GCP). • OpenStack. • VMware NSX. • Kubernetes.	
Połączenia VPN	1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: • Wsparcie dla IKE v1 oraz v2. • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19, 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. • Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. • Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. • Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling” dla połączeń Client-to-Site. 2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. • Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.	Spełnia TAK/NIE*
Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie zapewnia obsługę: Routingu statycznego. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. BFD (Bidirectional Forwarding Detection). Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.	Spełnia TAK/NIE*

Parametr	Wymagania minimalne	Parametry oferowane
Funkcje SD-WAN	System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).	Spełnia TAK/NIE*
Zarządzanie pasmem	System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).	Spełnia TAK/NIE*
Ochrona przed malware	Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.	Spełnia TAK/NIE*
Ochrona przed atakami	Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. System dysponuje sygnaturami do ochrony przed atakami na systemy przemysłowe SCADA. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.	Spełnia TAK/NIE*
Kontrola aplikacji	Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na	Spełnia TAK/NIE*

Parametr	Wymagania minimalne	Parametry oferowane
	wartościach portów TCP/UDP. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).	
Kontrola WWW	Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.	Spełnia TAK/NIE*
Uwierzytelnianie użytkowników w ramach sesji	System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.	Spełnia TAK/NIE*
Zarządzanie	Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.	Spełnia TAK/NIE*

Parametr	Wymagania minimalne	Parametry oferowane
	Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.	
Logowanie	Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. Możliwość włączenia logowania per reguła w polityce firewall. System zapewnia możliwość logowania do serwera SYSLOG. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.	Spełnia TAK/NIE*
Certyfikaty	Poszczególne elementy systemu bezpieczeństwa posiadają następujące certyfikacje: ICSA lub EAL4 dla funkcji Firewall.	Spełnia TAK/NIE*
Testy wydajnościowe oraz funkcjonalne	Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.	
Serwisy i licencje	Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen, Sygnatury ochrony systemów przemysłowych SCADA na okres 12 miesięcy.	Spełnia TAK/NIE* Podać nazwę pakietu licencji: _____
Gwarancja oraz wsparcie	Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.	Spełnia TAK/NIE*
Rozszerzone wsparcie serwisowe	System jest objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 12 miesięcy.	Spełnia TAK / NIE*

Parametr	Wymagania minimalne	Parametry oferowane
AHB/SOS	System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie: Wsparcie telefoniczne zespołu certyfikowanych inżynierów. Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu. Doradztwo w zakresie konfiguracji. Zdalne wsparcie techniczne. Pomoc w zakładaniu zgłoszeń serwisowych u producenta. Pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą). Przygotowanie urządzenia do zdalnej konfiguracji. Zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami użytkownika. Minimum 5 zdalnych rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań użytkownika. Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich. Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich. Dla zapewnienia wysokiego poziomu usług, podmiot serwisujący posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Czas reakcji jest nie dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym. Wymagania powinny być potwierdzone dokumentami: Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). Certyfikat ISO 9001 podmiotu serwisującego.	Oświadczenia i certyfikaty dołączyć do oferty.

2. Komputer przenośny

Szczegółowy opis			Parametry oferowane
Komputer przenośny. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy (numer konfiguracji lub part numer) oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji. Jeśli na stronie internetowej producenta nie jest dostępna pełna oferta modeli sprzętu wraz z jego konfiguracją, do oferty należy dołączyć katalog producenta zaoferowanego produktu umożliwiający weryfikację oferty pod kątem zgodności z wymaganiami Zamawiającego.			Producent: Model: Numer katalogowy (numer konfiguracji lub part numer):
Nie dopuszcza się modyfikacji na drodze Producent-Zamawiający.			
Lp.	**Nazwa komponentu**	**Wymagane minimalne parametry techniczne komputerów**	**Parametry**
	Procesor	Procesor wielordzeniowy ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach przenośnych klasy x86, o wydajności liczonej w punktach równej lub wyższej procesorowi Intel Core i5-1235U na podstawie PerformanceTest w teście CPU Mark według wyników opublikowanych na http://www.cpubenchmark.net/. Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu.	Do oferty należy załączyć wydruk z przeprowadzonych testów na konfiguracji identycznej z zaoferowaną lub link do strony producenta testu z opublikowanym wynikiem.
	Pamięć operacyjna RAM	Min. 16 GB 3200 MHz non-ECC Możliwość rozbudowy pamięci do min. 40GB	
	Parametry pamięci masowej	M.2 256 GB SSD PCIe NVMe Dostępny drugi slot M.2 na dysk SSD. Możliwość rozbudowy do konfiguracji dwudyskowej.	
	Karta graficzna	Zintegrowana z procesorem	
	Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. Wbudowane w obudowie komputera: głośniki Dolby Audio stereo (2x2W), port słuchawek i mikrofonu typu COMBO, kamera video 1080p z mechaniczną zasłoną obiektywu, dwa mikrofony, sterowanie głośnością głośników za pośrednictwem wydzielonych klawiszy funkcyjnych na klawiaturze, wydzielony przycisk funkcyjny do natychmiastowego wyciszania głośników oraz mikrofonu (mute).	
	Obudowa	Wykonana z trwałych materiałów, co najmniej górna pokrywa alumininiowa. Obudowa o podwyższonej odporności spełniająca normy MIL-STD-810H.	Jako potwierdzenie parametrów wytrzymałościowych należy dostarczyć kartę katalogową producenta komputera lub jego oświadczenie dotyczące oferowanego modelu.
	Płyta główna	Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona (na laminacie płyty głównej) na etapie produkcji nazwą producenta oferowanej jednostki i dedykowana dla danego urządzenia. Płyta główna wyposażona w BIOS producenta komputera, zawierający numer seryjny komputera oraz numer seryjny płyty głównej.	
	Zgodność z systemami	Oferowany model komputera musi poprawnie współpracować z zamawianym systemem	

	operacyjnymi	operacyjnym (jako potwierdzenie poprawnej współpracy Wykonawca dołączy do oferty dokument w postaci wydruku potwierdzający certyfikację rodziny produktów bez względu na rodzaj obudowy, dodatkowo potwierdzony przez producenta oferowanego komputera).		
	Bezpieczeństwo	TPM 2.0 Slot umożliwiający fizyczne zabezpieczenie komputera np. Kensington		
	Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji).		
	BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: - wersji BIOS - nr seryjnym komputera - Ilości zainstalowanej pamięci RAM - typie procesora i jego prędkości - informacja o licencji systemu operacyjnego, która została zaimplementowana w BIOS Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności: Możliwość ustawienia hasła Administratora Możliwość ustawienia hasła Użytkownika Możliwość ustawienia hasła dysku twardego Możliwość włączania/wyłączania wirtualizacji z poziomu BIOS Możliwość ustawienia kolejności bootowania oraz wyłączenia poszczególnych urządzeń z listy startowej. Możliwość Wyłączania/Włączania: zintegrowanej karty sieciowej, karty WiFi, czytnika linii papilarnych, mikrofonu, zintegrowanej kamery, portów USB, bluetooth		
	Ekran	Matowy, matryca TFT 15” z podświetleniem w technologii LED, rozdzielczość FHD 1920x1080, 300nits, kontrast 800:1 w technologii IPS/PLS/WVA Kąt otwarcia pokrywy ekranu min.180 stopni.		
	Interfejsy / Komunikacja	4xUSB 3.2 z czego minimum 2 złącza Typu-C umożliwiające podłączenie stacji dokującej lub zasilania notebooka i dodatkowego ekranu (niezależnie od wybranego portu USB-C). Złącze słuchawek i złącze mikrofonu typu COMBO, HDMI min. 1.4b, RJ-45. Komputer musi obsługiwać komunikację Thunderbolt 4 za pomocą min. 1 złącza USB-C. Czytnik kart pamięci.		
	Karta sieciowa WLAN	Wbudowana karta sieciowa, pracująca w standardzie AX 2x2		

		Bluetooth 5.1		
	Klawiatura	Klawiatura odporna na zalanie cieczą, układ US, klawiatura wyposażona w 2 stopniowe podświetlanie przycisków.	Zamawiający wymaga dostarczenia karty katalogowej producenta potwierdzającej odporność klawiatury na zalanie cieczą.	
	Czytnik linii papilarnych	Wbudowany czytnik linii papilarnych w przycisku zasilania		
	Akumulator	Pozwalający na nieprzerwaną pracę urządzenia do min. 6 godzin – załączyć test Mobile Mark 2018 lub kartę katalogową oferowanego komputera potwierdzającą czas pracy na zasilaniu bateryjnym. Ponadto komputer ma być wyposażony w system szybkiego ładowania akumulatora, który umożliwia szybkie naładowanie akumulatora notebooka w czasie 30 minut od 0% do 50%.		
	Zasilacz	Zasilacz zewnętrzny 65W		
	Certyfikaty, oświadczenia i standardy	Dla producenta sprzętu należy dostarczyć: ISO 9001 ISO 14001 ISO 50001 Komputer spełniający: ENERGY STAR 8.0 Epeat Gold Mil-STD-810H Ochronę oczu TÜV Low Blue Light Deklaracja zgodności CE Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji operatora w trybie pracy (IDLE) wynosząca maksymalnie 18,3 dB (załączyć dokument producenta komputera potwierdzający głośność)		
	Waga/Wymiary	Waga urządzenia z akumulatorem max: 1,75 kg Grubość notebooka nie większa niż: 19 mm		
	System operacyjny	Microsoft Windows 11 Pro 64 bit lub system operacyjny klasy PC, który spełnia następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim		

		4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)." 24. Wbudowany mechanizm wirtualizacji typu hypervisor." 25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.	

		26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 34. Możliwość tworzenia wirtualnych kart inteligentnych. 35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38. Mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty inteligentne i certyfikaty (smartcard), c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN e. Certyfikat/Klucz i uwierzytelnienie biometryczne 39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń	
	Oprogramowanie do aktualizacji sterowników	Oprogramowanie producenta oferowanego sprzętu umożliwiające automatyczna weryfikacje i instalację sterowników oraz oprogramowania dołączanego przez producenta w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralna bazą		

		sterowników i oprogramowania producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika.	
	Gwarancja	Minimalny czas trwania wsparcia technicznego producenta wynosi 36 miesięcy w miejscu instalacji. Czas reakcji w następnym dniu roboczym. Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.	
	Wsparcie techniczne producenta	Zaawansowana diagnostyka sprzętowa oraz oprogramowania dostępna 24h/dobę na stronie producenta komputera Infolinia wsparcia technicznego dedykowana do rozwiązywania usterek oprogramowania – możliwość kontaktu przez telefon, formularz web lub chat online, dostępna w dni powszednie od 9:00-18:00 Możliwość sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio na stronie producenta.	
	Bezpieczeństwo i oprogramowanie dodatkowe	System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance +. Silnik musi umożliwiać co najmniej: • wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji, • wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych, • stosowanie kwarantanny, • wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear) • skanowanie urządzeń USB natychmiast po podłączeniu, • automatyczne odłączanie zainfekowanej końcówki od sieci, • skanowanie plików w czasie rzeczywistym, na żądanie, w interwałach czasowych lub poprzez harmonogram, w sposób w pełni konfigurowalny w stosunku do podejmowanych akcji w przypadku wykrycia zagrożenia, z możliwością wykluczenia typu pliku lub lokalizacji. • Zarządzanie „aktywami” stacji klienckiej, zbierające informacje co najmniej o nazwie komputera, producencie i modelu komputera, przynależności do grupy roboczej/domeny, szczegółach systemu operacyjnego, lokalnych kontach użytkowników, dacie i godzinie uruchomienia i ostatniego restartu komputera, parametrach sprzętowych (proc.,RAM, SN, storage), BIOS, interfejsach sieciowych, dołączonych peryferiach. • Musi posiadać moduł ochrony IDS/IPS • Musi posiadać mechanizm wykrywania skanowania portów • Musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania	Producent i nazwa oprogramowania:

		skanowania portów • Moduł wykrywania ataków DDoS musi posiadać kilka poziomów wrażliwości Szyfrowanie danych: • Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. Pełne szyfrowanie dysków działających m.in. na komputerach z systemem Windows. • Zapobiegające utracie danych z powodu utraty / kradzieży punktu końcowego. Oprogramowanie szyfruje całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnia je tylko autoryzowanym użytkownikom. Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej. Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej. Istnieje możliwość blokady zapisywanie plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach. Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji. Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom. Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika. Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną any ransomware. Zaawansowane monitorowanie krytycznych danych użytkownika zapewniające zapobiegające prze niezamierzonymi manipulacjami – ataki ransomware Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej: • Przechowywanie danych w bazie typu SQL, z której korzysta funkcjonalność raportowania konsoli • Zdalną instalację lub deinstalację oprogramowania ochronnego na stacjach klienckich, na pojedynczych punktach, zakresie adresów IP lub grupie z ActiveDirectory • Tworzenie paczek instalacyjnych oprogramowania klienckiego, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi dla Windows oraz formatach dla systemów Linux • Centralną dystrybucję na zarządzanych klientach uaktualnień definicji ochronnych, których źródłem będzie plik lub pliki wgrane na serwer konsoli przez administratora, bez dostępu do sieci Internet.			

		• Raportowanie dostępne przez dedykowany panel w konsoli, z prezentacją tabelaryczną i graficzną, z możliwością automatycznego czyszczenia starych raportów, z możliwością eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i dane/raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich • Definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji Zarządzanie przez Chmurę: 1. Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach 2. Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury 3. Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur 4. Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy 5. Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach 6. Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń 7. Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej Centralna konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, dystrybucji szyfrowania, polityk i centralnie zarządzanie informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych w nagłych przypadkach. Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania. 1. Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer 2. Oprogramowanie klienckie, zarządzane z poziomu serwera. System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej: • różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie • funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD • funkcje regulowania połączeń WiFi i Bluetooth • funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe • funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi • funkcje blokowania dostępu dowolnemu urządzeniu • możliwość tymczasowego dodania dostępu do urządzenia przez administratora • zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu			

		• możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka • możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora • możliwość zarządzani urządzeniami podłączanymi do końcówki, takimi jak iPhone, iPad, iPod, Webcam, card reader, BlackBerry • możliwość używania tylko zaufanych urządzeń sieciowych, w tym urządzeń wskazanych na końcówkach klienckich • funkcję wirtualnej klawiatury • możliwość blokowania każdej aplikacji • możliwość zablokowania aplikacji w oparciu o kategorie • możliwość dodania własnych aplikacji do listy zablokowanych • zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach klientach poprzez konsole administracyjna na serwerze • dodawanie innych aplikacji • dodawanie aplikacji w formie portable • możliwość wyboru pojedynczej aplikacji w konkretnej wersji • dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB • kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool • możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki. • możliwość zablokowania funkcji Printscreen • funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows jak i OSx • funkcje monitorowania i kontroli przepływu poufnych informacji • możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików • możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj • możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe • ochronę przed wyciekiem informacji na drukarki lokalne i sieciowe • ochrona zawartości schowka systemu • ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL • możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych • ochrona plików zamkniętych w archiwach • Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem • możliwość tworzenia profilu DLP dla każdej polityki • wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania • ochrona przez wyciekiem plików poprzez programy typu p2p			

		Monitorowanie zmian w plikach: • Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych. • Funkcje monitorowania określonych rodzajów plików. • Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania. • Generator raportów do funkcjonalności monitora zmian w plikach. • możliwość śledzenia zmian we wszystkich plikach • możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach • możliwość definiowana własnych typów plików Optymalizacja systemu operacyjnego stacji klienckich: • usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku • optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem • możliwość zaplanowania optymalizacje na wskazanych stacjach klienckich • instruktaż stanowiskowy pracowników Zamawiającego • dokumentacja techniczna w języku polskim Wspierane platformy i systemy operacyjne: 1. Microsoft Windows XP/7/8/10/ Professional (32-bit/64-bit) 2. Microsoft Windows Server Web / Standard / Enterprise/ Datacenter (32-bit/64-bit) 3. Mac OS X, Mac OS 10 4. Linux 64-bit, Ubuntu, openSUSE, Fedora 14-25, RedHat Platforma do zarządzania dla Android i iOS: • Musi zapewnić kompleksowy system ochrony i zarządzania urządzeniami mobilnymi z systemami Android oraz iOS a także ich ochronę • Funkcjonalność musi być realizowana za pomocą platformy w chmurze bez infrastruktury wewnątrz sieci firmowej. Zarządzanie użytkownikiem • Musi umożliwiać zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email • Musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, Nazwisko, adres email, Departament, numer telefonu stacjonarnego, numer telefonu komórkowego, typ użytkownika • Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi • Musi posiadać możliwość eksportu danych użytkownika Zarządzanie urządzeniem • Musi umożliwiać wdrożenie przez Email, SMS, kod QR oraz ADO • Musi umożliwiać import listy urządzeń z pliku CSV • Musi umożliwiać dodanie urządzeń prywatnych oraz firmowych • Musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: Data			

		wdrożenia, typ wdrożenia, status wdrożenia, status urządzenia, numer telefonu, właściciel, typ właściciela, grupa, reguły, konfiguracja geolokacji, wersja agenta • Musi umożliwiać podgląd co najmniej następujących informacji sprzętowych: model, producent, system, IMEI, ID SIM, dostawca SIM, adres MAC, bluetooth, Sieć, wolna przestrzeń na dysku, całkowita przeszłość na dysku, bateria, zużycie procesora, sygnał • Musi umożliwiać podgląd lokacji w zakresach czasu: dzisiaj, wczoraj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres • Musi zawierać podgląd aktualnie zainstalowanych aplikacji • Musi zawierać informacje o zużyciu łącza danych, a w tym: Ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych, • Musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł • Moduł raportowania musi umożliwiać podgląd w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres Oprogramowanie pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa: Wymagania dotyczące technologii: 1. Dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową 2. Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta. 3. Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych: - Microsoft Internet Explorer - Microsoft Edge - Mozilla Firefox - Google Chrome - Safari 4. Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących 5. Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie 6. Nod skanujący w postaci aplikacji instalowanej lokalnie dostępny jest na poniższe systemy operacyjne: - Windows 2008 R2 - Windows 2012 - Windows 2012 R2 - Windows 2016 7. Portal zarządzający musi umożliwiać: a) przegląd wybranych danych na podstawie konfigurowalnych widgetów b) zablokowania możliwości zmiany konfiguracji widgetów			

		c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów. d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności e) eksport wszystkich skanów podatności do pliku CSV			

3. Stacje robocze

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów	Parametry oferowane
	Komputer	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu.	Producent: Model: Numer katalogowy (numer konfiguracji lub part numer): Linki stron producenta umożliwiające weryfikacje Do oferty należy załączyć wydruk z przeprowadzonych testów na konfiguracji identycznej z zaoferowaną lub link do strony producenta testu z opublikowanym wynikiem. Zamawiający wymaga dostarczenia karty katalogowej producenta potwierdzającej minimalny wymagany czas pracy na baterii. Producent i nazwa oprogramowania (bezpieczeństwo i oprogramowanie do):
	Obudowa	Typu SFF z obsługą kart PCI Express o niskim profilu. Fabrycznie umożliwiająca montaż min. 2 kieszeni: 1 szt. na napęd optyczny (dopuszcza się stosowanie napedów slim) zewnętrzna, 1 szt. 3,5”na standardowy dysk twardy. Wolna zatoka do rozbudowy o dysk 3,5”/2,5” Wyposażona w czytnik kart multimedialnych - Obudowa trwale oznaczona nazwą producenta, nazwą komputera, numerem MTM, PN, numerem seryjnym - Wyposażona w budowany głośnik o mocy min. 1W	
	Zasilacz	Zasilacz maksymalnie 180W o sprawności minimum 85%	
	Chipset	Dostosowany do zaoferowanego procesora	
	Płyta główna	Zaprojektowana i wyprodukowana przez producenta komputera. Wyposażona w złącza min.: 1 x PCI Express 3.0 x16, 1 x PCI Express 3.0 x1, 2 x M.2 z czego min. 1 przeznaczona dla dysku SSD z obsługą PCIe NVMe	
	Procesor	Procesor wielordzeniowy ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach stacjonarnych klasy x86, o wydajności liczonej w punktach równej lub wyższej procesorowi Intel Core i3-12100 na podstawie PerformanceTest w teście CPU Mark według wyników Avarage CPU Mark opublikowanych na http://www.cpubenchmark.net/. Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu.	
	Pamięć operacyjna	Min. 8GB DDR4 3200MHz z możliwością rozszerzenia do 64 GB Ilość banków pamięci: min. 2 szt. Ilość wolnych banków pamięci: min. 1 szt.	
	Dysk twardy	Min 256GB SSD M.2 PCIe NVMe zawierający RECOVERY umożliwiające odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii.	
	Napęd optyczny	Nagrywarka DVD +/-RW	
	Karta graficzna	Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki w trybie UMA (Unified Memory Access) – z możliwością dynamicznego przydzielenia pamięci.	
	Audio	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition.	
	Karta sieciowa	LAN 10/100/1000 Mbit/s z funkją PXE oraz Wake on LAN WiFi 802.11ax 2x2 + BT 5.1	

	Porty/złącza	Wbudowane porty/złącza: Wideo różnego typu umożliwiające elastyczne podłączenie urządzenia bez stosowania przejściówek lub adapterów za pomocą min: - 1 x VGA, - 1 x HDMI 2.1, - 1 x DisplayPort 1.4, Pozostałe porty/złącza: - 7 x USB w tym: - z przodu obudowy min.3 x USB 3.2, w tym min. 1 x USB typ C - z tyłu obudowy min. 4 x USB, w tym min. 2 x USB 3.2 - port sieciowy RJ-45, - porty słuchawek i mikrofonu na przednim lub tylnym panelu obudowy - czytnik kart pamięci min. SD Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.	
	Klawiatura/mysz	Klawiatura przewodowa w układzie US Mysz przewodowa (scroll)	
	System operacyjny	System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim.	

		10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)." 24. Wbudowany mechanizm wirtualizacji typu hypervisor." 25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).	

		29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 34. Możliwość tworzenia wirtualnych kart inteligentnych. 35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38. Mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty inteligentne i certyfikaty (smartcard), c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN e. Certyfikat/Klucz i uwierzytelnienie biometryczne 39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń	
	BIOS	BIOS zgodny ze specyfikacją UEFI - Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych informacji o: - modelu komputera, PN - numerze seryjnym, - AssetTag, - MAC Adres karty sieciowej, - wersja Biosu wraz z datą produkcji, - zainstalowanym procesorze, jego taktowaniu i ilości rdzeni - ilości pamięci RAM wraz z taktowaniem,	

		- stanie pracy wentylatora na procesorze - napędach lub dyskach podłączonych do portów SATA oraz M.2 (model dysku i napędu optycznego) - wersji systemu operacyjnego preinstalowanego na komputerze Możliwość z poziomu Bios: - wyłączania/włączania portów USB zarówno z przodu jak i z tyłu obudowy - wyłączenia selektywnego (pojedynczego) portów SATA, - wyłączenia karty sieciowej, karty audio, czytnika kart pamięci - możliwość ustawienia portów USB w jednym z dwóch trybów: użytkownik może kopiować dane z urządzenia pamięci masowej podłączonego do pamięci USB na komputer ale nie może kopiować danych z komputera na urządzenia pamięci masowej podłączone do portu USB użytkownik nie może kopiować danych z urządzenia pamięci masowej podłączonego do portu USB na komputer oraz nie może kopiować danych z komputera na urządzenia pamięci masowej - ustawienia hasła: administratora, Power-On, HDD, - blokady aktualizacji BIOS bez podania hasła administratora - wglądu w system zbierania logów (min. Informacja o update Bios, błędzie wentylatora na procesorze, wyczyszczeniu logów) z możliwością czyszczenia logów - alertowania zmiany konfiguracji sprzętowej komputera - załadowania optymalnych ustawień Bios - obsługa Bios za pomocą klawiatury i myszy - możliwość ustawienia polityki dotyczącej haseł (długość i trudność hasła) - możliwość włączenia/wyłączenia Device Guard - możliwość włączenia/wyłączenia uruchomienia komputera za pomocą kombinacji klawiszy na podłączonej klawiaturze	
	Zintegrowany System Diagnostyczny	Wizualny system diagnostyczny producenta działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera umożliwiający na wykonanie diagnostyki następujących podzespołów: wykonanie testu pamięci RAM test dysku twardego lub SSD test monitora test magistrali PCI-e test portów USB test płyty głównej test procesora	

		Wizualna lub dźwiękowa sygnalizacja w przypadku błędów któregokolwiek z powyższych podzespołów komputera. Ponadto system powinien umożliwiać identyfikacje testowanej jednostki i jej komponentów w następującym zakresie: PC: Producent, model BIOS: Wersja oraz data wydania Bios Procesor: Nazwa, taktowanie, ilość pamięci CACHE Pamięć RAM: Ilość zainstalowanej pamięci RAM, producent oraz numer seryjny poszczególnych kości pamięci Dysk: model, numer seryjny, wersja firmware, pojemność, temperatura pracy Monitor: producent, model, rozdzielczość System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera.	
	Certyfikaty i standardy	Certyfikat ISO9001 dla producenta sprzętu (należy załączyć do oferty) Deklaracja zgodności CE (załączyć do oferty) Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki TCO Certified 9.0	
	Waga/rozmiary urządzenia	Waga urządzenia poniżej 4.7 kg Suma wymiarów nie przekraczająca 69 cm	
	Bezpieczeństwo i zdalne zarządzanie	Złącze typu Kensington Lock Oczko na kłódkę TPM 2.0 Czujnik otwarcia obudowy	
	Gwarancja	3 lata świadczona w miejscu użytkowania sprzętu (on-site) Oświadczenie producenta komputera, że w przypadku niewywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.	
	Wsparcie techniczne producenta	Dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej. - możliwość weryfikacji u producenta konfiguracji fabrycznej zakupionego sprzętu - Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.	
	Wymagania dodatkowe	Zamawiający zastrzega sobie prawo sprawdzenia pełnej zgodności parametrów oferowanego sprzętu z wymogami niniejszej SIWZ. W tym celu Wykonawcy na wezwanie Zamawiającego dostarczą do siedziby Zamawiającego w terminie 5 dni od daty otrzymania wezwania, próbkę oferowanego sprzętu. W odniesieniu do programowania mogą zostać dostarczone licencje tymczasowe, w pełni zgodne z oferowanymi. Ocena złożonych próbek zostanie dokonana przez	

		Komisję Przetargową na zasadzie spełnia / nie spełnia. Z badania każdej próbki zostanie sporządzony protokół. Pozytywna ocena próbki będzie oznaczała zgodność próbki (oferty) z treścią SIWZ. Niezgodność próbki z SIWZ chociażby w zakresie jednego parametru podlegającemu badaniu bądź nieprzedłożenie wymaganej próbki w sposób i terminie wymaganym przez Zamawiającego będzie oznaczało negatywny wynik oceny próbki i będzie skutkowało odrzuceniem oferty na podstawie art. 89 ust. 1 pkt 2 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2015 r. poz. 2164 ze zm.), tj. z uwagi na fakt, że treść oferty nie odpowiada treści specyfikacji istotnych warunków zamówienia. Szczegółowy sposób przygotowania i złożenia próbek zostanie dostarczony wykonawcom wraz z wezwaniem do złożenia próbek	
	Bezpieczeństwo i oprogramowanie dodatkowe	System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance +. Silnik musi umożliwiać co najmniej: • wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji, • wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych, • stosowanie kwarantanny, • wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear) • skanowanie urządzeń USB natychmiast po podłączeniu, • automatyczne odłączanie zainfekowanej końcówki od sieci, • skanowanie plików w czasie rzeczywistym, na żądanie, w interwałach czasowych lub poprzez harmonogram, w sposób w pełni konfigurowalny w stosunku do podejmowanych akcji w przypadku wykrycia zagrożenia, z możliwością wykluczenia typu pliku lub lokalizacji. • Zarządzanie „aktywami" stacji klienckiej, zbierające informacje co najmniej o nazwie komputera, producencie i modelu komputera, przynależności do grupy roboczej/domeny, szczegółach systemu operacyjnego, lokalnych kontach użytkowników, dacie i godzinie uruchomienia i ostatniego restartu komputera, parametrach sprzętowych (proc.,RAM, SN, storage), BIOS, interfejsach sieciowych, dołączonych peryferiach. • Musi posiadać moduł ochrony IDS/IPS • Musi posiadać mechanizm wykrywania skanowania portów • Musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania skanowania portów • Moduł wykrywania ataków DDoS musi posiadać kilka poziomów wrażliwości Szyfrowanie danych: • Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. Pełne szyfrowanie dysków działających m.in. na komputerach z systemem Windows. • Zapobiegające utracie danych z powodu utraty / kradzieży punktu końcowego. Oprogramowanie szyfruje całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y,	

		dyski USB i udostępnia je tylko autoryzowanym użytkownikom. Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej. Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej. Istnieje możliwość blokady zapisywanie plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach. Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji. Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom. Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika. Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną any ransomware. Zaawansowane monitorowanie krytycznych danych użytkownika zapewniające zapobiegające prze niezamierzonymi manipulacjami – ataki ransomware Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej: • Przechowywanie danych w bazie typu SQL, z której korzysta funkcjonalność raportowania konsoli • Zdalną instalację lub deinstalację oprogramowania ochronnego na stacjach klienckich, na pojedynczych punktach, zakresie adresów IP lub grupie z ActiveDirectory • Tworzenie paczek instalacyjnych oprogramowania klienckiego, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi dla Windows oraz formatach dla systemów Linux • Centralną dystrybucję na zarządzanych klientach uaktualnień definicji ochronnych, których źródłem będzie plik lub pliki wgrane na serwer konsoli przez administratora, bez dostępu do sieci Internet. • Raportowanie dostępne przez dedykowany panel w konsoli, z prezentacją tabelaryczną i graficzną, z możliwością automatycznego czyszczenia starych raportów, z możliwością eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i dane/raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich • Definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji Zarządzanie przez Chmurę:	

		1. Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach 2. Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury 3. Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur 4. Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy 5. Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach 6. Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń 7. Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej Centralna konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, dystrybucji szyfrowania, polityk i centralnie zarządzanie informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych w nagłych przypadkach. Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania. 1. Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer 2. Oprogramowanie klienckie, zarządzane z poziomu serwera. System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej: • różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie • funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD • funkcje regulowania połączeń WiFi i Bluetooth • funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe • funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi • funkcje blokowania dostępu dowolnemu urządzeniu • możliwość tymczasowego dodania dostępu do urządzenia przez administratora • zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu • możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka • możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora • możliwość zarządzani urządzeniami podłączanymi do końcówki, takimi jak iPhone, iPad, iPod, Webcam, card reader, BlackBerry • możliwość używania tylko zaufanych urządzeń sieciowych, w tym urządzeń wskazanych	

		na końcówkach klienckich • funkcję wirtualnej klawiatury • możliwość blokowania każdej aplikacji • możliwość zablokowania aplikacji w oparciu o kategorie • możliwość dodania własnych aplikacji do listy zablokowanych • zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach klientach poprzez konsole administracyjna na serwerze • dodawanie innych aplikacji • dodawanie aplikacji w formie portable • możliwość wyboru pojedynczej aplikacji w konkretnej wersji • dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB • kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool • możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki. • możliwość zablokowania funkcji Printscreen • funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows jak i OSx • funkcje monitorowania i kontroli przepływu poufnych informacji • możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików • możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj • możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe • ochronę przed wyciekiem informacji na drukarki lokalne i sieciowe • ochrona zawartości schowka systemu • ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL • możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych • ochrona plików zamkniętych w archiwach • Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem • możliwość tworzenia profilu DLP dla każdej polityki • wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania • ochrona przez wyciekiem plików poprzez programy typu p2p Monitorowanie zmian w plikach: • Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych. • Funkcje monitorowania określonych rodzajów plików. • Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania. • Generator raportów do funkcjonalności monitora zmian w plikach. • możliwość śledzenia zmian we wszystkich plikach	

		• możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach • możliwość definiowana własnych typów plików Optymalizacja systemu operacyjnego stacji klienckich: • usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku • optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem • możliwość zaplanowania optymalizacje na wskazanych stacjach klienckich • instruktaż stanowiskowy pracowników Zamawiającego • dokumentacja techniczna w języku polskim Wspierane platformy i systemy operacyjne: 1. Microsoft Windows XP/7/8/10/ Professional (32-bit/64-bit) 2. Microsoft Windows Server Web / Standard / Enterprise/ Datacenter (32-bit/64-bit) 3. Mac OS X, Mac OS 10 4. Linux 64-bit, Ubuntu, openSUSE, Fedora 14-25, RedHat Platforma do zarządzania dla Android i iOS: • Musi zapewnić kompleksowy system ochrony i zarządzania urządzeniami mobilnymi z systemami Android oraz iOS a także ich ochronę • Funkcjonalność musi być realizowana za pomocą platformy w chmurze bez infrastruktury wewnątrz sieci firmowej. Zarządzanie użytkownikiem • Musi umożliwiać zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email • Musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, Nazwisko, adres email, Departament, numer telefonu stacjonarnego, numer telefonu komórkowego, typ użytkownika • Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi • Musi posiadać możliwość eksportu danych użytkownika Zarządzanie urządzeniem • Musi umożliwiać wdrożenie przez Email, SMS, kod QR oraz ADO • Musi umożliwiać import listy urządzeń z pliku CSV • Musi umożliwiać dodanie urządzeń prywatnych oraz firmowych • Musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: Data wdrożenia, typ wdrożenia, status wdrożenia, status urządzenia, numer telefonu, właściciel, typ właściciela, grupa, reguły, konfiguracja geolokacji, wersja agenta • Musi umożliwiać podgląd co najmniej następujących informacji sprzętowych: model, producent, system, IMEI, ID SIM, dostawca SIM, adres MAC, bluetooth, Sieć, wolna przestrzeń na dysku, całkowita przeszłość na dysku, bateria, zużycie procesora, sygnał • Musi umożliwiać podgląd lokacji w zakresach czasu: dzisiaj, wczoraj, ostatnie 7 dni,	

		ostatnie 15 dni, ostatnie 30 dni, własny zakres • Musi zawierać podgląd aktualnie zainstalowanych aplikacji • Musi zawierać informacje o zużyciu łącza danych, a w tym: Ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych, • Musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł • Moduł raportowania musi umożliwiać podgląd w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres Oprogramowanie pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa: Wymagania dotyczące technologii: 1. Dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową 2. Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta. 3. Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych: - Microsoft Internet Explorer - Microsoft Edge - Mozilla Firefox - Google Chrome - Safari 4. Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących 5. Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie 6. Nod skanujący w postaci aplikacji instalowanej lokalnie dostępny jest na poniższe systemy operacyjne: - Windows 2008 R2 - Windows 2012 - Windows 2012 R2 - Windows 2016 7. Portal zarządzający musi umożliwiać: a) przegląd wybranych danych na podstawie konfigurowalnych widgetów b) zablokowania możliwości zmiany konfiguracji widgetów c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów. d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności e) eksport wszystkich skanów podatności do pliku CSV	

4. Serwer NAS

Nazwa komponentu	**Wymagane minimalne parametry techniczne komputerów**	**Parametry**
Procesor	Intel® Celeron® N5105/N5095 4-core/4-thread processor, tryb turbo do max. 2.9 GHz	SPEŁNIA / NIE SPEŁNIA*
Obudowa	Rack 1U o wymiarach: 43,3 × 482,6 × 483,9 mm (wys. x szer. x gł.) wraz z szynami do montażu w szafie rack.	
Pamięć RAM	4 GB SO-DIMM DDR4 (1 x 4 GB)	
Ilość obsługiwanych dysków	4 dyski 3,5-calowe SATA 6 Gb/s, 3 Gb/s	
Dyski	4 dyski kompatybilne z urządzeniem, min. 6TB SATA, 256MB cache	
Interfejsy sieciowe	2 porty 2,5 Gigabit sieci Ethernet (2,5G/1G/100M)	
	obsługa VLAN i Jumbo Frame.	
Porty	2x USB 2.0, 2x USB 3.2 Gen 2, 1x HDMI 1.4b	
Wskaźniki LED	HDD 1–4, stan, LAN, rozszerzenie, zasilanie	
Obsługa RAID	Pojedynczy dysk, JBOD, RAID 0,1,5,5+Spare,6,10. Obsługa BITMAP w celu przyspieszenia odbudowy. Możliwość skonfigurowania Global Spare Disk.	
Funkcje RAID	Możliwość zwiększania pojemności i migracja między poziomami RAID online.	
Szyfrowanie	Możliwość szyfrowania całych woluminów kluczem AES 256 bitów.	
System Operacyjny	Apple Mac OS 10.10 or later Ubuntu 14.04, CentOS 7, RHEL 6.6, SUSE 12 or later Linux IBM AIX 7, Solaris 10 or later UNIX Microsoft Windows 7, 8, and 10 Microsoft Windows Server 2008 R2, 2012, 2012 R2 and 2016, 2019	
Stacja monitoringu	Obsługa minimum 8 kanałów kamer IP	
Protokoły	CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP	
Usługi	Stacja monitoringu, Windows ACL, Integracja w Windows ADS, Serwer wydruku, Serwer WWW, Serwer plików, Manager plików przez WWW, Obsługa paczek QPKG, Funkcja Virtual Disk umożliwiająca zwiększenie pojemności serwera przy pomocy protokołu iSCSI, Montowanie obrazów ISO, Replikacja w czasie rzeczywistym, Serwer RADIUS, Klient LDAP, Serwer Syslog, Virtualization Station	

Zarządzanie dyskami	SMART, sprawdzanie złych sektorów	
Język GUI	Polski	
Gwarancja i serwis	36 miesięcy, producenta	
Waga	8,54 kg (brutto), 6,6 kg (netto)	
Pobór mocy	Uśpienie: 23 W (max) Praca: 37 W (max)	
System plików	Dyski wewnętrzne EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+	
Liczba kont użytkowników	4096	
Liczba grup	512	
Liczba udziałów	512	
Max ilość połączeń (CIFS)	1500	
Max liczba migawek	1024	
Zasilanie	250 W (x1), 100–240 V	
Wentylatory	2 x 80mm, 12VDC	
UPS	Obsługa sieciowych awaryjnych zasilaczy UPS.	

5. Oprogramowanie do tworzenia kopii zapasowych

Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów	Parametry
Ogólne	Oprogramowanie może być dostarczane w dwóch scenariuszach: Cloud(Software as Service), On-premise. Istnieje możliwość migracji w obie strony pomiędzy środowiskiem on-premise oraz cloud. Interfejs systemu dostępny jest w języku: polskim, angielskim, Oprogramowanie nie preferuje platformy sprzętowej, nie jest profilowane pod konkretnego dostawcę sprzętu serwerowego oraz pamięci masowych, Oprogramowanie może być uruchomione w kontenerze docker, Możliwość instalacji oraz uruchomienia serwera zarządzania na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy: Debian: 9+ Ubuntu: 16.04+ Fedora: 29+ centOS: 7+ RHEL: 6+ openSUSE: 15+ SUSE Enterprise Linux (SLES): 12 SP2+ Windows Client: 7, 8.1, 10 (1607+) Windows Server: 2008 R2+, System wykonuje kopię własnej bazy danych, która umożliwia odtworzenie wszystkich ustawień i całej konfiguracji, Oprogramowanie działa w architekturze wykluczającej pojedynczy punkt awarii(awaria jednego z komponentów nie spowoduje przestoju),	SPEŁNIA / NIE SPEŁNIA*
Wsparcie techniczne	Pomoc techniczna w językach: polskim, angielskim. Materiały samopomocowe: Baza wiedzy: polski, angielski	SPEŁNIA / NIE SPEŁNIA*
Zarządzanie	● Zarządzanie całością działania systemu (backup, przywracanie)z poziomu jednej konsoli webowej, ● Zarządzanie całym systemem poprzez dashboardy, ● Gradacja uprawnień kont administratorów z poziomu panelu zarządzającego, ● System posiada wbudowane predefiniowane zadania backupowe,	SPEŁNIA / NIE SPEŁNIA*

Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów	Parametry
	● System umożliwia tworzenie zadań backupowych w oparciu o kalendarz. ● Automatyczne oraz ręczne uruchamianie kopii zapasowych zgodnie z ustalonym harmonogramem, ● Automatyczne oraz ręczne uruchamianie procesu przywracania zgodnie z ustalonym harmonogramem, ● Monitorowanie postępu działania zadania, ● Posiada system powiadamiania poprzez e-mail o zdarzeniach w następujących przypadkach: Zadanie zostało zakończone pomyślnie, Zadanie zostało zakończone z ostrzeżeniami, Zadanie zostało zakończone z błędem, Zadanie zostało anulowane, Zadanie nie zostało uruchomione. ● System generuje alerty na konsoli WEB w przypadku zaistnienia określonego zdarzenia systemowego. ● Możliwość zdefiniowania okna backupowego dla każdego z zadań, ● Oprogramowanie posiada wbudowany menadżer haseł do przechowywania kluczy szyfrujących oraz poświadczeń do magazynów, ● System pozwala na klonowanie planów kopii zapasowych, ● System umożliwia reset hasła administratora w przypadku jego utraty, ● Oprogramowanie umożliwia definiowanie retencji według schematów: GFS(Grandfather-Father-Son), FIFO(First-In, First-Out). ● Oprogramowanie umożliwia tworzenie kont użytkowników nie będących administratorami, ● Konta użytkowników mogą być tworzone poprzez import pliku CSV, ● Oprogramowanie umożliwia tworzenie grup urządzeń, ● Oprogramowanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera(urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera(urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów). ● System pozwala na zarządzanie multi-tenantowe - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.: System Administrator, Backup operator, Restore operator, Viewer.	
Składowanie danych	Oprogramowanie jest systemem multi-storageowym i umożliwia tworzenie wielu repozytoriów danych jednocześnie z poziomu jednej konsoli,	SPEŁNIA / NIE SPEŁNIA*

Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów	Parametry
	System umożliwia składowanie danych: Lokalnie: Zasób SMB, Zasób NFS, Zasób ISCSI, Zasób S3, Katalog zabezpieczonego urządzenia. W chmurze: Amazon Web Service, Magazyn zgodny z S3, Dostarczanej bezpośrednio przez producenta. System pozwala na zdefiniowanie zapasowej ścieżki repozytorium, na wypadek niedostępności głównej lokalizacji, System oferuje mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle. System pozwala na replikację pomiędzy dowolnymi wspieranymi magazynami według ustalonego przez administratora harmonogramu.	
Odtwarzanie	Odtwarzanie granularne: Pojedynczych plików z kopii obrazu dysku, Pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365, Wykorzystanie funkcjonalności Bare Metal Restore(kopii zapasowej całego dysku - łącznie z partycjami i danymi startowymi) dla odtwarzania systemu po awarii, wsparcie dostępne jest dla systemów: Windows: 7+, Windows Server: 2008 R2+, Odtwarzanie Bare metal Restore może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika. Uruchamianie procesu Bare Metal Restore odbywa się z bootowalnej płyty CD lub pendrive'a, Oprogramowanie umożliwia odtwarzanie systemu w scenariuszach: P2P, P2V, V2P, V2V. Oprogramowanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie(VHD, VHDX, VMDK), Odtwarzanie zasobów plikowych bez praw dostępu(tzw. ACL), Odtwarzanie zasobów plikowych z prawami dostępu, Przywracanie plików pomiędzy systemami operacyjnymi(np. odtwarzanie danych plikowych Linux na systemie Windows), Odtwarzanie danych według harmonogramu,	SPEŁNIA / NIE SPEŁNIA*

Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów	Parametry
	Przywracanie danych z określonego urządzenia/użytkownika, Przywracanie kopii z wybranego magazynu. Przywracanie danych Microsoft 365: do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku: pst, mbox. do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji), System posiada możliwość nieodwracalnego kasowania danych, Przywracanie repozytoriów GIT: Przywracanie pomiędzy hostingami repozytoriów(GitHub/BitBucket), przywracanie między kontami.	
Backup	Wykonywanie pełnych, różnicowych, przyrostowych kopii zapasowych, a także backupu syntetycznego dla: Systemów operacyjnych: Alpine 3.10+, Debian: 9+, Ubuntu: 16.04+, Fedora: 29+, centOS: 7+, RHEL: 6+, openSUSE: 15+, SUSE Enterprise Linux(SLES): 12 SP2+, macOS: 10.13+, Windows: 7, 8.1, 10(1607+), Windows Server: 2008 R2+, Środowisk wirtualnych: Hyper-V, VMware: 6.7+. Dowolne inne w sposób agentowy Repozytoriów GIT: GitHub, Bitbucket. Wykonywanie pełnych, różnicowych oraz przyrostowych oraz logów transakcyjnych kopii zapasowych dla: Baz danych: Microsoft SQL, MySQL,	SPEŁNIA / NIE SPEŁNIA*

Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów	Parametry
	PostgreSQL, Firebird, Dowolnych innych przez podpięcie skryptów pre/post. Szyfrowanie danych wykonywana po stronie stacji roboczej za pomocą algorytmu AES w trybie CBC z kluczem szyfrującym o długości: 128 bit, 192 bit, 256 bit. Kompresja danych wykonywana po stronie stacji roboczej za pomocą algorytmów: ZStandard, LZ4. Oprogramowanie umożliwia zarządzanie poziomem kompresji, Wykonywanie kopii zapasowej otwartych plików(VSS), System umożliwia uruchamianie skryptów przed i po backupie, System umożliwia uruchamianie skryptów po wykonaniu migawki VSS, System umożliwia automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku błędów, Backup jednego oraz wielu dysków/całego systemu operacyjnego(Windows) ze wsparciem dla partycji MBR oraz GPT, Backup plikowy, Oprogramowanie realizuje funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie dyskowe, Oprogramowanie umożliwia konsolidację wersji kopii zapasowych, Oprogramowanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia, Oprogramowanie pozwala na automatyczne uruchomienie kopii zapasowej podczas zamykania systemu operacyjnego. Oprogramowanie pozwala na backup zaszyfrowanych partycji. GIT Oprogramowanie zapewnia wsparcie dla repozytoriów lokalnych oraz zdalnych(dostępnych w usługach zewnętrznych), Oprogramowanie umożliwia zabezpieczenie metadanych repozytoriów(w zależności od zabezpieczanej usługi m.in.: issues, pull requests, actions/pipelines, wiki).	
Licencjonowanie	Sposób licencjonowania opiera się na: Ilości serwerów/endpointów- dla fizycznych urządzeń, Ilości fizycznych hostów - dla środowisk wirtualnych, Ilości repozytoriów - dla GIT. Licencje w subskrypcji rocznej powinny pozwalać na :	SPEŁNIA / NIE SPEŁNIA*

Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów	Parametry
	zabezpieczenie 45 fizycznych endpointów zabezpieczenie 1 fizycznego serwera zabezpieczenie 1 fizycznego hosta maszyn wirtualnych Wsparcie techniczne: Świadczone jest w języku polskim, bezpośrednio przez główną siedzibę producenta, Zapewnia dostęp do aktualizacji oprogramowania, Umożliwia korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego, Obowiązuje przez okres 12 miesięcy.	

6. Serwer

Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów	Parametry
Obudowa	typu rack o wysokości 1U o długości 75 cm pozwalająca na montaż 8 dysków twardych 2,5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack	Producent serwera: …….. Model serwera: …… Producent procesora: …….. Model procesora: …… SPEŁNIA / NIE SPEŁNIA*
Procesor	Zainstalowany procesor 10-rdzeniowy o częstotliwości 2.4 GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wynik 15155 Average CPU Mark w teście dostępnym na stronie https://www.cpubenchmark.net/	
Płyta główna	Płyta główna z możliwością zainstalowania dwóch procesorów. Płyta główna zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.	
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych	
Pamięć operacyjna	32GB DDR4 DDR4 2933Mhz ECC Registered, na płycie znajduje się 12 slotów przeznaczonych do instalacji pamięci. Płyta obsługuje do 768GB Pamięci RAM	
Wsparcie dla następujących technologii zabezpieczenia pamięci	ECC, SDDC, ADDDC, Memory mirroring, Memory rank sparing, Patrol & Demand Scrubbing	
Gniazda PCI	trzy sloty PCIe	
Kontroler raid	sprzętowy kontroler umożliwiający konfigurację poziomów raid 0,1,5,10 oraz trybu JBOD	
Dyski twarde	możliwość instalacji dysków SAS,SATA,SSD zainstalowane 2 dyski SSD o pojemnościach 480GB z wytrzymałością na poziomie 2,8 DWPD każdy	
Video	Zintegrowna karta graficzne umożliwiająca wyświetlanie rozdzielczości 1920x1200	
Zasilanie	Zainstalowane dwa zasilacze 750W Platinum Hot Swap	
Wbudowane porty	Przednie: 1x USB 2.0, 1xUSB 3.0 opcjonalna możliwość montażu portu VGA Tylne: 2xUSB 3.0, 1xVGA, opcjonalnie możliwość montażu portu szeregowego	
Karty sieciowe	Wbudowane dwa porty 1Gb Ethernet, możliwość montażu modułu 2x10Gb SFP+ nie zajmującego slotów PCie	

Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów	Parametry
Bezpieczeństwo	wbudowany port TPM 2.0	
Zdalne zarządzanie	Niezależny od systemu operacyjnego system zarządzania wraz z dedykowanym portem pozwalający na: -zbieranie i przegląd informacji o systemie -monitorowanie stanu i kondycji systemu -zdalne sterowanie serwerem (włączenie, wyłączenie, ponowne uruchomienie) -zdalne przeglądanie wideo w rozdzielczości 1920x1200 -możliwość mapowania plików ISO i obrazów przez HTTPS, CIFS i NFS -monitorowanie zużycia energii w czasie rzeczywistym oraz możliwość ograniczenia zużycia energii	
Gwarancja	3 lata z czasem reakcji w następnym dniu roboczym, gwarancja realizowana w miejscu użytkowania sprzętu	

7. Switch zarządzalny – 48 portów

Nazwa komponentu	**Wymagane minimalne parametry techniczne komputerów**	**Parametry**
Typ przełącznika	Zarządzany	Producent: …….. Model: …… SPEŁNIA / NIE SPEŁNIA*
Przełącznik wielowarstwowy	L2+	
Obsługa jakość serwisu (QoS)	Tak	
Zarządzanie przez stronę www	Tak	
Podstawowe przełączanie RJ-45 Liczba portów Ethernet	48	
Podstawowe przełączania Ethernet RJ-45 porty typ	Gigabit Ethernet (10/100/1000)	
Liczba zainstalowanych modułów SFP	4	
Ilość slotów Modułu SFP	4	
Złącze zasilania	DC-in jack	
Standardy komunikacyjne	IEEE 802.3,IEEE 802.3ab,IEEE 802.3u,IEEE 802.3x	
Obsługa 10G	Nie	
Pełny dupleks	Tak	
Podpora kontroli przepływu	Tak	
Agregator połączenia	Tak	
Limit częstotliwości	Tak	
Protokół drzewa rozpinającego	Tak	
Obsługa sieci VLAN	Tak	
Liczba VLANs	64	
Wielkość tabeli adresów	8000 wejścia	
Latency (10-100 Mbps)	20 µs	

Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów	Parametry
Zgodny z Jumbo Frames	Tak	
Pamięci bufora pakietów	1,632 MB	
Funkcje DHCP	DHCP client	
Lista kontrolna dostępu (ACL)	Tak	
Możliwości montowania w stelażu	Tak	
Kolor produktu	Niebieski	
Bezpieczeństwo	UL listed (UL 1950)/cUL, IEC 950/EN 60950	
Certyfikaty	CE mark, commercial FCC Part 15 Class A VCCI Class A EN 55022 (CISPR 22), Class A EN 50082-1 EN 55024 C-Tick	
System operacyjny	Windows, MAC, Linux	
Poziom hałasu	52 dB	
MTBF (Średni okres międzyawaryjny)	108000 h	
Napięcie wejściowe AC	100 - 240 V	
Częstotliwość wejściowa AC	50 - 60 Hz	
Pobór mocy	66 W	
Maksymalne zużycie mocy	70 W	
Obsługa PoE	Nie	
Zakres temperatur (eksploatacja)	0 - 40 °C	
Zakres temperatur (przechowywanie)	-10 - 70 °C	
Zakres wilgotności względnej	0 - 90%	
Dopuszczalna wilgotność względna	0 - 95%	
Dopuszczalna wysokość podczas eksploatacji (n.p.m.)	0 - 3000 m	
Dopuszczalna wysokość (n.p.m.)	0 - 3000 m	
Przewody	LAN (RJ-45)	

8. Switch zarządzalny – 24 porty

Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów	Parametry
Klasa przełącznika	SMART	Producent: ……..
Warstwa przełączania	L2	
Dostęp	SNMP v1/v2c/v3	Model: ……
Architektura sieci	Gigabit Ethernet	
Całkowita liczba portów	26	
Złącza	RJ-45 10/100/1000 Mbps - 24 szt. SFP - 2 szt.	
Obsługiwane protokoły i standardy	- IEEE 802.3 10BASE-T Ethernet	SPEŁNIA / NIE SPEŁNIA*

Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów	Parametry
	- IEEE 802.3u 100BASE-TX Fast Ethernet - IEEE 802.3ab 1000BASE-T Gigabit Ethernet - IEEE 802.3x full-duplex	
QoS	DSCP - L3 QoS • 802.1p-based prioritization • Layer 3-based prioritization • Rate-limiting	
Zarządzanie, monitorowanie, konfiguracja	- IGMP snooping v1/v2 - IEEE 802.1x (RAIDUS) - Access control list (ACL) - MAC, IP - SNTP - IEEE 802.1ab LLDp - HTTP and HTTPS - Zabezpieczenie przed (DoS) - Syslog - Ping & traceroute - Konfiguracja poprzez web - Zapis oraz odczyt konfiguracji - Dostęp zabezpieczony hasłem	
Rozmiar tablicy MAC	8 k	
Ramka Jumbo	9,216 B	
Liczba grup VLAN	128	
Algorytm przełączania	Store-and-forward	
Przepustowość	48 Gb/s	
Bufor pamięci	512 kB	
Dodatkowe informacje	Link Aggregation	
Typ obudowy	Rack	
Zasilacz	Wewnętrzny	
Pobór mocy	21.5 W	
Czas pracy pomiędzy awariami (MTBF)	465998 h	
Akcesoria w zestawie	- GS724T - Podkładki - Kabel zasilający - Zestaw do instalacji w szafie - Smart Switch CD zawierający materiały - Smart Switch Instrukcja instalacji - Karta z informacją na temat gwarancji	
Zasilanie	100-240V AC/50-60 Hz	

9. Szkolenie - Wdrożenie i szkolenie z zakupionych technologii

- Wdrożenie realizowane jest bezpośrednio przez wykonawcę
- Inżynier prowadzący szkolenie i wdrożenie musi posiadać certyfikat NSE7
- Wdrożenie realizowane jest w formie zdalnej
- Komunikacja musi odbywać się w języku polskim,
- Wdrożenie obejmuje pełną konfigurację wszystkich zakupionych urządzeń.
- Czas wdrożenia – 14 dni od dostarczenia sprzętu.
- Wdrożenie zakończone jest szkoleniem z obsługi oprogramowania urządzenia UTM.