Załącznik nr 2.5 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA Przedmiotem zamówienia jest dostawa urządzeń oraz oprogramowania. **Przedmiot zamówienia obejmuje niżej wymieniony asortyment**	
Cecha/ Funkcjonalność	**Minimalne parametry wymagane przez Zamawiającego**
Macierz blokowa – rozbudowa – 1komplet	
Wymagania	1. Zamawiający wymaga rozbudowy posiadanej infrastruktury, tj. systemu pamięci masowej Hitachi E590o dyski klasy Enterprise w liczbie nie mniejszej niż 16 sztuk, o pojemności nie mniejszej niż 3.8TB NVMe SSD -każdy, zapewniających pojemność użytkową min. 43 TB. Obecna konfiguracja wymaga zwiększenia pojemności i wydajności w związku z planowanym rozszerzeniem usług oraz wzrostem zapotrzebowania na przestrzeń do przechowywania danych. 2. Zamawiający wymaga, aby dostarczone dyski były w pełni kompatybilne z posiadanym modelem E590, zarówno pod względem sprzętowym, jak i oprogramowania zarządzającego, a w szczególności aby w wyniku rozbudowy zachowane zostało pełne wsparcia producenta oraz zgodność z obowiązującymi umowami serwisowymi. 3. Rozbudowa powinna opierać się na dyskach klasy Enterprise, zoptymalizowanych pod kątem pracy z dużym obciążeniem i wysoką dostępnością. 4. Zamawiający wymaga, aby proponowane rozwiązanie pozwalało na uruchomienie nowych maszyn wirtualnych oraz rozszerzenie istniejących wolumenów bez przestojów i ingerencji w działające systemy. Zamawiający wymaga dostawy ewentualnych dodatkowych komponentów niezbędnych do instalacji, w szczególności tacki montażowe, kable czy licencje. 5. Zamawiający wymaga, aby rozbudowa została przeprowadzona z zachowaniem najlepszych praktyk oraz zgodnie z wytycznymi producenta sprzętu. 6. Dyski muszą pochodzić z polskiego autoryzowanego kanału sprzedaży.
Macierz obiektowa – 2 szt.	
Typ obudowy	Urządzenie do montażu w szafie typu RACK 19”, z wszystkimi elementami potrzebnymi do montażu. Maksymalna wysokość rozwiązania 4U.
Przestrzeń dyskowa	Macierz musi udostępniać przestrzeń zbudowaną w oparciu o minimum: 18 dysków HDD o pojemności min. 10TB, dostępne od frontu urządzenia, wyprodukowane w technologii SAS. Wymagana ilość dysków może zostać osiągnięta poprzez dedykowaną półkę dyskową.

Załącznik nr 2.5 do SWZ

Możliwość rozbudowy	Minimalna obsługa 144 dysków HDD przez pojedynczą macierz. Macierz powinna umożliwiać rozbudowę do klastra złożonego z minimum 6 par kontrolerów, każda para w identycznej konfiguracji z obsługą HA.
Obsługa dysków	Macierz musi być macierzą hybrydową i obsługiwać dyski HDD oraz SSD.
Sposób zabezpieczenia danych	Obsługa RAID 5,6 lub mechanizm równoważny do wymienionych, zabezpieczający przed utratą (awarią) dwóch dysków w tej samej grupie RAID.
Tryb pracy kontrolerów macierzowych	Dwa niezależne, redundantne kontrolery, każdy wyposażony w co najmniej: 2 porty SFP28 minimum 25Gb/s dedykowane do połączenia w parę HA, 3 porty 12Gb SAS oraz minimum 64 GB cache. Zawartość pamięci cache zapisu (write cache) każdego kontrolera musi być zabezpieczona za pomocą baterii i w przypadku awarii zasilania dane muszą pozostać w pamięci cache zapisu do momentu przywrócenia kontrolera do działania. Pamięć cache zapisu musi być zabezpieczona lustrzaną kopią w parze HA (high availablity). Kontrolery muszą współpracować w trybie active-active, równocześnie, obsługując protokoły dostępu, a jednocześnie każdy kontroler musi przejąć pracę partnera w razie awarii w sposób bezprzerwowy. Macierz musi posiadać 2 TB pamięci typu Flash opartej o NVMe (1 TB per kontroler), zamontowanej w kontrolerach, dedykowanej do akceleracji odczytów. Pamięć ta, ma przyspieszać dostęp do danych poprzez inteligentne buforowanie w czasie rzeczywistym najczęściej odczytywanych danych użytkownika i metadanych, z naciskiem na obciążenia losowe odczytowe (bazy danych, poczta, usługi plikowe). Buforowanie ma być realizowane sprzętowo i działać w sposób przezroczysty dla wolumenów (bez zmian w sposobie zapisu). Dane zapisywane nadal muszą trafiać na dyski mechaniczne. Użycie tej pamięci musi być przezroczyste dla użytkowników końcowych. Macierz musi umożliwiać przekształcenie istniejącej lokalnej puli dysków HDD pulę hybrydową poprzez dodanie SSD jako osobnych grup RAID, które będą pełnić rolę cache. Rozwiązanie musi pozwalać na określenie poziomu RAID dla SSD cache; domyślnie cache dziedziczy poziom RAID z HDD. Polityki muszą umożliwiać konfigurację zasad odczytów i zapisów (read/write). Musi być możliwość konfiguracji pracy SSD cache w trybie write cache. Użycie tej pamięci musi być przezroczyste dla użytkowników końcowych.
Obsługa protokołów	Macierz musi obsługiwać protokoły FC, iSCSI, SMB, NFS, S3. Obsługa wymienionych protokołów musi odbywać się w sposób natywny.
Interfejsy	Macierz musi posiadać co najmniej: • 4 porty SFP28, • 4 porty FC 32Gb dedykowane do hostów, • 6 portów SAS 12Gb. Co najmniej 2 porty w każdym kontrolerze muszą być wyposażone we wkładki 32Gb/s.

Załącznik nr 2.5 do SWZ

Zarządzanie	1. Zarządzanie urządzeniem przez interfejs WWW przez dedykowany port Ethernet. 2. Alarmy przez SNMP i E-mail. 3. Monitoring zużycia dysków SSD, diagnozowanie potencjalnych awarii. 4. Integracja z VMWare vCenter, VASA i SRM, Microsoft VDS, VSS.
Zarządzanie grupami dyskowymi oraz dyskami logicznymi	Macierz musi umożliwiać utworzenie co najmniej 1000 wolumenów w dostępie blokowym. Macierz musi posiadać funkcjonalność dynamicznej zmiany wielkości wolumenów logicznych oraz zmiany poziomu RAID bez konieczności przerwania komunikacji pomiędzy wolumenem i systemem operacyjnym korzystającym z wolumenu. System operacyjny kontrolerów macierzy musi oferować funkcjonalność QoS (Quality of Service) dla dowolnego wolumenu blokowego, to znaczy musi być możliwość ograniczenia liczby operacji IO na sekundę lub przepustowości w kB (lub analogicznych jednostkach) na sekundę, jaka jest możliwa do uzyskania ze wskazanego wolumenu.
Wewnętrzne kopie migawkowe	Funkcjonalność tworzenia snapshotów i klonów, minimum 1000 per wolumen. System kopii migawkowych musi działać w trybie Redirect On Write dla danych blokowych i plikowych.
Zdalna replikacja danych	Funkcjonalność replikacji danych z takim samym urządzeniem w trybie synchronicznym i asynchronicznym.
Redundancja	Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap", a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.
Deduplikacja i kompresja	Macierz musi posiadać funkcjonalność deduplikacji oraz kompresji inline. Procesy nie mogą być wykonywane przez dedykowane układy wbudowane w dyski, ani zewnętrzne oprogramowanie.
Ochrona	Wbudowana w system operacyjny funkcjonalność ochrony przed działaniem typu ransomware dla trybu plikowego, realizowana poprzez analizę zachowań systemu plików, automatyczne tworzenie kopii migawek w przypadku wykrycia podejrzanej aktywności oraz zabezpieczenie danych przed modyfikacją i usunięciem za pomocą kopii migawkowych. Usunięcie kopii migawkowej musi być potwierdzone przez minimum dwóch administratorów za pomocą wbudowanego mechanizmu autentykacji wielopoziomowej. Rozwiązanie musi umożliwiać przywracanie danych po incydencie za pomocą jednej komendy oraz integrację z systemami bezpieczeństwa bez konieczności stosowania dodatkowego oprogramowania.
Dodatkowe wymagania	1. Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez

Załącznik nr 2.5 do SWZ

	dostarczenie wielu macierzy dyskowych. 2. Wymaga się dostarczenia jednej dedykowanej aplikacji w postaci konsoli zarządzającej producenta macierzy dyskowej i serwerów do wykrywania tych urządzeń w sieci, podglądu statusu i monitorowania elementów sprzętowych wchodzących w skład postępowania zakupowego. Każdy element postępowania, tzn. macierze i serwer muszą posiadać licencję na dedykowaną wtyczkę do obsługi w konsoli zarządzającej. Kompatybilność oferowanych urządzeń musi być potwierdzona linkiem do strony producenta urządzeń, na której będą wymienione modele oferowanych produktów.
Gwarancja	Min. 36 miesięcy gwarancji producenta macierzy z czasem reakcji w następnym dniu roboczym (NBD) w trybie na miejscu u Zamawiającego (on-site). Komunikacja ze wsparciem technicznym w godzinach 9:00-16:00 powinna odbywać się w języku polskim. Naprawa urządzeń musi być realizowana przez producenta macierzy lub autoryzowanego partnera serwisowego. Uszkodzone dyski twarde pozostają u Zamawiającego. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników. Funkcja automatycznego zgłaszania usterek i awarii sprzętowych w helpdesk/servicedesk producenta sprzętu. Macierz musi być wyprodukowana zgodnie z normą ISO-9001, ISO-14001 oraz ISO-50001 lub równoważnymi. Producent macierzy powinien posiadać oficjalne przedstawicielstwo w Polsce. Wszystkie dostarczone elementy w ramach postępowania muszą pochodzić z polskiego, autoryzowanego kanału dystrybucji producenta. Macierz musi posiadać deklarację CE. Musi być zapewniona możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie na miejscu u Zamawiającego (on-site). Możliwość odpłatnego rozszerzenia gwarancji o gwarantowany czas naprawy w przeciągu 24 godzin.
Przełączniki FC – 2 szt.	
Wymagania funkcjonalne	1. Przełącznik FC musi być wykonany w technologii FC minimum 64 Gb/s i zapewniać możliwość pracy portów FC z prędkościami 64, 32, 16, 10, 8 Gb/s w zależności od rodzaju zastosowanych wkładek SFP. 2. Dostarczony przełącznik FC musi być wyposażony, w co najmniej 24 aktywne porty FC obsadzone wkładkami SFP+ typu shortwave obsługujących prędkość 32/16/8 Gb/s. 3. Wszystkie zaoferowane porty przełącznika FC muszą umożliwiać działanie bez tzw. oversubskrypcji (ang. oversubscritpion), gdzie wszystkie porty w maksymalnie rozbudowanej konfiguracji przełącznika

	mogą pracować równocześnie z pełną prędkością 64Gb/s. 4. Całkowita przepustowość przełącznika FC w konfiguracji z 24 aktywnymi portami wyposażonej we wkładki 64Gb/s musi wynosić minimum 1536 Gb/s end-to-end. 5. Oczekiwana wartość opóźnienia przy przesyłaniu ramek FC między dowolnymi portami przełącznika nie może być większa niż 460ns dla portów pracujących z prędkością 64Gbps. 6. Rodzaj obsługiwanych portów, co najmniej: E, EX, D, F oraz N. 7. Przełącznik FC musi umożliwiać obsługę agregacji do 8 fizycznych połączeń ISL, między dwoma przełącznikami i tworzenia w ten sposób logicznych połączeń typu ISL Trunk (magistrala) o przepustowości minimum 512 Gb/s half duplex (dla wkładek 64Gbps) dla każdego logicznego połączenia. Load balancing ruchu między fizycznymi połączeniami ISL w ramach połączenia logicznego typu ISL. Trunk musi być realizowany na poziomie pojedynczych ramek FC, a połączenie logiczne musi zachowywać kolejność przesyłanych ramek. 8. Przełącznik FC musi być wyposażony w mechanizm balansowania ruchu, pomiędzy co najmniej 16 różnymi połączeniami o tym samym koszcie wewnątrz wielodomenowych sieci fabric, przy czym balansowanie ruchu musi odbywać się w oparciu o 3 parametry nagłówka ramki FC: DID, SID I OXID. 9. Przełącznik FC musi być wyposażony w mechanizm jednoczesnej obsługi ISL. Trunk oraz balansowania ruchu w oparciu o DID/SID/OXID. 10. Przełącznik FC musi być dostarczony z aktywnym mechanizmem routingu FC (FCR) zapewniającym możliwość komunikacji wybranych urządzeń z różnych izolowanych sieci fabric. 11. Przełącznik FC musi obsługiwać sprzętową kompresję ramek FC dla wybranych połączeń ISL na co najmniej 4 portach przełącznika. 12. Przełącznik FC musi być dostarczony z aktywną możliwością przydzielenia, co najmniej 1400 tzw. buffer credits do wybranego portu FC przełącznika. 13. W przełączniku FC musi istnieć możliwość wydzielenia logicznych, izolowanych od siebie przełączników. Każdy z logicznych przełączników musi mieć własny Domain ID, własne usługi fabric (tzw. fabric services), niezależną bazę zoningu oraz możliwość przypisanie własnego administratora. 14. Musi istnieć możliwość połączenia wybranych logicznych przełączników wydzielonych w różnych fizycznych przełącznikach FC za pomocą przeznaczonych do tego celu połączeń ISL. Połączone w ten sposób przełączniki muszą tworzyć pojedynczą sieć fabric. 15. Przełącznik FC musi realizować kategoryzację ruchu między parami urządzeń (initiator - target) oraz przydzielenie takich par urządzeń do kategorii o wysokim, średnim lub niskim priorytecie. Konfiguracja przydziału do różnych klas priorytetów musi się odbywać za pomocą

	standardowych narzędzi do konfiguracji zoningu. 16. Przełącznik FC musi być wyposażony w mechanizm automatycznej kategoryzacji przepływów danych na podstawie prędkości pracy portu docelowego z przydziałem przepływów o prędkościach 16/8/4Gbps, 32Gbps i 64Gbps do różnych grup. Przepływy danych przydzielone do różnych grup nie mogą wpływać wzajemnie na swoją gospodarkę tzw, buffer credits. wartości parametru. 17. Przełącznik FC musi realizować kategoryzację ruchu na podstawie CS CTL w nagłówku ramki FC oraz odpowiednie przydzielenie ramki do kategorii wysokim, średnim lub niskim priorytecie. 18. Wsparcie dla N_Port ID Virtualization (NPIV). Obsługa, co najmniej 255 wirtualnych. urządzeń na pojedynczym porcie przełącznika. 19. Przełącznik FC musi realizować sprzętową obsługę zoningu (przez tzw. układ ASIC) na podstawie portów i adresów WWN. 20. Przełącznik FC musi wspierać następujące mechanizmy zwiększające poziom bezpieczeństwa: a) mechanizm szyfrowania i kompresji wybranych połączeń ISL wspierany, na co najmniej 4 portach przełącznika FC. Symetryczny klucz szyfrujący nie może być krótszy niż 256-bitów, b) mechanizm tzw. Fabric Binding, który umożliwia zdefiniowanie listy kontroli dostępu regulującej prawa przełączników FC do uczestnictwa w sieci fabric, c) uwierzytelnianie (ang. authentication) przełączników w sieci Fabric za pomocą protokołów DH-CHAP I FCAP, d) uwierzytelnianie (ang. authentication) urządzeń końcowych w sieci Fabric za pomocą protokołu DH-CHAP, e) szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2, f) definiowanie wielu kont administratorów z możliwością ograniczenia ich uprawnień za pomocą mechanizmu tzw. RBAC (Role Based Access Control), g) definiowane kont administratorów w środowisku RADIUS, LDAP w MS Active Directory, Open LDAP, TACACS+, h) szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS, i) obsługa SNMP v1 oraz v3, j) IP Filter dla portu administracyjnego przełącznika, k) wgrywanie nowych wersji firmware przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP, l) wykonywanie kopii bezpieczeństwa konfiguracji przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP. 21. Przełącznik FC musi mieć możliwość konfiguracji przez: a) polecenia tekstowe w interfejsie znakowym konsoli terminala, b) przeglądarkę internetową z interfejsem graficznym lub przeznaczone

	do tego oprogramowanie. 22. Przełącznik FC być wyposażony w następujące narzędzia diagnostyczne i mechanizmy obsługi ruchu FC: a) logowanie zdarzeń poprzez mechanizm „syslog", b) ciągle monitorowanie parametrów pracy przełącznika, portów, wkładek SFP i sieci fabric z automatycznym powiadamianiem administratora, wyłączeniem pracy portu lub przesunięciem przepływów tzw. slow drain na niski priorytet w przypadku przekroczenia zdefiniowanych wartości granicznych, powiadamianie administratora musi być możliwe za pomocą wysyłania wiadomości e-mail, pułapki SNMP lub komunikatu w logu, c) port diagnostyczny tzw. D port, port diagnostyczny musi umożliwiać wykonanie testów sprawdzających komunikację portu przełącznika z wkładką SFP, połączenie optyczne pomiędzy dwoma przełącznikami, testowe obciążenie połączenia pełną przepustowością 16/32/64Gbps oraz pomiar opóźnienia i odległości między przełącznikami z dokładnością co najmniej do 5m dla wkładek SFP 16/32/64Gbps, testy wykonywane przez port diagnostyczny nie mogą wpływać w żaden sposób na działanie pozostałych portów przełącznika i całej sieci fabric, d) FCping, e) FC traceroute, f) kopiowanie wybranych przepływów danych na wskazany lokalny port przełącznika, g) przełącznik musi być wyposażony w mechanizm sprzętowego generatora ruchu umożliwiającego symulowanie komunikacji w wielodomenowych sieciach SAN bez konieczności angażowania fizycznych urządzeń takich jak serwery lub macierze dyskowe, h) przełącznik musi być wyposażony w mechanizm umożliwiający kopiowanie pierwszych 64 bajtów ramek dla wybranych przepływów danych do pamięci lokalnej przełącznika w celu dalszej analizy, i) przełącznik musi obsługiwać wysyłanie komunikatów FPIN typu: Link Integrity Notification, Delivery Notification, Peer Congestion Notification, Congestion Notification, j) przełącznik musi obsługiwać wysyłanie sprzętowych sygnałów typu End Device Congestion za pomocą mechanizmu prymitywów FC typu ARB. 23. Przełącznik FC musi mieć możliwość wymiany i aktywacji wersji firmware'u (zarówno na wersję wyższą jak i na niższą) w czasie pracy urządzenia i bez zakłócenia przesyłanego ruchu FC. 24. Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet RJ45 oraz konsolowy mini-USB. 25. Przełącznik FC musi zapewniać obsługę protokołu NVMe over FC. 26. Przełącznik FC musi zapewniać obsługę interfejsu zarządzającego REST

Załącznik nr 2.5 do SWZ

	API. 27. Przełącznik FC musi mieć wysokość maksymalnie 1U (jednostka wysokości szafy montażowej) i szerokość 19" oraz zapewniać techniczną możliwość montażu w standardowej szafie dystrybucyjnej 19". 28. Maksymalny dopuszczalny pobór mocy przełącznika FC wyposażonego w 24 aktywne porty obsadzone optyką 64Gbps SWL nie może przekraczać 105W. 29. Przełącznik FC musi posiadać nadmiarowe zasilacze i wentylatory, których wymiana musi być możliwa w trybie „na gorąco" bez przerywania pracy przełącznika. 30. Przełącznik FC musi wydmuchiwać gorące powietrze od strony zasilania (od przodu do tyłu).
Gwarancja	Min. 36 miesięcy gwarancji producenta urządzenia z czasem reakcji w następnym dniu roboczym (NBD) w trybie na miejscu u Zamawiającego (on-site). Komunikacja ze wsparciem technicznym w godzinach 9:00-16:00 powinna odbywać się w języku polskim. Naprawa urządzeń musi być realizowana przez producenta urządzenia lub autoryzowanego partnera serwisowego. Funkcja automatycznego zgłaszania usterek i awarii sprzętowych w helpdesk/servicedesk producenta sprzętu. Urządzenie musi być wyprodukowane zgodnie z normą ISO-9001, ISO-14001 oraz ISO-50001 lub równoważnymi. Urządzenie musi posiadać deklarację CE.
System kopii zapasowych– 1 szt.	
Wymagania ogólne	1. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019, 2022 i 2025. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej, 2. Oprogramowanie musi współpracować z infrastrukturą Nutanix w wersji 6.5.x - 7.0, Red Hat Virtualization 4.4 SP1, Oracle Linux Virtualization 4.5.4 lub nowszy oraz Proxmox VE 8.2 lub nowszy, 3. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure, Microsoft Azure Data Lake, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux. 4. Wsparcie serwisowe przez okres36 miesięcy dla 45 maszyn wirtualnych.
Całkowite koszty posiadania	1. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej, 2. Oprogramowanie musi tworzyć “samowystarczalne” archiwa do

	odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków, 3. Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji, 4. Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu, 5. Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla conajmniej trzech pamięci masowych to takiej puli, 6. Oprogramowanie musi pozwalać na przechowywanie kopii bezpieczeństwa w chmurze producenta, 7. Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier, 8. Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu, 9. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania, 10. Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time), 11. Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu, 12. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API, 13. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji, 14. Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji, 15. Oprogramowanie musi posiadać mechanizmy chroniące przed utratą

Załącznik nr 2.5 do SWZ

	hasła szyfrowania, 16. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych, 17. Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej, 18. Oprogramowanie musi wymagać autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np skasowanie backupu, dodanie kolejnego administratora), 19. Oprogramowanie musi posiadać integracje z systemami zarządzania kluczami szyfrującymi (KMS), 20. Oprogramowanie musi posiadać integracje z systemami typu SIEM, 21. Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji.
Wymagania RPO	1. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej, 2. Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych, 3. Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna conajmniej dla platformy VMware i Hyper-V, 4. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku Vmware, 5. Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją Vmware, 6. Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO), 7. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son), 8. Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard, 9. Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS,

	10. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN, 11. Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji, 12. Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO, 13. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik, 14. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding), 15. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN).
Wymagania RTO	1. Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych, 2. Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna), 3. Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami, 4. Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre, 5. Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne, 6. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej

	maszyny, plików konfiguracji i dysków, 7. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform, 8. Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików, 9. Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V, 10. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell, 11. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM, 12. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej, 13. Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł, 14. Oprogramowanie musi pozwalać na backup i odtwarzanie usługi Entra ID. W szczególności użytkowników, grupy, role, jednostki administracyjne, entrprise applications oraz logi audytowe i sign-in, 15. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego, 16. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur, 17. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji, 18. Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux,

	19. Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux, 20. Oprogramowanie musi wspierać granularne odtwarzanie baz danych MongoDB. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux, 21. Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji, 22. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN, 23. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle, 24. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI, 25. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2, 26. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN.
Ograniczenie ryzyka	1. Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna), 2. Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych, 3. Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem, 4. Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32, 5. Oprogramowanie musi posiadać swój wbudowany program antywirusowy zoptymalizowany do przeszukiwania kopii backpowych, 6. Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware, 7. Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania, 8. Oprogramowanie, bazując na wyuczonym modelu maszynowym

	(machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków, 9. Oprogramowanie musi posiadać mechanizm wykrywania oznak ataku hakerskiego tzw Indicators of Compromise, 10. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego, 11. Oprogramowanie musi mieć możliwość integracji z innymi systemami bezpieczeństwa - minimum Splunk, Palo Alto Networks XSOAR.
Środowiska fizyczne	1. Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego, 2. Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych, 3. Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE, Rocky Linux, AlmaLinux, 4. Rozwiązanie musi wspierać system operacyjny macOS, 5. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix, 6. Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą), 7. Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster, 8. Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów, 9. Rozwiązanie musi wspierać backup podłączonych dysków USB, 10. Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym, 11. Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury), 12. Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone, 13. Rozwiązanie musi wspierać kontrolę pasma sieciowego, 14. Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych, 15. Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN, 16. Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas

Załącznik nr 2.5 do SWZ

	wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft, 17. Rozwiązanie musi wspierać technologię BitLocker, 18. Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania, 19. Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych, 20. Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych, 21. Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle I PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu, 22. Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform, 23. Rozwiązanie musi wspierać szyfrowanie, 24. Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne, 25. Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego, 26. Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej, 27. Rozwiązanie musi wspierać tworzenie wielu zadań backupowych.
Monitoring	1. System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich, 2. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie, 3. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019, 2022 oraz 2025 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie, 4. System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter,

	5. System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn, 6. System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel, 7. System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk, 8. System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora, 9. System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów, 10. System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard), 11. System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna, 12. System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego, 13. System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta, 14. System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych, 15. System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu, 16. System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy Vmware.
Raportowanie	1. System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie, 2. System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019, 2022 oraz 2025 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie, 3. System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów, 4. System musi być systemem bezagentowym. Nie dopuszcza się możliwości

	instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V, 5. System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF, 6. System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc, 7. System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach, 8. System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów, 9. System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych, 10. System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych, 11. System musi mieć możliwość analizowania „przeszacowanych" wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury, 12. System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta, 13. System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych, 14. System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach 'what-if', 15. System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy Vmware, 16. System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots), 17. System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie.
Serwer backup – 1 szt.	
Obudowa	Do instalacji w szafie Rack 19", wysokość nie więcej niż 1U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych. Możliwość instalacji ramienia do zarządzania kablami. Możliwość instalacji do min. 8 dysków SAS/SATA.
Procesor	Architektura x86, maksymalny TDP dla procesora – maksymalnie 150W.

Załącznik nr 2.5 do SWZ

	Wymagana ilość rdzeni dla procesora – min. 12. Minimalna częstotliwość pracy procesora 2.2GHz. Minimalna ilość kanałów procesora – 8. Wynik wydajności procesora nie powinien być niższy niż 285 punkty base w teście SPECrate 2017 Integer w konfiguracji dwuprocesorowej, opublikowanym przez SPEC.org (www.spec.org), dla serwera oferowanego producenta. Wynik musi dotyczyć konfiguracji odpowiadającej oferowanemu modelowi serwera i procesora (w szczególności: liczba procesorów, rdzeni oraz taktowanie) i pochodzić z oficjalnie opublikowanych rezultatów SPEC. **Wykonawca zobowiązany jest do wskazania w ofercie linku do oficjalnego raportu SPEC potwierdzającego spełnienie powyższego wymagania**. Liczba zainstalowanych procesorów: 2.
Płyta główna	Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów wykonujących 64-bitowe instrukcje.
Pamięć operacyjna	Zainstalowane minimum 256GB pamięci RAM o częstotliwości 6400MHz. Pamięć zainstalowana w ilości zapewniającej największą przepustowość oraz wydajność. Minimum 32 sloty na pamięć. Możliwość rozbudowy do 8TB RAM.
Zabezpieczenie pamięci	Memory mirroring, ECC, SDDC, ADDDC.
Karta Graficzna	Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz.
Dyski	W chwili dostawy serwer musi posiadać zainstalowane minimum 2 sztuki dysków M.2 o pojemności przynajmniej 480 GB sterowanych dedykowanym kontrolerem sprzętowym umożliwiającym redundancję RAID 1 z możliwością wymiany „na gorąco". Dodatkowo zainstalowane 3 sztuki dysków SSD SATA o pojemności 960GB typu hot-swap, podłączone do dedykowanego kontrolera dysków Wymagany jest wewnętrzny slot na kartę Micro SD.
Kontroler dysków	Umożliwia obsługę co najmniej 8 dysków SAS/SATA w trybach RAID 0, 1, 5, 6, 10, 50, 60. Powinien posiadać min. 4GB pamięci cache, zapewniać obsługę dysków HDD oraz SSD. Kontroler powinien wspierać pracę w trybie JBOD oraz obsługiwać dyski samoszyfrujące.
Zasilacz	Minimum dwa redundantne zasilacze o mocy minimum 1300W z certyfikatem minimum Titanium. Moc pojedynczego zasilacza musi być wystarczająca do zasilenia serwera w oferowanej konfiguracji.
Interfejsy sieciowe	Zainstalowana jedna dwuportowa karta 10Gb/25Gb wyposażona w dedykowane wkładki 10/25Gb. Karta nie może zajmować żadnego ze slotów PCIe wymienionych w punkcie Sloty I/O. Zainstalowana jedna dwuportowa karta FC 32Gb wyposażona w dedykowane wkładki 32Gb. Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty

	zarządzającej.
Dodatkowe sloty I/O	Serwer w momencie dostawy powinien posiadać 2 sloty PCIe Gen5 x16 z czego jeden slot pełnej wysokości, 2 sloty OCP Gen5 oraz dedykowane połączenie PCIe dla kontrolera dyskowego niezajmujące slotów PCIe.
Dodatkowe porty	2x USB 3, 1x VGA, 1x RJ-45 do zarządzania serwerem. Możliwość instalacji portu DB9. Wszystkie tylne porty USB, port RJ-45 służący do zarządzania, tylny port VGA, wewnętrzny port na kartę Micro SD, będą umieszczone na osobnej dedykowanej płytce I/O, którą łączy się bezpośrednio z płytą główną serwera
Chłodzenie	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1.
Zarządzanie	Wymagany wbudowany sprzętowy kontroler zdalnego zarządzania, który musi być umieszczony na osobnej dedykowanej płytce I/O (wspomnianej w sekcji Dodatkowe Porty). 1. Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna. 2. Pozyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres IP karty zarządzającej, utylizacja CPU, utylizacja pamięci oraz komponentów I/O, lokalizacja. 3. Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów. 4. Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń. 5. Wysyłanie określonych zdarzeń poprzez SMTP oraz SNMPv3. 6. Update systemowego firmware. 7. Możliwość aktualizacji wielu komponentów z wykorzystaniem jednego pakietu (bundle) aktualizacyjnego, bezpośrednio ze strony producenta. 8. Monitoring i możliwość ograniczenia poboru prądu. 9. Zdalne włączanie/wyłączanie/restart. 10. Zapis video zdalnych sesji. 11. Podmontowanie lokalnych mediów z wykorzystaniem Java client. 12. Przekierowanie konsoli szeregowej przez IPMI. 13. Zrzut ekranu w momencie zawieszenia systemu. 14. Możliwość przejęcia zdalnego ekranu. 15. Możliwość zdalnej instalacji systemu operacyjnego. 16. Alerty Syslog. 17. Przekierowanie konsoli szeregowej przez SSH. 18. Wyświetlanie danych aktualnych i historycznych dla użycia energii oraz temperatury serwera.

	19. Możliwość mapowania obrazów ISO z lokalnego dysku operatora. 20. Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS, Samba oraz NFS. 21. Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę. 22. wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API. 23. Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego. 24. Kontroler zarządzania musi posiadać 4GB wewnętrznej pamięci (dopuszcza się zastosowanie karty Micro SD w celu uzyskania tej pojemności). Pamięć kontrolera zarządzania musi pełnić funkcję RDOC (Remote Disc on Card) oraz musi umożliwiać przechowywanie plików firmware. 25. Monitorowanie zmian sprzętowych w celu wykrycia nieoczekiwanych zmian. Po wykryciu zmiany zapis w logu serwera lub uniemożliwienie boot'u. 26. Możliwość synchronizacji konfiguracji i poziomów firmware pomiędzy serwerami. 27. Możliwość monitorowania i zarządzania grupą serwerów z poziomu kontrolera zarządzania pojedynczego serwera. Ilość serwerów możliwych do zarządzania – minimum 200. 28. Możliwość instalacji dodatkowego oprogramowania do zarządzania, posiadającego następujące funkcjonalności: a) zarządzanie infrastruktura serwerów i storage bez udziału dedykowanego agenta, b) przedstawianie graficznej reprezentacji zarządzanych urządzeń, c) możliwość skalowania do minimum 1000 urządzeń, d) obsługę szyfrowanej komunikacji z zarządzanymi urządzeniami, wsparcie dla NIST 800-131A oraz FIPS 140-2, e) wsparcie dla certyfikatów SSL tzw. self-signed oraz zewnętrznych, f) udostępnianie szybkiego podgląd stanu środowiska, g) udostępnianie podsumowania stanu dla każdego urządzenia, h) tworzenie alertów przy zmianie stanu urządzenia, i) monitorowanie oraz tracking zużycia energii przez monitorowane urządzenie, możliwość ustalania granicy zużycia energii, j) konsola zarządzania oparta o HTML 5, k) dostępność konsoli monitorującej na urządzeniach przenośnych ze wsparciem dla systemu Android oraz iOS, aplikacja musi umożliwiać włączenie wyłączenie oraz restart urządzenia, musi również mieć

	możliwość aktywowania diody lokacyjnej na urządzeniu, l) automatyczne wykrywanie dołączanych systemów oraz szczegółowa inwentaryzacja, m) możliwość podnoszenia wersji oprogramowania dla komponentów zarządzanych serwerów w oparciu o repozytorium lokalne jak i zdalne dostępne na stronie producenta oferowanego rozwiązania, n) definiowanie polityk zgodności wersji firmware komponentów zarządzanych urządzeń, o) definiowanie roli użytkowników oprogramowania, p) obsługa REST API oraz Windows PowerShell, q) obsługa SNMP, SYSLOG, Email Forwarding, r) autentykacja użytkowników: centralna (możliwość definiowania wymaganego poziomu skomplikowania danych autentykacyjnych) oraz integracja z MS AD oraz obsługa single sign on oraz SAML, s) obsługa tzw. Forward Secrecy w komunikacji z zarządzanymi urządzeniami, t) przedstawianie historycznych aktywności użytkowników, u) blokowanie możliwości podłączenia innego systemu zarzadzania do urządzeń zarządzanych, v) tworzenie dziennika zdarzeń ukończonych sukcesem lub bledem, oraz zdarzeń będących w trakcie. Możliwość definiowania filtrów wyświetlanych zdarzeń z dziennika. Możliwość eksportu dziennika zdarzeń do pliku csv, w) Obsługa NTP, x) przesyłanie alertów do konsoli firm trzecich, y) tworzenie wzorców konfiguracji zarządzanych urządzeń (definiowanie przez konsole albo kopiowanie konfiguracji z już zaimplementowanych urządzeń), z) instalowanie systemów operacyjnych oraz wirtualizatorów Vmware i Hyper-V. Wymagana jest integracja konsoli zarządzania z konsolą wirtualizatora tak, aby zarządzanie środowiskiem sprzętowym mogło odbywać się z konsoli wirtualizatora. Wymaga się możliwości instalacji systemu na przynajmniej 20 nodach jednocześnie, aa) możliwość automatycznego tworzenia zgłoszeń w centrum serwisowym producenta dla określonych zdarzeń wraz z przesyłem plików diagnostycznych, Producent serwera ponadto powinien mieć w swojej ofercie narzędzia integrujące zarządzanie infrastrukturą z następującymi produktami: VMware vCenter, Microsoft AdminCenter, Microsoft SystemCenter, RedHat CloudForms, Splunk.
Funkcje zabezpieczeń	Możliwość instalacji czujnika otwarcia obudowy zintegrowanego z modułem zarządzania serwerem, hasło włączania, hasło administratora, moduł RoT (umieszczony na dedykowanej płytce I/O wspomnianej w sekcji Dodatkowe porty) wspierający TPM2.0 oraz Platform Firmware Resiliency (PFR).,

	Możliwość instalacji przedniego panelu zamykanego na klucz. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. Możliwość włączania i wyłączania portów USB na obudowie z poziomu karty zarządzania. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z systemu zarządzania serwerem. Wbudowany w BIOS mechanizm umożliwiający usunięcie konfiguracji kart zarządzających, BIOS oraz danych ze wszystkich wewnętrznych urządzeń pamięci masowej. Możliwość automatycznego przywrócenia BIOS do wspieranej wersji w przypadku wykrycia nieautoryzowanej modyfikacji. Urządzenie musi posiadać mechanizm ochrony integralności platformy, umożliwiający monitorowanie i weryfikację kluczowych elementów sprzętowych w celu wykrywania prób nieautoryzowanych modyfikacji. Rozwiązanie powinno działać niezależnie od systemu operacyjnego i umożliwiać raportowanie stanu integralności platformy do systemów zarządzania producenta
Urządzenia hot swap	Dyski twarde, zasilacze, wentylatory.
Obsługa	Możliwość instalacji serwera oraz serwisowania (instalacji oraz deinstalacji) komponentów takich jak: riser'ów PCIe, backplane'ów dysków twardych, kart rozszerzeń, wentylatorów, bez użycia dodatkowych narzędzi mechanicznych.
Diagnostyka	Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID.
Wspierane systemy operacyjne	Microsoft Windows Server 2022, 2025; Red Hat Enterprise Linux 9.x, 10,x; SUSE Linux Enterprise Server 15 SP6, SP7; VMware vSphere (ESXi) 8.0 U3, 9.0; Ubuntu 22.04, 24.04, Oracle Linux 9.6, XenServer 8.
Waga	maksimum: 21 kg
Dodatkowe wymagania	Wymaga się dostarczenia jednej dedykowanej aplikacji w postaci konsoli zarządzającej producenta macierzy dyskowej i serwerów do wykrywania tych urządzeń w sieci, podglądu statusu i monitorowania elementów sprzętowych wchodzących w skład postępowania zakupowego. Każdy element postępowania, tzn. macierze i serwer muszą posiadać licencję na dedykowaną wtyczkę do obsługi w konsoli zarządzającej. Kompatybilność oferowanych urządzeń musi być potwierdzona linkiem do strony producenta urządzeń, na której będą wymienione modele oferowanych produktów.
Gwarancja	Min. 36 miesięcy gwarancji producenta serwera z czasem reakcji w następnym dniu roboczym (NBD) w trybie na miejscu u Zamawiającego (on-site). Komunikacja ze wsparciem technicznym w godzinach 9:00-16:00 powinna odbywać się w języku polskim. Naprawa urządzeń musi być realizowana przez producenta serweralub autoryzowanego partnera serwisowego. Uszkodzone dyski twarde pozostają u Zamawiającego. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz

	sterowników. Funkcja automatycznego zgłaszania usterek i awarii sprzętowych w helpdesk/servicedesk producenta sprzętu. Serwer musi być wyprodukowany zgodnie z normą ISO-9001, ISO-14001 oraz ISO-50001 lub równoważnymi. Producent serwera powinien posiadać oficjalne przedstawicielstwo w Polsce. Wszystkie dostarczone elementy w ramach postępowania muszą pochodzić z polskiego, autoryzowanego kanału dystrybucji producenta. Serwer musi posiadać deklarację CE. Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie na miejscu u Zamawiającego (on-site). Możliwość odpłatnego rozszerzenia gwarancji o gwarantowany czas naprawy w przeciągu 24 godzin.
Oprogramowanie systemowe	Wymagania minimalne – system operacyjny serwera 1. Rodzaj i przeznaczenie o System operacyjny klasy serwerowej, przeznaczony do pracy ciągłej (24/7), dla architektury x86-64. o Przeznaczony do instalacji na serwerze fizycznym oraz do pracy jako system gościa w środowisku wirtualnym. 2. Wsparcie producenta i legalność o System musi być objęty wsparciem producenta w dniu dostawy oraz posiadać zapewnione aktualizacje bezpieczeństwa. o Dostarczony w modelu licencjonowania umożliwiającym legalne użytkowanie w środowisku Zamawiającego (licencja komercyjna, bez ograniczeń naruszających użycie produkcyjne). 3. Instalacja i tryby pracy o Możliwość instalacji w trybie z interfejsem graficznym oraz w trybie minimalnym (core/minimal footprint). o Obsługa instalacji na platformach z UEFI oraz mechanizmami bezpieczeństwa rozruchu (np. Secure Boot). 4. Zarządzanie i administracja o Wbudowane narzędzia do zdalnego zarządzania i automatyzacji (konsola/CLI, zdalne zarządzanie usługami i rolami, obsługa skryptów administracyjnych). o Możliwość centralnego zarządzania politykami i konfiguracją stacji/serwerów w domenie (mechanizmy polityk i szablonów administracyjnych). o Obsługa rejestrowania zdarzeń systemowych oraz audytu bezpieczeństwa. 5. Role i usługi serwerowe o Możliwość uruchomienia co najmniej następujących funkcji/ ról (wbudowanych lub dostarczanych przez producenta systemu): ▪ usługi katalogowe/domenowe wraz z mechanizmami uwierzytelniania, ▪ usługi DNS i DHCP, ▪ usługi plików z kontrolą uprawnień (ACL) oraz

	udziałami sieciowymi, ▪ usługi drukowania (opcjonalnie – jeśli potrzebne), ▪ mechanizmy klastra wysokiej dostępności (failover clustering) – jeśli wymagane w projekcie. 6. Sieć i protokoły o Pełna obsługa IPv4/IPv6, VLAN, NIC teaming/bonding (lub równoważne), QoS. o Obsługa nowoczesnych wersji protokołów udostępniania plików (SMB) wraz z mechanizmami podpisywania i szyfrowania. 7. Bezpieczeństwo o Mechanizmy wzmacniania bezpieczeństwa: zapora systemowa, kontrola aplikacji, ochrona poświadczeń, szyfrowanie danych wolumenów (np. BitLocker lub równoważne). o Możliwość wymuszenia silnych protokołów kryptograficznych (TLS 1.2 lub nowszy) oraz zarządzania certyfikatami. 8. Magazyn danych o Obsługa nowoczesnych systemów plików i funkcji serwerowych (np. deduplikacja danych, migawki/Shadow Copies lub równoważne). o Obsługa iSCSI (inicjator/target – zgodnie z potrzebą) oraz MPIO (lub równoważne). 9. Wirtualizacja i kontenery (jeśli dotyczy) o Możliwość uruchomienia roli hypervisora oraz obsługa wirtualizacji sprzętowej (Intel VT-x/AMD-V). o Obsługa konteneryzacji na poziomie systemu operacyjnego (jeżeli wymagane). 10. Kompatybilność aplikacyjna • Zgodność z uruchamianiem usług i aplikacji Zamawiającego opartych o popularne środowiska uruchomieniowe (np. .NET / środowisko uruchomieniowe aplikacji serwerowych), w tym możliwość instalacji ról wymaganych przez te aplikacje. 11. Równoważność • Zamawiający dopuszcza systemy równoważne, pod warunkiem spełnienia wszystkich wymagań funkcjonalnych, bezpieczeństwa i zarządzania określonych powyżej oraz zapewnienia kompatybilności z istniejącą infrastrukturą Zamawiającego.
Zapora sieciowa– 1 szt.	
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 5 administratorów do poszczególnych instancji systemu. System wspiera protokoły IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	1. 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. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
Interfejsy, Dysk, Zasilanie	1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: a) 10 portami Gigabit Ethernet RJ-45. b) 8 gniazdami SFP 1 Gbps. c) 2 gniazdami SFP+ 10 Gbps. 2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB. 3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System jest wyposażony w zasilanie AC.
Parametry wydajnościowe	1. W zakresie Firewall'a obsługa nie mniej niż 1.4 mln jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 11 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 2.5 Gbps.

	6. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.
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. 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. 11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 12. Możliwość filtrowania zapytań DNS 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).
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: a) Translację jeden do jeden oraz jeden do wielu. b) 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: adresy 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.

Załącznik nr 2.5 do SWZ

	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. a) Amazon Web Services (AWS), b) Microsoft Azure, c) Cisco ACI, d) Google Cloud Platform (GCP), e) OpenStack, f) VMware NSX, g) Kubernetes.
Połączenia VPN	1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: a) Wsparcie dla IKE v1 oraz v2, b) Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM), c) Obsługa protokołu Diffie-Hellman grup 19, 20, d) Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, e) Tworzenie połączeń typu Site-to-Site oraz Client-to-Site, f) Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności, g) Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego, h) Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat, i) Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu, j) Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu, k) Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth, l) Mechanizm „Split tunneling" dla połączeń Client-to-Site, 2. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie zapewnia obsługę: 1. Routingu statycznego, 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego), 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM, 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego

	routingu, 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routing, 6. BFD (Bidirectional Forwarding Detection), 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
Funkcje SD-WAN	1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
Zarządzanie pasmem	1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System daje możliwość określania pasma dla poszczególnych aplikacji. 3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum. 4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 7. 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 usłudze chmurowej realizowanej na terenie Unii Europejskiej. 8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego

	przez laboratoria producenta. 10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
Ochrona przed atakami	1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. 8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. 9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
Kontrola aplikacji	1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. 6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 7. 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	1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.

	2. 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. 3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. 4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: a) Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu, b) Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP, c) Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego. 3. 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. 4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. 3. Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego. 4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły

	SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). 9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
Logowanie	1. 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. 2. 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. 3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 4. Możliwość włączenia logowania per reguła w polityce firewall. 5. System zapewnia możliwość logowania do serwera SYSLOG. 6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
Testy wydajnościowe oraz funkcjonalne	Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni.
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 przez cały okres gwarancji.
Gwarancja	System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia

	zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres min. 36 miesięcy. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 lub równoważny w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe muszą być przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Urządzenia muszą posiadać deklarację CE.
Ochrona poczty e-mail– 1 komplet	
Wymagania ogólne	System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware'ową bez limitu licencyjnego na ilość chronionych kont użytkowników. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń. Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów: • Tryb Gateway, • Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).
Parametry fizyczne systemu antyspamowego	1. System musi być wyposażony w interfejsy: • 4 porty Gigabit Ethernet RJ-45. 2. System musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 2 TB z możliwością obsługi mechanizmu RAID 1 lub 5 lub 10. 3. System musi posiadać wbudowany port konsoli szeregowej. 4. Zasilanie z sieci 230V/50Hz.
Ogólne funkcje systemu ochrony poczty	Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje: 1. Wsparcie dla co najmniej 70 domen pocztowych. 2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 150 tys. wiadomości/godzinę. 3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all). 4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.

	5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości). 6. Możliwość ograniczenia ilości poczty wychodzącej do chronionych domen w oparciu o nie mniej niż: ilość jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie. 7. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej. 8. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów. 9. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP. 10. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika. 11. Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora. 12. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail. 13. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki. 14. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI. 15. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu. 16. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników. 17. Ochrona przed wyciekiem informacji poufnej DLP (Data Leak Preention). 18. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.
Kontrola antywirusowa i ochrona przed malware	W tym zakresie dostarczony system ochrony poczty musi zapewniać: 1. Skanowanie antywirusowe wiadomości SMTP. 2. Kwarantannę dla zainfekowanych plików. 3. Skanowanie załączników skompresowanych. 4. Definiowanie komunikatów powiadomień w języku polskim. 5. Blokowanie załączników w oparciu o typ pliku. 6. Możliwość zdefiniowania nie mniej niż 200 polityk kontroli antywirusowej. 7. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.

	8. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora. 9. Ochronę typu wirus outbrake.
Kontrola antyspamowa	System musi zapewniać poniższe funkcje i metody filtrowania spamu: 1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta. 2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania. 3. Szczegółowa kontrola nagłówka wiadomości. 4. Analiza Heurystyczna. 5. Współpraca z zewnętrznymi serwerami RBL, SURBL. 6. Filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen. 7. Możliwością dostrajania filtrów Bayes'a przez poszczególnych użytkowników. 8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF. 9. Kontrola w oparciu o Greylisting oraz SPF. 10. Filtrowanie treści wiadomości i załączników. 11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości. 12. Możliwość zdefiniowania nie mniej niż 200 polityk kontroli antyspamowej. 13. Ochrona typu outbrake. 14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: phishing, hacking). 15. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.
Ochrona przed atakami na usługę poczty	System musi zapewniać poniższe funkcje i metody filtrowania: 1. Ochrona przed atakami na adres odbiorcy (m.in. email bombing). 2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu. 3. Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu. 4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing). 5. Weryfikacja poprawności adresu e-mail nadawcy.
Funkcje logowania i raportowania	W tym zakresie dostarczony system ochrony poczty musi zapewniać: 1. Logowanie do zewnętrznego serwera SYSLOG.

Załącznik nr 2.5 do SWZ

	2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku. 3. Logowanie informacji na temat spamu oraz niedozwolonych załączników. 4. Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych. 5. Możliwość analizy przebiegu sesji SMTP. 6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych. 7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu. 8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.
Funkcje pracy w trybie wysokiej dostępności (HA)	System ochrony poczty musi zapewniać poniższe funkcje: 1. Konfigurację HA w każdym z trybów: gateway, transparent. 2. Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP. 3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu. 4. Monitorowanie stanu pracy klastra.
Aktualizacje sygnatur, dostęp do bazy spamu	W tym zakresie dostarczony system ochrony poczty musi zapewniać: 1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym. 2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.
Zarządzanie	System ochrony poczty musi zapewniać poniższe funkcje: 1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH. 2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy. 3. Powinna istnieć możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych.
Serwisy i licencje	W ramach postępowania muszą zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbrake przez cały okres gwarancji.
Gwarancja	System musi być objęty serwisem gwarancyjnym producenta przez okres min. 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas

Załącznik nr 2.5 do SWZ

	naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres min. 36 miesięcy. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 lub równoważny w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Urządzenie musi posiadać deklarację CE.
System uwierzytelniania, autoryzacji i kontroli dostępu	
Ogólne	1. Oferowane rozwiązanie musi pozwalać na centralne zarządzenie kontami użytkowników oraz procesem uwierzytelnienia – w tym celu musi zapewniać wszystkie wymienione poniżej funkcje. 2. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne, odpowiednio zabezpieczone systemy operacyjne dla poszczególnych komponentów. 3. System musi zapewniać nie mniej niż: a) Możliwość pracy w konfiguracji HA (High Availability) z trybem Active-Passive lub Active-Active w celu zwiększenia niezawodności. b) Graficzną reprezentację statusu uwierzytelnionych użytkowników. c) Logowanie wszystkich zdarzeń uwierzytelniania wraz z ich statusem, szczegółami dotyczącymi powodów niepowodzenia oraz nazwą użytkownika: • Lokalnie, • Zdalnie w oparciu o protokół Syslog, • Konfigurację Captive Portalu.
Parametry systemu	Poszczególne elementy wchodzące w skład systemu muszą zapewniać obsługę: a) 4 wirtualnych interfejsów sieciowych, b) Możliwość uruchomienia w środowiskach: Microsoft Hyper-V Server 2010, 2012 R2 oraz 2016; VMware ESXi, ESX wersje:4,5,6; KVM, Xen, Microsoft Azure, AWS, Oracle OCI.
Parametry wydajnościowe i licencyjne	System musi obsługiwać co najmniej: a) Uwierzytelnianie dla 100 użytkowników, b) 200 tokenów dla uwierzytelniania dwuskładnikowego, c) 30 klientów protokołu RADIUS (urządzeń NAS, które można podpiąć do systemu), d) Możliwość zdefiniowania co najmniej 10 grup użytkowników, e) 5 lokalnych centrów certyfikacji (CA), f) Możliwość wygenerowania 100 certyfikatów dla użytkowników.

Załącznik nr 2.5 do SWZ

Wymagania funkcjonalne – uwierzytelnianie	Celem realizacji funkcji uwierzytelniających, system musi zapewniać nie mniej niż: 1. Lokalną, wbudowaną bazę użytkowników. 2. Przechowywanie następujących informacji o użytkowniku: nazwa, imię i nazwisko, adres email, numer telefonu, adres, kraj, województwo. 3. Możliwość zdefiniowania co najmniej 3 indywidualnie konfigurowalnych pól dla każdego z użytkowników. 4. Możliwość importu informacji o użytkownikach z zewnętrznego serwera LDAP lub pliku CSV. 5. Konfigurowalną politykę haseł użytkowników w ramach której możliwym jest określenie: a) poziomu złożoności hasła (jego długości minimalnej, występowania małych i dużych liter, cyfr i znaków specjalnych), b) czasu ważności hasła, 6. Konfigurowalną politykę blokowania kont, która będzie uwzględniać: a) ilość nieudanych logowań, b) czas blokowania konta, c) okres nieaktywności, po którym konto jest blokowane. 7. Możliwość odzyskiwania haseł: a) z wykorzystaniem adresu email, b) z wykorzystaniem pytania pomocniczego. 8. Obsługę protokołu RADIUS zgodną z RFC, w tym zakresie system musi oferować: a) wbudowany serwer RADIUS, b) integrację z zewnętrznymi serwerami RADIUS – praca jako klient. 9. Obsługę protokołu LDAP, w tym zakresie system musi oferować: a) wbudowany serwer LDAP, b) możliwość zautomatyzowanej synchronizacji z zewnętrznym serwerem LDAP (zarówno kont użytkowników jak i atrybutów LDAP). 10. Obsługę protokołu SAML - Identity Provider (IdP) proxy. 11. Realizację funkcji SSO (Single Sign On) w oparciu o: a) integrację z Active Directory, również bez konieczności instalacji dodatkowego oprogramowania na kontrolerach domeny, b) dedykowaną aplikację instalowaną na stacjach roboczych z systemem Windows, c) kontekst użytkownika przesyłany z serwera RADIUS, d) informacje uzyskiwane poprzez protokół Syslog.
Wymagania funkcjonalne – uwierzytelnianie dwuskładnikowe	1. Obsługę dla tokenów sprzętowych (hardware): a) wspomniane tokeny muszą pochodzić od tego samego producenta co system uwierzytelniania. 2. Wsparcie dla tokenów programowych (software token) dla takich systemów operacyjnych jak iOS, Android, Windows Phone (8 i 8.1) oraz Windows 10 Mobile.

Załącznik nr 2.5 do SWZ

	3. Dla tokenów na system iOS i Android wymaga się: a) aktywacji z centralnego systemu uwierzytelniania (seed provisioning), b) możliwości konfiguracji ilości generowanych cyfr (6 lub 8), c) generowania kodu (cyfr) co 30 lub 60 sekund, d) możliwości dezaktywacji tokenu oraz jego reinstalacji (przeniesienia na inne urządzenie mobilne), e) ochrony dostępu poprzez konfigurowalny kod PIN.
Wymagania funkcjonalne – 802.1x	System powinien umożliwiać realizację uwierzytelniania z wykorzystaniem protokołu 802.1x, spełniając nie mniej niż następujące warunki: 1. Obsługa co najmniej poniższych protokołów EAP: a) PEAP, b) EAP-TTLS, c) EAP-TLS, d) EAP-GTC. 2. Wsparcie dla uwierzytelnienia w oparciu o adres MAC (MAC based authentication). 3. Zarządzanie certyfikatami (w oparciu o własne CA) celem wykorzystania w ramach PEAP, TTLS, TLS.
Wymagania funkcjonalne – zarządzanie certyfikatami	System powinien spełniać następujące wymagania w zakresie zarządzania certyfikatami, nie mniej niż: 1. Obsługa wbudowanego CA (Certificate Authority). 2. Obsługa CA pośredniczących (Intermediate CA). 3. Ręczne generowanie certyfikatów z wykorzystaniem interfejsu graficznego. 4. Możliwość pobrania wygenerowanych certyfikatów. 5. Możliwość podpisywania certyfikatów z wykorzystaniem protokołu SCEP. 6. Możliwość automatycznego i ręcznego generowania certyfikatów z wykorzystaniem protokołu SCEP. 7. Możliwość generowania certyfikatów typu wildcard. 8. Realizacja CRL (Certificate Revocation List). 9. Wsparcie dynamicznego odwoływania certyfikatów z wykorzystaniem protokołu OCSP (RFC2560). 10. Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych.
Zarządzanie	1. Zarządzanie w oparciu o protokół HTTPS (interfejs graficzny) z wykorzystaniem przeglądarki. 2. System udostępnia graficzny interfejs zarządzania poprzez szyfrowane połączenie HTTPS. 3. Tworzenie kopii bezpieczeństwa konfiguracji z poziomu graficznego interfejsu zarządzającego (GUI) oraz na zewnętrzny serwer FTP/SFTP w oparciu o harmonogram, który będzie umożliwiał wskazanie konkretnego czasu kiedy proces ma się rozpocząć. 4. Możliwość zdefiniowania co najmniej 4 lokalnych kont

	administracyjnych.
Serwis i usługi	Wymaga się aby dostawa obejmowała również serwis producenta przez okres 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.
Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów programowych	
Ogólne	1. W ramach postępowania powinny zostać dostarczone co najmniej 100 tokenów programowych współpracujących z posiadanym przez Zamawiającego urządzeniem FortiGate, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów oraz w ramach połączeń VPN typu client-to-site. 2. Wsparcie dla tokenów programowych (software token) dla takich systemów operacyjnych jak iOS, Android oraz Windows 10 Mobile. 3. Dla tokenów na system iOS i Android wymaga się: a) aktywacji z systemu firewall, b) generowania kodu (cyfr) co 30 lub 60 sekund, c) możliwości dezaktywacji tokenu oraz jego reinstalacji (przeniesienia na inne urządzenie mobilne), d) ochrony dostępu poprzez konfigurowalny kod PIN.
Usługi wdrożeniowe – 1 szt.	
Ogólne	Przedmiotem zamówienia jest dostawa, instalacja, konfiguracja oraz wdrożenie urządzeń i systemów infrastruktury informatycznej niezbędnych do zapewnienia ciągłości pracy systemów szpitalnych oraz podniesienia poziomu bezpieczeństwa teleinformatycznego, w tym: a) macierz blokowa – rozbudowa istniejącej infrastruktury – 1 szt., b) macierz obiektowa – 2 szt., c) przełączniki FC (Fibre Channel) – 2 szt., d) system kopii zapasowych – 1 szt., e) serwer backup – 1 szt., f) zapora sieciowa – 1 szt. (klaster HA), g) system ochrony poczty e-mail – 1 komplet.
Cel wdrożenia	Realizacja zamówienia ma na celu: 1. zwiększenie dostępności, niezawodności i bezpieczeństwa przechowywania danych szpitalnych, 2. zapewnienie zgodności z wymaganiami Krajowego Systemu Cyberbezpieczeństwa i KRI, 3. poprawę ciągłości działania systemów w przypadku awarii, 4. podniesienie poziomu cyberbezpieczeństwa zgodnie z zakresem przedsięwzięcia D1.1.2 „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia”.
Zakres usług wdrożeniowych	Usługa wdrożeniowa powinna obejmować co najmniej: 1. Przygotowanie środowiska wdrożeniowego: a) Analizę środowiska technicznego Zamawiającego,

Załącznik nr 2.5 do SWZ

	2. Dostawa i instalacja urządzeń: a) Montaż i podłączenie urządzeń w pomieszczeniach wskazanych przez Zamawiającego, b) Konfiguracja sieci SAN, LAN i VLAN z uwzględnieniem segmentacji sieci i redundancji połączeń, c) Implementacja redundancji w klastrze zapory sieciowej (HA). 3. Konfiguracja i uruchomienie systemów: a) Konfiguracja macierzy blokowej i obiektowej (LUN, RAID, multipathing), b) Konfiguracja przełączników FC, c) Konfiguracja systemu kopii zapasowych wraz z integracją z serwerem backupowym, d) Wdrożenie harmonogramów backupu, e) Testy przywracania danych (restore), f) Konfiguracja zapory sieciowej NGFW w trybie HA z politykami bezpieczeństwa, filtrowaniem treści, IPS/IDS i VPN, g) Wdrożenie ochrony poczty e-mail. 4. Testy i odbiory: a) Przeprowadzenie testów funkcjonalnych i bezpieczeństwa (w tym testów odtworzeniowych i testów konfiguracji), b) Opracowanie raportu z testów potwierdzającego skuteczność wdrożonych rozwiązań, c) Przekazanie kompletnej dokumentacji powdrożeniowej. 5. Szkolenia: a) Przeprowadzenie szkolenia administratorów z obsługi wdrożonych rozwiązań.
Dokumentacja powdrożeniowa	Wykonawca zobowiązany jest do przekazania Zamawiającemu: 1. Dokumentacji technicznej i konfiguracyjnej każdego z wdrożonych komponentów. 2. Schematów połączeń sieciowych i architektury logicznej. 3. Raportów z testów funkcjonalnych i bezpieczeństwa. 4. Protokołów odbioru poszczególnych etapów wdrożenia. 5. Potwierdzenia przeszkolenia personelu działu informatycznego.
Ochrona stacji roboczych oraz serwerów (rozwiązania klasy EDR)– 1 komplet	
Ogólne	Zamawiający wymaga dostawy 450 licencji ze wsparciem serwisowym przez okres 36 miesięcy.
Wspierane systemy operacyjne	
System Operacyjny Windows	Systemy Operacyjne Komputerów: • Windows 11 October 2024 Update (24H2) • Windows 11 October 2023 Update (23h2) • Windows 10 November 2022 Update (22H2)

	• Windows 11 September 2022 Update (22H2) • Windows 11 (initial release) • Windows 10 November 2021 Update (21H2) • Windows 10 May 2021 Update (21H1) • Windows 10 October 2020 Update (20H2) • Windows 10 May 2020 Update (20H1) • Windows 10 May 2019 Update (19H1) • Windows 10 October 2018 Update (Redstone 5) • Windows 10 April 2018 Update (Redstone 4) • Windows 10 Fall Creators Update (Redstone 3) • Windows 10 Creators Update (Redstone 2) • Windows 10 Anniversary Update (Redstone 1) • Windows 10 November Update (Threshold 2) • Windows 10 (initial release) • Windows 8.1 • Windows 8 • Windows 7 SP1 Windows Tablet oraz systemy wbudowane: • Windows 10 IoT Enterprise • Windows Embedded 8.1 Industry • Windows Embedded 8 Standard • Windows Embedded Standard 7 • Windows Embedded Compact 7 • Windows Embedded POSReady 7 • Windows Embedded Enterprise 7 Windows ARM64 desktop: • Windows 11 October 2024 Update (24H2) • Windows 10 November 2022 Update (22H2) • Windows 11 September 2022 Update (22h2) • Windows 10 November 2021 Update (21H2) Systemy operacyjne serwera: • Windows Server 2025 64x • Windows Server 2022 Core • Windows Server 2022 • Windows Server 2019 Core • Windows Server 2019 • Windows Server 2016 • Windows Server 2016 Core • Windows Server 2012 R2 • Windows Server 2012

	• Windows Small Business Server (SBS) 2011 • Windows Server 2008 R2
Systemy Operacyjne Linux i wersja kernel	Oparte o RPM • RHEL 7.x - 3.10.0 (build 957) 64-bit • RHEL 8.x - 4.18.0 64-bit • RHEL 9.x - 5.14.0 64-bit • Oracle Linux 7.x (UEK) - 4.18.0 64-bit • Oracle Linux 7.x (RHCK) - 3.10.0 build 957 64-bit • Oracle Linux 8.x (UEK) - 5.4.17 / 5.15.0 64-bit • Oracle Linux 8.x (RHCK) – 4.18.0 64-bit • Oracle Linux 9.x (UEK) – 5.15.0 64-bit • Oracle Linux 9.x (RHCK) – 5.14.0 64-bit • CentOS 7.x - 3.10.0 (build 957) 32-bit/64-bit • CentOS 8 Stream - 4.18.0 64-bit • CentOS 9 Stream - 5.14.0 64-bit • Fedora 37 – 42 – wsparcie do wygaśnięcia. 64-bit • AlmaLinux 8.x - 4.18.0 64-bit • AlmaLinux 9.x - 5.14.0 64-bit • Rocky Linux 8.x - 4.18.0 64-bit • Rocky Linux 9.x - 5.14.0 64-bit • CloudLinux 7.x - 3.10 (build 957) 64-bit • CloudLinux 8.x - 4.18.0 64-bit • Miracle Linux 8.x - 4.18.0 64-bit • Kylinv10 RHEL - 4.19.90 64-bit • Microsoft Azure Linux 3 – 6.6.64.x.azl3 64-bit Oparte o Debian • Debian 9 - 4.9.0 32-bit/64-bit • Debian 10 - 4.19 32-bit/64-bit • Debian 11 - 5.10 32-bit/64-bit • Debian 12 – 6.1.0 64-bit • Ubuntu 16.04.x - 4.8 / 4.10 / 4.13 / 4.15 32-bit/64-bit • Ubuntu 18.04.x - 5.0 / 5.3 / 5.4 64-bit • Ubuntu 20.04.x - 5.4 / 5.8 / 5.11 / 5.13 / 5.15 64-bit • Ubuntu 22.04.x - 5.15 / 5.19 64-bit • Ubuntu 23.04.x – 6.2.0 64-bit • Ubuntu 24.04.x – 6.8.0 64- bit • PopOS 22.04.x – 6.2.6 64-bit • Pardus 21 – 5.10.0 64-bit • Mint 20.x – 5.4.0 64-bit • Mint 21.x – 5.15.0 64-bit

	• Mint 22.x – 6.8.0.x 64-bit • Zorin OS – 6.5.x 64-bit • Linux Mint Debian Edition 6 – 6.1.x 64-bit Oparte o SUSE • SLES 12 SP4 - 4.12.14-x 64-bit • SLES 12 SP5 - 4.12.14-x 64-bit • SLES 15 SP1 - 4.12.14-x 64-bit • SLES 15 SP2 - 5.3.18-x 64-bit • SLES 15 SP3 - 5.3.18-x 64-bit • SLES 15 SP4 – 5.14.21 64-bit • SLES 15 SP5 – 5.14.21 64-bit • SLES 15 SP6 – 6.4.x 64-bit • SLED 15 SP4 – 5.14.21 64-bit • openSUSE Leap 15.4 - 15.5 - 5.14.21 64-bit Cloud based Linux • AWS Bottlerocket 2020.03 - 5.4.x, 5.10.x 64-bit • Amazon Linux v2 - 4.14.x / 4.19.x / 5.10 64-bit • Amazon Linux 2023 – 6.1.x 64-bit • Google COS Milestones 77, 81, 85 - 4.19.112 / 5.4.49 64-bit • Azure Mariner 2 - 5.15 64-bit
Linux dla ARM	Oparte o RPM • RHEL 8.x – 4.18.0-x • RHEL 9.x – 5.14 • AlmaLinux 9.x – 5.14 • Rocky Linux 9.x – 5.14 Oparte o Debian • Debian 11 – 5.10 / 6.1 • Debian 12 – 6.1.0.x • Ubuntu 20.04.x – 5.15 • Ubuntu 22.04.x – 5.15 / 5.19 • Ubuntu 24.04.x – 6.8.0.x Oparte o SUSE • SLES 15 SP4 – 5.14.21-x • openSUSE Leap 15.4-15.5 – 5.14.21-x Oparte o chmurę • Amazon Linux v2 – 5.10 • Amazon Linux 2023 - 6.1
Systemy Operacyjne Mac OS X	• macOS Tahoe (26.x) • macOS Sequoia (15.x) • macOS Sonoma (14.x)

	• macOS Ventura (13.x) • macOS Monterey (12.x) • macOS Big Sur (11.x)
Obsługiwane Środowiska Microsoft Exchange	Security for Exchange wspiera następujące wersje i role Microsoft Exchange: • Exchange Server 2019 z rolą Edge Transport lub Mailbox • Exchange Server 2016 z rolą Edge Transport lub Mailbox • Exchange Server 2013 z rolą Edge Transport lub Mailbox • Exchange Server 2010 z rolą Edge Transport, Hub Transport lub Mailbox Security for Exchange jest kompatybilny z Microsoft Exchange Database AvailabilityGroups (DAG).
Ochrona środowisk wirtualnych (SVE)	1. Możliwość zastosowania zewnętrznego silnika skanującego w postaci maszyny wirtualnej. 2. Maszyna wirtualna pełniąca rolę silnika skanującego może być pobrana w formacie: • OVA • XVA • VHD • VHDX • VMDK Środowiska wspierane: • VMware vSphere and vCenter Server: - version 6.5 - version 6.7, including update 1, update 2a and update 3 - version 7.0, including update 1, update 2, update 2b, update 2c and update 2d - version 8.0, including update 1, update 2 • VMware ESXi 8.0, including update 1, update 2 • VMware Horizon/View 7.8, 7.7, 7.6, 7.5, 7.1, 6.x, 5.x • VMware Workstation 11.x, 10.x, 9.x, 8.0.6 • VMware Player 7.x, 6.x, 5.x • Citrix Xen Hypervisor: 8.4. • Citrix Xen Hypervisor: 7.1 (with the XS71ECU2060 hotfix), 8.2. • Citrix Virtual Apps and Desktops 7 1808, 7 1811, 7 1903, 7 1906 • Citrix XenApp and XenDesktop 7.18, 7.17, 7.16, 7.15 LTSR, 7.6 LTSR • Citrix VDI-in-a-Box 5.x • Microsoft Hyper-V Server 2008 R2, 2012, 2012 R2, 2016, 2019 or Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019 (including Hyper-V Hypervisor), 2022, 2025 • Proxmox Virtual Environment 8.4, 9.0

	• Red Hat Enterprise Virtualization 3.0 (including KVM Hypervisor) • Oracle VM 3.0 • Oracle VM VirtualBox 5.2, 5.1
Ochrona antywirusowa i antyspyware	1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 2. Interfejs oraz pomoc techniczna świadczona w języku polskim. 3. Wykrywanie zagrożeń i analiza procesów technikami heurystycznymi. 4. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. 5. Wbudowana technologia do ochrony przed rootkitami. 6. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 7. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie". 8. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 9. Możliwość ustawienia zadania skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu. 10. Możliwość skanowania dysków sieciowych i dysków przenośnych. 11. Skanowanie plików spakowanych i skompresowanych. 12. Ochrona krytycznych kluczy rejestru przed ich wykorzystaniem lub nieautoryzowanym dostępem do nich. 13. Możliwość dodawania wykluczeń na podstawie: a) Plik b) Folder c) Rozszerzenie d) Proces e) Hash pliku f) Hash certyfikatu g) Nazwa zagrożenia h) Wiersz poleceń i) IP/maska 14. Skanowanie poczty opartej o protokoły IMAP, MAPI, POP3 i SMTP w czasie rzeczywistym. 15. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie w przeglądarce. 16. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Dodatkowo zdefiniowane są grupy stron przez producenta. 17. Wsparcie przeglądarek Internet Explorer 8+, Mozilla Firefox 30+, Google Chrome 34+, Safari 4+, Microsoft Edge 20+ i Opera 21+ bez konieczności zmian w konfiguracji. 18. Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz

	szyfrowanych protokołów HTTPS, RDP, FTPS, SCP/SSH, IMAPS, MAPI, POP3S, SMTPS. 19. Program powinien skanować ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe. 20. W GUI programu na punkcie końcowym z systemem Windows oraz macOS możliwość wyświetlenia aktualnej wersji produktu i aktualnej wersji silników. 21. W GUI programu na punkcie końcowym z systemem Windows oraz macOS możliwość wyświetlenia, kiedy była przeprowadzana ostatnia aktualizacja z dokładnością co do dnia i godziny. 22. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń. 23. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy. 24. Administrator musi mieć możliwość ukrycia ikony oprogramowania w obszarze powiadomień systemu Windows. 25. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na punkcie końcowym Windows i macOS. 26. Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet. 27. Oprogramowanie klienckie posiada wbudowaną funkcję do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej. 28. System musi umożliwiać kontrolę dostępu do urządzeń na podstawie interfejsów, do których zostały one podłączone. 29. Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej na podstawie ich wykrycia lub wpisanych ręcznie ID urządzenia lub ID produktu. 30. Funkcja blokowania informacji wysyłanych przez HTTP lub SMTP jak: (adresy e-mail, Piny, Konta bankowe, hasła itp.). 31. Funkcja blokowania wysyłanych informacji konfigurowana zdalnie przez administratora. 32. Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego. 33. Wbudowany IDS. 34. Możliwość wykorzystania funkcji skanowania lokalnego lub hybrydowego ze sprawdzaniem reputacji plików w chmurze. 35. Możliwość tworzenia list sieci zaufanych. 36. Możliwość dezaktywacji funkcji zapory sieciowej. 37. Dodatkowa funkcja ochrony przeciwko znanym zagrożeniom typu ransomware. 38. Użytkownik na punkcie końcowym ma możliwość opóźnienia restartu potrzebnego do zakończenia jednego lub wielu zadań (konfigurowalne w

	polityk bezpieczeństwa). 39. Komunikacja między konsolą zarządzającą, a punktami końcowymi jest szyfrowana. 40. Wbudowana ochrona przed exploitami wyposażona w minimum 15 różnych technik wykrycia exploitów z możliwością włączenia lub wyłączenia każdej z nich oraz dająca możliwość dodania własnych procesów. Funkcja umożliwia również: a) Możliwość wymuszenia funkcji DEP systemu Windows. b) Możliwość wymuszenia relokacji modułów (ASLR) dla Windows. 41. Ochrona przed atakami sieciowymi – Mechanizm obronny przed atakującymi próbującymi uzyskać dostęp do systemu poprzez wykorzystanie luk w sieci. Funkcja ta musi obejmować ochronę przed technikami takimi jak: a) Pierwszy dostęp, b) Dostęp do poświadczeń, c) Wykrycie, d) Crimeware, e) Ruch boczny. 42. Ochrona przed ransomware - możliwość wykrywania i blokowania ataków typu ransomware niezależnie od tego czy atak został przeprowadzony lokalnie lub zdalnie na punkcie końcowym oraz utworzenie kopii zapasowej plików w momencie szyfrowania, a w przypadku ataku odzyskanie i przywrócenie ich do pierwotnej lokalizacji. Oprogramowanie musi dać możliwość odzyskania plików na żądanie lub automatycznie, o następujących rozszerzeniach: 3fr, ai, arw, bay, cdr, cer, cr2, crt, crw, dcr, der, dll, dng, doc, docm, docx, dwg, dxf, dxg, eps, erf, exe, indd, jpe, jpeg, jpg, mdf, mef, mrw, nef, nrw, odb, odc, odm, odp, ods, odt, orf, p12, p7b, p7c, pdd, pdf, pef, pem, pfx, ppt, pptm, pptx, psd, pst, ptx, png, r3d, raf, rtf, rw2, rwl, sr2, srf, srw, wb2, wpd, wps, x3f, xlk, xls, xlsb, xlsm, xlsx, msg, py, ini, xml, msi, cab, tsf, dgn, log, gif, csv, avi, mov, mp4 43. System musi wykrywać podatne sterowniki zainstalowane na punkcie końcowym z Windows i Linux. 44. Agent i usługi oprogramowania antywirusowego zainstalowanego na punkcie końcowym muszą być chronione przed próbami manipulacji i naruszenia ich integralności w systemie Windows. 45. Oprogramowanie musi skanować nośniki USB zanim użytkownik zaloguje się do systemu Windows. 46. System musi umożliwiać skanowanie oprogramowania układowego UEFI. 47. System umożliwia przechwytywanie TLS handshake pozwalając na skanowanie ruchu sieciowego bez konieczności deszyfracji. 48. Telemetria - Możliwość przesyłania nieprzetworzonych danych bezpieczeństwa z punktów końcowych z systemem operacyjnym

Załącznik nr 2.5 do SWZ

	Windows i macOS do SIEM Splunk (wymaga TLS 1.2 lub wyższy) lub z systemem Windows i Linux do serwera Syslog (JSON). 49. Oprogramowanie pozwala na skanowanie punktów końcowych pod kątem wyszukiwania wskaźników naruszeń bezpieczeństwa (IOC).
Stacje robocze i serwery	1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. 3. Jedna wersja instalacyjna na stacje robocze i serwery plików Windows. 4. Oprogramowanie zawiera monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego. 5. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program powinien pytać o hasło. 6. Produkt i zawartość zabezpieczeń powinny być aktualizowane nie rzadziej niż raz na godzinę. 7. Oprogramowanie posiada możliwość raportowania zdarzeń informacyjnych. 8. Oprogramowanie musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju. 9. Oprogramowanie musi posiadać możliwość skanowania jedynie nowych i zmienionych plików. 10. Oprogramowanie posiada możliwość odblokowania ustawień lokalnych konfiguracji na systemach Windows po doinstalowaniu odpowiedniego modułu. Zmiana ustawień zabezpieczona jest hasłem. 11. Po kliknięciu prawym klawiszem myszy na ikonie programu i wybraniu opcji „O programie”, możliwość wyświetlenia danych do pomocy technicznej tj: adres strony pomocy, adres e-mail do administratora ochrony, numer telefonu do administratora ochrony z wyłączeniem systemów Linux. 12. Dla maszyn z systemem Linux możliwość wskazania katalogów, które mogą być chronione w czasie rzeczywistym.
Ochrona Exchange	1. Rozwiązanie musi zapewniać filtrowanie antymalware dla przychodzącego, wewnętrznego i wychodzącego ruchu mailowego. 2. Rozwiązanie musi wspierać skanowanie "na życzenie" oraz skanowanie według harmonogramu dla skrzynek pocztowych i folderów publicznych, w tym możliwość zarówno wykluczenia konkretnych skrzynek bądź folderów publicznych, jak i skanowania tylko emaili z załącznikami bądź emaili otrzymanych w ciągu określonego czasu. 3. Zdolność konfigurowania różnych akcji wykonywanych na plikach zainfekowanych, podejrzanych oraz niemożliwych do przeskanowania.

	4. Możliwość skanowania w poszukiwaniu potencjalnie niechcianych aplikacji (PUA). 5. Możliwość skanowania malware wewnątrz archiwów. 6. Rozwiązanie musi zapewniać filtr antyspamowy dla ruchu mailowego, z możliwością dodania do białej listy konkretnych adresów email i domen. 7. Możliwość odpytania serwerów Realtime Blackhole List (RBL) zdefiniowanych przez administratorów i odfiltrowania wiadomości zaklasyfikowanych jako spam bazując na reputacji wysyłającego serwera. 8. Zdolność automatycznego oznaczenia jako spam wiadomości mailowych napisanych przy użyciu alfabetów azjatyckich bądź cyrylicy. 9. Zdolność do wykonania zapytań bazujących na chmurze dla udoskonalonej ochrony przeciw nowemu spamowi. 10. Zdolność do podjęcia różnych akcji na wykrytych mailach ze spamem, takich jak poprzedzanie tematu maila konkretną etykietą, usunięcie, przeniesienie do kwarantanny bądź przekierowanie maila do konkretnej skrzynki pocztowej. 11. Rozwiązanie musi zapewniać funkcjonalności filtrowania zawartości dla przychodzącego, wewnętrznego i wychodzącego ruchu mailowego, bazujące na konkretnym tekście bądź wyrażeniach regularnych zgodnych z tematem maila i/lub jego zawartością. 12. Zdolność do podejmowania różnych akcji na emailach, pasujących do reguł filtrowania treści, takich jak dodawanie prefiksu w postaci taga do tematu maila, usuwanie, wysyłanie do kwarantanny bądź przekierowywanie emaila do konkretnej skrzynki.
Konsola zdalnej administracji	1. System musi umożliwiać centralne zarządzanie i konfigurację ochrony wspieranych stacji roboczych i serwerów. 2. Możliwość integracji wielu domen Active Directory. 3. Możliwość uruchomienia zdalnego skanowania wybranych punktów końcowych. 4. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony punktu końcowego (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania na żądanie, zainstalowanych modułów, ostatniej aktualizacji oraz przypisanej polityki). 5. Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci, analityk bezpieczeństwa lub z ustawieniami niestandardowymi. 6. Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, systemu operacyjnego. 7. Możliwość centralnej aktualizacji punktów końcowych z serwera w sieci lokalnej lub z Internetu. 8. Możliwość wysłania linku instalacyjnego bezpośrednio z poziomu konsoli administracyjnej. 9. Możliwość uruchomienia centralnej konsoli jedynie z poziomu

	przeglądarki internetowej. 10. Możliwość ręcznego (na żądanie) i automatycznego generowania raportów (według ustalonego harmonogramu) oraz wyeksportowanie ich do formatu: pdf i csv. Również zbiorczo w formie archiwum zip. 11. Raport generowany według harmonogramu z możliwością automatycznego wysłania go do osób zdefiniowanych w tym raporcie. 12. Możliwość generowania raportu co godzinę. 13. Pierwsza aktywacja modułu kontroli urządzeń nie wymaga restartu stacji docelowej. 14. Możliwość dodania etykiety do stacji roboczej. 15. Możliwość dezinstalacji oprogramowania antywirusowego innych firm w trakcie instalacji zdalnej. 16. Możliwość przechowywania kwarantanny maksymalnie 180 dni. 17. Możliwość definiowania, czy pliki z kwarantanny mają być przesyłane do producenta i co ile godzin ma się ta czynność odbywać. 18. Po aktualizacji zawartości bezpieczeństwa opcja automatycznego przeskanowania kwarantanny. 19. Wsparcie techniczne mailowe i telefoniczne w j. polskim od poniedziałku do piątku w godzinach 8:00-16:00. W pozostałych godzinach możliwość bezpośredniego kontaktu z producentem (24/7) w j. angielskim. 20. Po integracji z lokalnym Active Directory możliwość przypisywania polityk automatycznie po zalogowaniu do systemu operacyjnego w zależności od tego jaki użytkownik domenowy się zalogował lub do jakiej grupy domenowej on należy. 21. Możliwość automatycznego przypisywania polityk na podstawie reguły lokalizacji. Określenie lokalizacji na podstawie: a) Zakres adresów IP/IP, b) Adres bramy, c) Adres serwera WINS, d) Adres serwera DNS, e) Połączenie DHCP sufiksów DNS, f) Punkt końcowy może rozwiązać hosta, g) Typ sieci, h) Nazwa hosta. 22. Uwierzytelnienie dwuskładnikowe realizowane przy pomocy aplikacji kompatybilnej ze standardem RFC6238. 23. Możliwość naprawy instalacji agenta z poziomu konsoli. 24. Możliwość utworzenia reguły, która będzie usuwała punkty końcowe z konsoli zarządzającej, jeżeli punkt końcowy nie połączył się z konsolą przez określoną liczbę dni. Funkcja ta pozwala również na określenie wzoru nazw maszyn, które automatycznie będą usuwane oraz na określenie godziny, o której te maszyny będą usuwane. 25. Możliwość wyświetlania adresu MAC dołączonego do nazwy hosta. 26. Możliwość wyświetlenia czy punkt końcowy jest serwerem czy stacją

	roboczą. 27. Możliwość wyświetlenia informacji czy zainstalowany na punkcie końcowym system operacyjny to Windows, Linux lub MacOS. 28. Możliwość filtrowania punktów końcowych, które były online w ciągu ostatnich 24 godzin, 7 lub 30 dni. 29. Menu tworzenia paczek instalacyjnych musi określać czy dany moduł jest dostępny dla stacji roboczych Windows, Serwerów Windows, Linux, MacOS. 30. Oprogramowanie umożliwia pobranie oddzielnego pakietu instalacyjnego dla systemów MacOS z Intel x86 oraz oddzielnego dla Apple M oraz osobnego pakietu dla systemów Windows z Intel x86 oraz oddzielnego dla architektury ARM. 31. System umożliwia pobieranie plików poddanych kwarantannie z poziomu centralnej konsoli administracyjnej. 32. Możliwość wygenerowania i zapisania logów na stacji roboczej z poziomu konsoli zarządzającej. 33. Możliwość zarządzania ochroną na serwerach Exchange, tworzenie polityk i konfiguracji zdalnej ochrony. 34. Znaczniki punktów końcowych – oprogramowanie musi umożliwiać przypisywanie znaczników (tagów) do punktów końcowych. Przypisywanie musi odbywać się ręcznie lub automatycznie. Musi istnieć możliwość filtrowania punktów końcowych na podstawie kilku wybranych znaczników w jednym czasie. 35. Ochrona proaktywna oparta o maszynowe uczenie, która działa w fazie poprzedzającej wykonanie. Ochrona ta musi wykrywać zagrożenia takie jak: a) Ukierunkowane ataki, b) Podejrzane pliki i ruch w sieci, c) Exploity, d) Ransomware, e) Grayware. 36. Moduł ochrony proaktywnej musi posiadać oddzielne działania jakie będzie podejmował dla plików i oddzielne dla ruchu sieciowego. 37. Moduł ochrony proaktywnej musi działać w trybach, które administrator może dowolnie zmieniać na: a) Tolerancyjny, b) Normalny, c) Agresywny. 38. Zintegrowany sandbox po stronie producenta, który pozwala na analizę pliku: a) Plik może zostać wysłany automatycznie ze stacji roboczej, jeżeli oprogramowanie uzna go za podejrzany lub ręcznie z poziomu konsoli przez administratora, b) Możliwość ręcznego przesłania archiwum zabezpieczonego hasłem,

	c) Możliwość ręcznego przesłania adresu URL, d) W przypadku ręcznego przesłania wielu plików jednorazowo, możliwość detonacji próbek pojedynczo. 39. Wbudowany sandbox musi działać w trybie monitorowania i blokowania. 40. Wbudowany sandbox musi oferować działania naprawcze takie jak dezynfekcja, przeniesienie do kwarantanny lub tylko raportowanie. 41. Wbudowany sandbox musi oferować opcję wstępnego filtrowania plików z kategorii aplikacje, dokumenty, skrypty, archiwa, maile zapisane do pliku, pod kątem podejrzanego zachowania. 42. Wbudowany sandbox musi posiadać opcję, która pozwala na dodanie określonych rozszerzeń do wyjątków, pliki z tym rozszerzeniem nie zostaną przesłane do sandboxa. 43. Minimalny rozmiar pliku jaki może zostać automatycznie przesłany do sandboxa to 1KB. 44. Maksymalny rozmiar pliku jaki może zostać automatycznie przesłany do sandboxa to 50MB. 45. System zarządzania ryzykiem – Zintegrowany z konsolą zarządzającą system, który pozwala oszacować podatność środowiska na atak na podstawie punktów ryzyka. Punkty ryzyka powinny być przydzielane od 0 do 100, gdzie liczba mniejsza stanowi mniejsze ryzyko, a liczba większa większe ryzyko. System ponadto musi posiadać: a) Funkcję, która pozwala wyszukiwać podatności ustawień punktów końcowych oraz naprawiać je lub ignorować z podziałem na typ wykrytej konfiguracji: - Przeglądarka - Sieć - System operacyjny - Luki System ponadto musi określać nasilenie zagrożenia wynikłego z wykrytej podatności w oparciu o punkty procentowe oraz posiadać funkcję cofnięcia wprowadzonych zmian w ustawieniach systemów. b) System zarządzania ryzykiem powinien określać luki w wykrytym zainstalowanym oprogramowaniu podając przy tym numer CVE tych luk. c) System pozwala na śledzenie i wykrywanie ryzykownych działań jakie podejmuje użytkownik na punkcie końcowym wraz z poinformowaniem o liczbie użytkowników, których takie działanie dotyczy oraz jaka jest jego szkodliwość. d) System pozwala na skanowanie punktów końcowych pod kątem wykrywania ryzyka na podstawie harmonogramu lub pojedynczo utworzonego zadania. e) System pozwala na raportowanie na ilu urządzeniach wykryto błędną konfigurację i luki w aplikacjach oraz jaka jest ilość takich podatności i ich szkodliwość wyrażona w procentach.

	f) System pozwala na wykrywanie podatności w oparciu o standardy bezpieczeństwa zgodne z: CIS v8.0, CMMC 2.0 (US), Cyber Essentials v3.2 (UK), Essential Eight v2023.11 (AU), HIPPA (US), SOC 2, ISO/IEC 27001:2022, PCI DSS v4.0.1, GDPR (EU), NIS2 (EU), DORA (EU). 46. Możliwość scentralizowanego podglądu wykrytych zagrożeń z wszystkich modułów ochrony w jednym miejscu i odfiltrowania ich według daty, kategorii, typu zagrożenia, działań naprawczych i innych. 47. Możliwość ustawienia wymagania zmiany hasła logowania do konsoli co 90 dni. 48. Możliwość zablokowania konta w konsoli, jeżeli użytkownik tego konta podejmował pięć kolejnych prób logowania nieprawidłowym hasłem. 49. Funkcja pojedynczego logowania – Single Sign-on (SSO) przy integracji z Microsoft Azure. 50. Raport podsumowujący - Możliwość podglądu raportu, który streszcza stan środowiska firmowego w ciągu ostatnich 24h, 7 dni lub 30 dni. Z rozróżnieniem na takie sekcje jak: a) Zarządzane punkty końcowe, b) Ilość zajętych miejsc w licencji z rozróżnieniem na stacje robocze Windows, serwery Windows, macOS, Linux oraz fizyczne punkty końcowe i maszyny wirtualne, c) Pięć rodzajów najczęściej blokowanych zagrożeń, d) Podział zagrożeń na urządzenia takie jak stacje robocze i serwery, e) Status incydentów bezpieczeństwa, które wystąpiły, f) Stan modułów punktów końcowych, g) Ocena ryzyka firmy, h) Zablokowane strony WWW w oparciu o wykryte tam szkodliwe oprogramowanie, phishing, oszustwa, i) Zablokowane techniki ataku sieciowego z podziałem na takie jak wczesny dostęp, dostęp do poświadczeń, wykrycie, ruch boczny, crimeware. 51. Możliwość integracji z innymi systemami poprzez API takich elementów bądź sekcji jak: a) Firmy, b) Raporty, c) Licencjonowanie, d) Konta, e) Pakiety, f) Incydenty, g) Sieć, h) Kwarantanna, i) Integracje, j) Event Push Service, k) Polityki.

	52. Early access – Oprogramowanie musi umożliwiać dobrowolne przystąpienie do darmowych testowych programów wczesnego dostępu. Programy wczesnego dostępu powinny umożliwiać testowanie najnowszych funkcji oprogramowania, których nie ma jeszcze w wersji końcowej produktu. Uzyskanie dostępu do programu testowego musi być natychmiastowe. 53. Możliwość utworzenia konsoli typu Partner, która pozwala na zarządzanie wieloma firmami z poziomu jednej scentralizowanej konsoli zarządzającej, konsola partnerska musi umożliwiać: a) Pobieranie przez partnera plików z kwarantanny podległych firm, b) Zarządzanie systemem ochrony firm podrzędnych przez Partnera z jednej konsoli lub tworzenie bezpośrednich dostępów użytkowników dla tych firm, c) Odseparowanie przez administratora konsoli podrzędnej od konsoli partnera nadrzędnego. 54. Profil firmy - Możliwość określenia profilu przedsiębiorstwa w konsoli webowej. Dostępne są kategorie m.in: Lotnictwo, Budownictwo, Edukacja, Służba zdrowia, Handel i inne. 55. System musi umożliwiać wybór trzech poziomów obciążenia procesora dla zadań określonych w harmonogramie skanowania na systemach Linux i macOS. 56. System musi posiadać funkcję wstrzymywania skanowania podczas pracy na baterii. 57. Konsola administracyjna umożliwia zmianę motywu dla interfejsu spośród jasnego, ciemnego lub wybranego automatycznie w oparciu o ustawienia systemowe. 58. System umożliwia tymczasowe wyłączenie wszystkich lub wybranych modułów ochrony na określony czas, który wynosi 15 minut, 30 minut, 1 godzina, 2 godziny, 4 godziny. Po ponownym uruchomieniu ochrony możliwość przeprowadzenia pełnego skanowania. 59. Centrum integracji – Panel umożliwiający zarządzanie integracjami z rozwiązaniami zewnętrznymi tj. Vmware vCenter, Veeam Backup & Replication, Microsoft Active Directory, Vmware Tanzu, Microsoft Exchange (on-premises), SecurityCoach (KnowBe4). 60. Wbudowany sandbox musi posiadać możliwość przesyłania pliku do analizy z komputera zdalnego za pomocą podanej ścieżki. Wielkość pliku nie może przekraczać 100MB. 61. Filtrowanie wykrytych incydentów bezpieczeństwa m.in. na podstawie: a) ID, b) Ostatnia aktualizacja, c) Status, d) Osoba przydzielająca, e) Data utworzenia, f) Priorytet,

	g) Ocena szkodliwości w skali 0-100, h) Podmioty, i) Zasoby, j) Ostatnia faza killchain, k) Wykonane czynności, l) Skorelowane incydenty, m) Typ incydentu. 62. System umożliwia wygenerowanie i pobranie zestawu informacji z chronionych punktów końcowych w formie archiwum. Funkcja powinna być dostępna dla systemów Windows, Linux oraz macOS. Archiwum musi zawierać co najmniej informacje: a) Windows - Logi zainstalowanego agenta, - Dziennik zdarzeń Windows, - Informacje o systemie, - DnsCache, - Webcache, - Informacje z głównych katalogów rejestru (SYSTEM, SOFTWARE, DEFAULT, DRIVERS, SAM, SECURITY), - Harmonogram zadań, - Historia Powershell (jeśli włączono). b) Linux - Podstawowy log pomocy technicznej zainstalowanego agenta, - Certyfikaty, - Autorun i usługi, - Informacje sieciowe, - Informacje systemowe, - Zainstalowane pakiety. c) macOS - Podstawowy log pomocy technicznej zainstalowanego agenta, - Autorun, - Lista procesów, - Informacje sieciowe, - Informacje o systemie. 63. Oprogramowanie musi umożliwiać przegląd konfiguracji punktów końcowych w czasie rzeczywistym poprzez tworzenie zapytań pod kątem wykrywania: a) historia powłoki, b) wczytywanie bibliotek .dll z podejrzanej lokalizacji, c) Sesje logowania z użyciem jawnych danych uwierzytelniających. d) Arp cache, e) Ip forwarding, f) Lista zamontowanych nośników, g) Konfiguracja ip tables,

	h) Połączenia TLS które używają certyfikatów self-signed, i) Używane rozszerzenia w przeglądarce Chrome, j) Używane rozszerzenia w przeglądarce Firefox, k) Używane rozszerzenia w przeglądarce Safari, l) Źródła apt w systemach Linux, m) Wyświetlanie zainstalowanych pakietów DEB, n) Wyświetlanie zainstalowanych pakietów RPM, o) Pakiety Python zainstalowane w systemie, p) Lista użytkowników, którzy zostali utworzeni w ciągu ostatnich 30 dni (Linux), q) Wykrywanie czy aplikacje zdalnego dostępu są zainstalowane w systemie MacOS, r) Wykrywanie czy Kontrola Kont Użytkowników (UAC) jest wyłączona, s) Wykrywanie czy SecureBoot jest włączony, t) Lista zapamiętanych sieci bezprzewodowych, u) Wykrywa, czy zmienił się domyślny folder startowy użytkownika, v) Wykrywa, czy zmienił się domyślny folder startowy maszyny. 64. Oprogramowanie musi umożliwiać tworzenie konfigurowalnych reguł, po spełnieniu których może zostać wygenerowany incydent bezpieczeństwa. Funkcja ta powinna: a) Oferować opcję podjęcia automatycznych działań po spełnieniu warunków tj.: izolacja punktu końcowego, wygenerowanie archiwum diagnostycznego, przesłanie pliku do analizy sandbox, zakończenie procesu i innych. b) Automatyczne działania zapobiegawcze są zależne od wyboru kategorii. c) Tworzenie reguł musi być określone poprzez wybór operatora np. „to", „zawiera", „jest jednym z" itp. d) Dotyczyć określonych kryteriów tj. proces, plik, rejestr, połączenia. e) Zapewniać możliwość tworzenia zapytań YARA. f) Umożliwiać określenie priorytetu kolejności automatyzacji. g) Administrator powinien mieć możliwość wyboru poziomu szkodliwości potencjalnie wygenerowanych incydentów (wysokie, średnie i niskie).
EDR-Endpoint Detection and Response	Produkt zapewnia szczegółowe informacje o wykrytych incydentach, interaktywną mapę incydentów i działania naprawcze.
Wspierane systemy operacyjne	Systemy desktopowe • Windows 11 October 2024 Update (24H2) • Windows 11 October 2023 Update (23H2) • Windows 10 November 2022 Update (22H2) • Windows 11 September 2022 Update (22H2) • Windows 11 (initial release)

	• Windows 10 November 2021 Update (21H2) • Windows 10 May 2021 Update (21H1) • Windows 10 October 2020 Update (20H2) • Windows 10 May 2020 Update (20H1) • Windows 10 May 2019 Update (19H1) • Windows 10 October 2018 Update (Redstone 5) • Windows 10 April 2018 Update (Redstone 4) • Windows 10 Fall Creators Update (Redstone 3) • Windows 10 Creators Update (Redstone 2) • Windows 10 Anniversary Update (Redstone 1) • Windows 10 November Update (Threshold 2) • Windows 10 (initial release) • Windows 8.1 • Windows 8 • Windows 7 SP1 Systemy operacyjne dla serwerów: • Windows Server 2025 64x • Windows Server 2022 Core • Windows Server 2022 • Windows Server 2019 Core • Windows Server 2019 • Windows Server 2016 • Windows Server 2016 Core • Windows Server 2012 R2 • Windows Server 2012 • Windows Small Business Server (SBS) 2011 • Windows Server 2008 R2 MacOS: • macOS Tahoe (26.x) • macOS Sequoia (15.x) • macOS Sonoma (14.x) • macOS Ventura (13.x) • macOS Monterey (12.x) • macOS Big Sur (11.x) Linux Oparte o RPM • RHEL 7.x - 3.10.0 (build 957) 64-bit • RHEL 8.x - 4.18.0 64-bit • RHEL 9.x - 5.14.0 64-bit • Oracle Linux 7.x (UEK) - 4.18.0 64-bit

	• Oracle Linux 7.x (RHCK) - 3.10.0 build 957 64-bit • Oracle Linux 8.x (UEK) - 5.4.17 / 5.15.0 64-bit • Oracle Linux 8.x (RHCK) – 4.18.0 64-bit • Oracle Linux 9.x (UEK) – 5.15.0 64-bit • Oracle Linux 9.x (RHCK) – 5.14.0 64-bit • CentOS 7.x - 3.10.0 (build 957) 32-bit/64-bit • CentOS 8 Stream - 4.18.0 64-bit • CentOS 9 Stream - 5.14.0 64-bit • Fedora 37 – 42 – wsparcie do wygaśnięcia. 64-bit • AlmaLinux 8.x - 4.18.0 64-bit • AlmaLinux 9.x - 5.14.0 64-bit • Rocky Linux 8.x - 4.18.0 64-bit • Rocky Linux 9.x - 5.14.0 64-bit • CloudLinux 7.x - 3.10 (build 957) 64-bit • CloudLinux 8.x - 4.18.0 64-bit • Miracle Linux 8.x - 4.18.0 64-bit • Kylinv10 RHEL - 4.19.90 64-bit • Microsoft Azure Linux 3 – 6.6.64.x.azl3 64-bit Oparte o Debian • Debian 9 - 4.9.0 32-bit/64-bit • Debian 10 - 4.19 32-bit/64-bit • Debian 11 - 5.10 32-bit/64-bit • Debian 12 – 6.1.0 64-bit • Ubuntu 16.04.x - 4.8 / 4.10 / 4.13 / 4.15 32-bit/64-bit • Ubuntu 18.04.x - 5.0 / 5.3 / 5.4 64-bit • Ubuntu 20.04.x - 5.4 / 5.8 / 5.11 / 5.13 / 5.15 64-bit • Ubuntu 22.04.x - 5.15 / 5.19 64-bit • Ubuntu 23.04.x – 6.2.0 64-bit • Ubuntu 24.04.x – 6.8.0 64- bit • PopOS 22.04.x – 6.2.6 64-bit • Pardus 21 – 5.10.0 64-bit • Mint 20.x – 5.4.0 64-bit • Mint 21.x – 5.15.0 64-bit • Mint 22.x – 6.8.0.x 64-bit • Zorin OS – 6.5.x 64-bit • Linux Mint Debian Edition 6 – 6.1.x 64-bit Oparte o SUSE • SLES 12 SP4 - 4.12.14-x 64-bit • SLES 12 SP5 - 4.12.14-x 64-bit • SLES 15 SP1 - 4.12.14-x 64-bit

	• SLES 15 SP2 - 5.3.18-x 64-bit • SLES 15 SP3 - 5.3.18-x 64-bit • SLES 15 SP4 – 5.14.21 64-bit • SLES 15 SP5 – 5.14.21 64-bit • SLES 15 SP6 – 6.4.x 64-bit • SLED 15 SP4 – 5.14.21 64-bit • openSUSE Leap 15.4 - 15.5 - 5.14.21 64-bit Cloud based Linux • AWS Bottlerocket 2020.03 - 5.4.x, 5.10.x 64-bit • Amazon Linux v2 - 4.14.x / 4.19.x / 5.10 64-bit • Amazon Linux 2023 – 6.1.x 64-bit • Google COS Milestones 77, 81, 85 - 4.19.112 / 5.4.49 64-bit • Azure Mariner 2 - 5.15 64-bit
Komponenty EDR	Główne elementy: 1. Sensor EDR, który gromadzi i przetwarza dane dotyczące punktu końcowego i zachowania aplikacji w celu ich raportowania. 2. Analityka Bezpieczeństwa, komponent służący do interpretacji metadanych gromadzonych przez sensor EDR. 3. Możliwość instalacji dodatkowego, dedykowanego agenta z sensorem EDR dla urządzeń z systemem Windows, aby rozszerzyć już zainstalowaną równolegle ochronę świadczoną przez innego producenta oprogramowania antywirusowego.
Wykrywanie podejrzanej aktywności	Monitorowanie zdarzeń na punktach końcowych w poszukiwaniu oznak ataku i wywoływanie incydentów po wykryciu takiej aktywności. 1. Bazowanie na systemach opartych o techniki MITRE ATT&CK i własnej inteligencji. 2. Zgłaszanie naruszeń jako incydent w module EDR.
Badanie incydentów i wizualizacja	1. Produkt zapewnia wsparcie analizy incydentów poprzez dostarczenie narzędzi, które pomagają filtrować, badać i podejmować działania dotyczące wszystkich zdarzeń bezpieczeństwa wykrytych przez czujnik EDR w określonym czasie. 2. Produkt integruje się z bazą wiedzy MITRE ATT&CK i odpowiednio oznacza zdarzenia bezpieczeństwa. 3. Produkt zapewnia zaawansowaną wizualizację zdarzeń bezpieczeństwa z określonymi danymi lub działaniami z następującymi informacjami: a) Karta podsumowująca zawiera przegląd wpływu zdarzenia i szczegółowe informacje o każdym węźle zdarzenia, b) Funkcja osi czasu zbiera informacje o rozwoju zdarzenia bezpieczeństwa w kolejności chronologicznej, c) System gromadzi informacje o działaniach podejmowanych przez produkt w związku ze zdarzeniem bezpieczeństwa.
Incydenty	1. Oprogramowanie pozwala na informowanie o zagrożeniach wykrytych i zablokowanych w formie grafu i chronologicznej linii zdarzeń oraz daje

	możliwość: a) Filtrowania zdarzeń, b) Zakończenia procesów, c) Dodania procesów do czarnej listy, d) Dodania procesów do białej listy, e) Izolacji hosta, f) Przesłania pliku do Sandbox, g) Sprawdzenia informacji o pliku w Google, h) Sprawdzenia informacji o pliku w VirusTotal. 2. Możliwość szybkiego podglądu incydentów za pomocą spersonalizowanych widoków list lub widoku domyślnego. 3. Możliwość wyświetlenia 10,20,30,50,100 zdarzeń na jednej stronie. 4. System umożliwia blokowanie na podstawie utworzonych reguł czarnej listy przy pomocy kategorii: a) Hash MD5 lub SHA256, b) Pełna ścieżka do aplikacji, c) Reguła połączenia. 5. Możliwość importu reguł czarnej listy dla hash, ścieżek do aplikacji oraz reguł połączeń z pliku CSV. 6. System musi oferować szeroki zakres filtrowania dodanych reguł blokowania minimum po nazwie pliku, hash pliku, typu hash, ścieżce, protokole porcie/zakresie portów, daty dodania. 7. Możliwość wygenerowania i wyeksportowania listy incydentów do pliku .csv.
Komputery z monitorami– 50 zestawów / szt.	
Komputer	
Obudowa	Typu Small Form Factor (SFF), umożliwiająca montaż minimum dwóch dysków, w tym jednego dysku HDD o rozmiarze 3,5”. Wbudowany głośnik multimedialny. Obudowa trwale oznaczona nazwą producenta i modelem komputera.
Chipset	Dostosowany do zaoferowanego procesora
Płyta główna	Zaprojektowana i wyprodukowana przez producenta komputera, trwale oznaczona nazwą producenta komputera (na etapie produkcji). Płyta główna wyposażona w min. 2 złącza M.2 z czego 1 dedykowane dla dysku SSD PCIe. Płyta główna wyposażona w min. 2 sloty pamięci RAM DDR5.
Procesor	Procesor klasy x86, zaprojektowany do pracy w komputerach stacjonarnych, o wydajności nie niższej niż procesor Intel Core i5-13400 lub równoważny według punktacji w teście Passmark CPU Mark opublikowanej na stronie- http://www.cpubenchmark.net/. Na potwierdzenie spełnienia wymagań wykonawca załącza do oferty wydruk lub zrzut ekranu ze strony www.cpubenchmark.net przedstawiający wynik

Załącznik nr 2.5 do SWZ

	testu zaoferowanego procesora, pochodzący z okresu pomiędzy datą publikacji dokumentacji zamówienia a terminem składania ofert**.** Wymaga się wydruku w formie PDF lub pliku graficznego, umożliwiający weryfikację daty pozyskania oraz źródła informacji. Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu.
Pamięć operacyjna	Min. 16GB DDR5, Maksymalna ilość obsługiwanej pamięci RAM min. 64GB, 2 sloty na pamięć RAM, w tym 1 slot wolny.
Dysk twardy	Min. 512GB SSD M.2 PCIe 4.0, zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii.
Karta graficzna	Karta graficzna zintegrowana z procesorem.
Audio	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition.
Sieć	Karta sieciowa LAN obsługująca prędkości 10/100/1000. Wbudowana karta sieci bezprzewodowej, pracująca w standardzie WIFI 6E Bluetooth min. 5.3.
Napęd optyczny	Urządzenie wyposażone we wbudowany napęd optyczny na jego przednim panelu. Nie dopuszcza się stosowania zewnętrznych napędów, podłączanych do urządzenia za pomocą złącza USB.
Porty/złącza	Z przodu obudowy min.: a) 1x USB 3.2 typu C, b) 2x USB 3.2 typu A, c) 1x złącze audio combo 3,5mm, d) 1x złącze mikrofonowe 3,5mm. Z tyłu obudowy min.: a) 4x USB 2.0 typu A, b) 1x HDMI 2.1, c) 1x DisplayPort 1.4, d) 1x VGA, e) RJ-45. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.
Klawiatura/mysz	Przewodowa USB: klawiatura w układzie US + mysz z rolką.
Zasilacz	Energooszczędny zasilacz o mocy min. 170W oraz sprawności na poziomie min. 85%.
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,

Załącznik nr 2.5 do SWZ

	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, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. 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: a) modelu komputera, b) numerze seryjnym, c) numerze inwentarzowym (AssetTag), d) wersji BIOS, e) dacie wydania BIOS, f) zainstalowanym procesorze wraz z taktowaniem, g) zainstalowanej pamięci RAM wraz z taktowaniem, h) dyskach podłączonych do złącz M.2 oraz SATA. Administrator z poziomu BIOS musi mieć możliwość: a) wyłączenia portów USB, b) wyłączenia karty sieciowej, c) wyłączenia karty audio, d) wyłączenia funkcji Wake on LAN, e) wyłączenia wirtualizacji, f) wyłączenia modułu TPM, g) ustawienia hasła: administratora, Power-On, h) wyboru trybu uruchomienia komputera po utracie zasilania, i) ustawienia trybu wyłączenia komputera w stan niskiego poboru energii, j) zdefiniowania sekwencji bootowania, k) załadowania optymalnych ustawień BIOS bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.
System	Zaimplementowany w UEFI BIOS system diagnostyczny z graficznym

Załącznik nr 2.5 do SWZ

Diagnostyczny	interfejsem użytkownika dostępny z poziomu szybkiego menu boot umożliwiający jednoczesne przetestowanie w celu wykrycia błędów zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. Działający nawet w przypadku uszkodzenia dysku twardego. System obsługiwany za pomocą myszy lub klawiatury, umożliwiający wykonanie minimum następujących czynności diagnostycznych: 1. Wykonanie testu komponentów w zakresie przyspieszonym lub rozszerzonym z możliwością wyboru algorytmów testowania oraz liczby cykli testowych do przeprowadzenia. System diagnostyczny powinien umożliwiać wykonanie testu następujących komponentów: a) pamięci ram, b) procesora, c) pamięci masowej, d) płyty głównej. 2. Identyfikację jednostki i jej komponentów w następującym zakresie: a) urządzenie (producent, model, numer seryjny), b) bios (wersja oraz data wydania), c) procesor (nazwa, taktowanie, ilości pamięci L1, L2, L3, liczba rdzeni), d) pamięć ram (ilość zainstalowanej pamięci ram, producent oraz numer seryjny), e) dysk twardy (producent, model, numer seryjny, pojemność), f) płyta główna (liczba złącz USB, liczba złącz PCI).
Bezpieczeństwo	• Złącze typu Kensington Security Slot, • Sprzętowy moduł TPM 2.0 (dTPM 2.0) z certyfikacją TCG, • Czujnik otwarcia obudowy.
Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji.
Oprogramowanie	Dedykowane oprogramowanie producenta sprzętu umożliwiające automatyczną weryfikację i instalację sterowników oraz oprogramowania użytkowego producenta, w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralna bazą sterowników i oprogramowania użytkowego producenta, sprawdzać dostępne aktualizacje i zapewniać ich zbiorczą instalację.
Gwarancja	Min. 36 miesięcy gwarancji producenta komputera w trybie na miejscu u Zamawiającego (on-site). Komunikacja ze wsparciem technicznym w godzinach 9:00-16:00 powinna odbywać się w języku polskim. Komputer musi być wyprodukowany zgodnie z normą ISO-9001, ISO-14001, ISO-50001 lub równoważnymi. Komputer musi posiadać certyfikat TCO min. 9.0 lub równoważny oraz deklarację zgodności CE. Komputer musi spełniać kryteria środowiskowe, w tym zgodności z

	dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Naprawa urządzeń musi być realizowana przez producenta komputera lub autoryzowany przez producenta serwis zgodnie z systemem ISO 9001 lub równoważnym. Dedykowany portal techniczny producenta komputera, wyposażony w funkcję automatycznej identyfikacji urządzenia, umożliwiający Zamawiającemu uzyskanie informacji w zakresie co najmniej: • fabrycznej konfiguracji urządzenia, • rodzaju gwarancji, • dacie wygaśnięcia gwarancji, • aktualizacjach. Zaawansowana diagnostyka urządzenia i oprogramowania dostępna na stronie producenta komputera.
Monitor	
Typ ekranu	Ekran ciekłokrystaliczny z aktywną matrycą IPS min. 23.8”
Rozmiar plamki (maksymalnie)	0,275 mm x 0,275 mm
Jasność	250 cd/m2
Kontrast	1300:1
Kąty widzenia (pion/poziom)	178/178 stopni
Czas reakcji matrycy (maksymalnie)	4ms (gray to gray) w trybie „typical”
Rozdzielczość maksymalna	1920 x 1080 przy 100Hz
Częstotliwość odświeżania poziomego	30 – 115kHz
Częstotliwość odświeżania pionowego	50 – 100Hz
Nachylenie monitora	W zakresie 25 stopni
Powłoka powierzchni ekranu	Antyodblaskowa
Podświetlenie	System podświetlenia W-LED
Zużycie energii	Typowo 16W, czuwanie mniej niż 0,6W
Waga bez podstawy	Maksymalnie 2,6kg
Waga z podstawą	Maksymalnie 3,0kg
Złącze	1x VGA, 1x HDMI (v1.4), 1x Audio in

	1x Audio out
Głośniki	Wbudowane min. 2W x 2
Gwarancja	Min. 36 miesięcy
Inne	VESA 100mmx100mm

Opis równoważności certyfikatów

1. Certyfikat ISO 9001 – System Zarządzania Jakością

Certyfikat równoważny wobec ISO 9001 powinien potwierdzać wdrożenie i utrzymywanie systemu zarządzania jakością w organizacji, zapewniającego zgodność z zasadami i wymaganiami normy ISO 9001:2015 lub równoważnej.
Parametry równoważności:

1. Zakres systemu
   System zarządzania jakością musi obejmować wszystkie procesy istotne z punktu widzenia realizacji przedmiotu zamówienia, w tym planowanie, realizację usług/produktów, nadzór nad dostawcami, monitorowanie jakości oraz doskonalenie.
2. Zarządzanie procesowe
   Certyfikat równoważny musi potwierdzać, że organizacja stosuje podejście procesowe obejmujące:
   a. identyfikację i mapowanie procesów,
   b. określenie ich wzajemnych powiązań i kryteriów skuteczności,
   c. monitorowanie i doskonalenie procesów w oparciu o dane pomiarowe.
3. Zarządzanie ryzykiem i szansami
   System powinien zawierać procedury identyfikacji, oceny i reagowania na ryzyka i szanse
4. Nadzór nad jakością wyrobów i usług
   Certyfikat równoważny musi potwierdzać istnienie procedur zapewniających:
   a. kontrolę jakości,
   b. weryfikację i walidację procesów,
   c. postępowanie z niezgodnościami i działaniami korygującymi.
5. Zarządzanie zasobami i kompetencjami personelu System musi obejmować wymagania w zakresie kwalifikacji, szkoleń i oceny kompetencji pracowników.
6. Ciągłe doskonalenie
   Certyfikat równoważny musi potwierdzać funkcjonowanie mechanizmów ciągłego doskonalenia, przeglądów zarządzania oraz monitorowania satysfakcji klienta.
7. Weryfikacja i audyty
   Certyfikat musi być:
   a. ważny i aktywny,
   b. wydany przez niezależną, akredytowaną jednostkę certyfikującą,
   c. podlegający okresowym audytom nadzoru (co najmniej raz w roku).

2. Certyfikat ISO 14001 – System Zarządzania Środowiskowego

Certyfikat równoważny wobec ISO 14001 powinien potwierdzać wdrożenie i utrzymywanie systemu zarządzania środowiskowego zgodnego z wymaganiami ISO 14001:2015 lub równoważnej.
Parametry równoważności:

1. Polityka środowiskowa i zobowiązanie kierownictwa
   System musi zapewniać istnienie zatwierdzonej polityki środowiskowej obejmującej zobowiązanie do:
   a. ochrony środowiska (w tym zapobiegania zanieczyszczeniom),
   b. spełniania wymagań prawnych i innych,
   c. ciągłego doskonalenia.
2. Identyfikacja aspektów środowiskowych
   Certyfikat równoważny musi potwierdzać, że organizacja:
   a. identyfikuje aspekty środowiskowe swoich działań, produktów i usług,
   b. ocenia ich znaczenie,
   c. ustanawia kontrolę operacyjną w celu ograniczenia wpływu.
3. Zgodność z przepisami prawnymi
   System musi obejmować mechanizmy identyfikacji i oceny zgodności z obowiązującymi przepisami środowiskowymi oraz działania korygujące w przypadku niezgodności.
4. Cele i programy środowiskowe
   Certyfikat równoważny powinien obejmować wymaganie ustanawiania, monitorowania i przeglądu celów środowiskowych oraz programów ich realizacji.
5. Monitorowanie i pomiary
   System musi przewidywać regularne pomiary wpływu działalności na środowisko (emisje, odpady, zużycie energii, wody, surowców itp.) oraz raportowanie wyników.
6. Komunikacja i świadomość
7. Certyfikat równoważny musi obejmować działania dotyczące:
   a. komunikacji wewnętrznej i zewnętrznej w zakresie środowiska,
   b. szkoleń i podnoszenia świadomości ekologicznej personelu.
8. Audyty i przeglądy
   Certyfikat musi być:
   a. ważny i aktywny,
   b. wydany przez niezależną, akredytowaną jednostkę certyfikującą,
   c. podlegający regularnym audytom zewnętrznym,
   d. obejmować ciągłe doskonalenie wyników środowiskowych.

3. Certyfikat ISO 50001 – System Zarządzania Energią

Certyfikat równoważny wobec ISO 50001 powinien potwierdzać wdrożenie i utrzymywanie systemu zarządzania energią zgodnego z wymaganiami normy ISO 50001:2018 lub innego standardu zapewniającego równoważny poziom zarządzania efektywnością energetyczną, monitorowania zużycia energii i ciągłego doskonalenia wyników energetycznych.
Parametry równoważności:

1. Zakres i kontekst systemu

System zarządzania energią musi obejmować wszystkie procesy, obiekty, instalacje i urządzenia mające istotny wpływ na zużycie energii w zakresie działalności związanej z realizacją przedmiotu zamówienia.
Certyfikat równoważny powinien potwierdzać, że organizacja:

- określiła granice i zakres systemu zarządzania energią,
- uwzględniła czynniki zewnętrzne i wewnętrzne wpływające na wyniki energetyczne,

- zidentyfikowała strony zainteresowane oraz ich wymagania w zakresie efektywności energetycznej.

2. Polityka energetyczna

Certyfikat równoważny musi potwierdzać, że organizacja ustanowiła i utrzymuje politykę energetyczną, która:

- zobowiązuje do ciągłego doskonalenia efektywności energetycznej,
- gwarantuje spełnianie wymagań prawnych i innych zobowiązań dotyczących użytkowania i zużycia energii,
- zapewnia dostępność informacji i zasobów niezbędnych do osiągnięcia celów energetycznych.

3. Planowanie energetyczne

System równoważny musi obejmować formalny proces planowania energetycznego zgodny z zasadami ISO 50001, w tym:

- identyfikację i ocenę aspektów energetycznych,
- określenie bazowej linii energetycznej (EnB) i wskaźników efektywności energetycznej (EnPI),
- analizę danych dotyczących zużycia energii,
- określenie celów, zadań i planów działania w zakresie poprawy efektywności energetycznej.

4. Wdrożenie i eksploatacja systemu

Certyfikat równoważny musi potwierdzać, że organizacja:

- wdraża środki kontroli operacyjnej i technologicznej mające wpływ na efektywność energetyczną,
- zapewnia właściwe utrzymanie urządzeń energetycznych,
- zarządza projektami inwestycyjnymi i zakupami z uwzględnieniem kryteriów efektywności energetycznej,
- prowadzi szkolenia i podnosi świadomość energetyczną pracowników.

System powinien obejmować także wymagania dotyczące projektowania i nabywania urządzeń, usług lub systemów wpływających na zużycie energii.

5. Monitorowanie, pomiary i analiza danych

Certyfikat równoważny musi obejmować obowiązek prowadzenia ciągłego monitoringu i analizy danych energetycznych, w tym:

- pomiarów zużycia energii na poziomie procesów, obiektów lub urządzeń,
- analizy trendów i odchyleń od bazowych wskaźników,
- stosowania mierników EnPI do oceny postępów,
- raportowania wyników energetycznych i działań doskonalących.

6. Ocena zgodności i audyty

System musi przewidywać:

- regularne audyty wewnętrzne systemu zarządzania energią,
- ocenę zgodności z wymaganiami prawnymi i normatywnymi,
- przeglądy zarządzania z udziałem najwyższego kierownictwa, w celu oceny skuteczności systemu i podejmowania działań korygujących.

7. Certyfikacja i weryfikacja niezależna

Certyfikat równoważny wobec ISO 50001 musi być:

- aktualny i ważny na dzień składania oferty,
- wydany przez niezależną jednostkę certyfikującą, akredytowaną w ramach uznanych międzynarodowych systemów akredytacji (np. PCA, UKAS, DAkkS, IAF, EA lub podobny),
- podlegający regularnym audytom nadzoru (co najmniej raz w roku),
- obejmujący zakres działalności odpowiadający przedmiotowi zamówienia,
- potwierdzający, że system zarządzania energią jest wdrożony, utrzymywany i stale doskonalony.

8. Równoważność względem ISO 50001

Za równoważny uznaje się system zarządzania energią, który:

- zapewnia systemowe podejście do poprawy efektywności energetycznej,
- obejmuje planowanie, wdrażanie, monitorowanie, ocenę oraz doskonalenie wyników energetycznych,
- zawiera procedury nadzoru, dokumentacji, audytów i przeglądów zarządzania,
- prowadzi do mierzalnych efektów w zakresie ograniczenia zużycia energii i zwiększenia efektywności energetycznej,
- jest zweryfikowany przez niezależny, kompetentny organ certyfikujący.

4. Certyfikat TCO

W zakresie produkcji:

- Potwierdzenie niezależnej organizacji certyfikacyjnej o charakterze i zasięgu międzynarodowym, że proces produkcji oferowanego sprzętu przebiega w bezpiecznych warunkach, a w szczególności nie wystawia pracowników na działanie niekorzystnych substancji chemicznych.
- Potwierdzenie niezależnej organizacji certyfikacyjnej o charakterze i zasięgu międzynarodowym o przestrzeganiu w stosunku do wszystkich osób zaangażowanych w produkcję praw człowieka oraz praw dziecka.
- Producent musi posiadać certyfikat ISO 14001 lub równoważną na proces produkcji oraz serwisowania sprzętu.

W zakresie bezpieczeństwa użytkownika końcowego:

- Certyfikat niezależnej organizacji certyfikacyjnej o charakterze i zasięgu międzynarodowym potwierdzający, że oferowany sprzęt jest w pełni bezpieczny dla użytkownika końcowego, a w szczególności zabezpiecza go przed porażeniem prądem elektrycznym.
- Potwierdzenie niezależnej organizacji o charakterze i zasięgu międzynarodowym, że oferowany sprzęt nie emituje szkodliwego promieniowania elektromagnetycznego – dotyczy komputerów stacjonarnych, komputerów All-In-One oraz ekranów komputerów przenośnych.

W zakresie wydajności oraz kosztów użytkowania sprzętu:

- Certyfikat efektywności energetycznej przyznany przez niezależną organizację certyfikacyjną o charakterze i zasięgu międzynarodowym potwierdzający całkowity koszt użytkowania (TCO - Total Cost of Ownership) sprzętu – szczególnie w zakresie zużycia energii elektrycznej.
- Wykonane przez niezależną organizację certyfikacyjną o charakterze i zasięgu międzynarodowym badanie emisji hałasu oferowanego sprzętu - dotyczy komputerów stacjonarnych, komputerów All-In-One oraz komputerów przenośnych.

W zakresie obsługi i przedłużenia cyklu przydatności:

- Funkcja umożliwiająca łatwe i bezpowrotne usunięcie wrażliwych danych w przypadku utylizacji, rozwiązanie sprzętowe, działające również w przypadku uszkodzenia lub braku systemu operacyjnego na dysku - dotyczy komputerów stacjonarnych, komputerów All-In-One oraz komputerów przenośnych.
- Oświadczenie producenta o zapewnieniu dostępności w cyklu życia produktu części zamiennych oraz eksploatacyjnych.

W zakresie bezpieczeństwa środowiska naturalnego:

- Badanie niezależnej organizacji certyfikacyjnej o charakterze i zasięgu międzynarodowym potwierdzające, że oferowane produkty nie zawierają kadmu, rtęci, ołowiu, sześciowartościowego chromu oraz innych uznanych za niebezpieczne substancji.

W zakresie recyklingu:

- Oświadczenie producenta o prowadzeniu programu utylizacji sprzętu uszkodzonego lub po zakończeniu cyklu życia sprzętu.

Dokumentacja równoważna do TCO Certifted		
Wszystkie normy, certyfikaty i standardy sporządzone przez niezależne, akredytowane jednostki na terenie Polski lub Unii Europejskiej (jeżeli dotyczy) lub normy równoważne		
Zakres	**Norma, Standard, Certyfikat**	**Uwagi**
Dla podmiotu będącego producentem/fabryki	**PN-EN ISO 9001:2015**	System Zarządzania Jakością
	PN-EN ISO 14001:2015	System Zarządzania Środowiskowego
	PN-ISO 45001:2018	System Zarządzania Bezpieczeństwem i Higieną Pracy
	PN-EN ISO/IEC 27001:2017	System Zarządzania Bezpieczeństwem Informacji
	PN-ISO 37001:2017	System Zarządzania działaniami antykorupcyjnymi
	PN-EN ISO 50001:2018	System Zarządzania Energią, Zarządzanie energią i efektywnością energetyczną w przedsiębiorstwie
	IEEE 1680.1 - 2018	Standard IEEE dla oceny odpowiedzialności środowiskowej i społecznej komputerów i wyświetlaczy W zakresie dla producenta/fabryki – w zakresie odpowiedzialności społecznej i w zakresie ochrony środowiska przy projektowaniu sprzętu

		komputerowego
Dla produktu	**PN-EN ISO 14024:2018**	Etykiety i deklaracje środowiskowe -- Etykietowanie środowiskowe I typu. Zasady i procedury.
	PN-EN ISO 7779:2019	Akustyka - Pomiar hałasu rozprzestrzeniającego się w powietrzu, wytwarzanego przez urządzenia informatyczne i telekomunikacyjne Norma w zakresie akustyki oraz prowadzenia pomiarów głośności urządzeń
	ISO 9296:2017	Akustyka - Deklarowane wartości emisji hałasu urządzeń informatycznych i telekomunikacyjnych. Norma dotycząca metodologii określania wartości uśrednionych poziomów głośności dla partii sprzętów teleinformatycznych
	PN-EN ISO 3741:2011	Akustyka -- Wyznaczanie poziomów mocy akustycznej i poziomów energii akustycznej źródeł hałasu na podstawie pomiarów ciśnienia akustycznego -- Metody dokładne w komorach pogłosowych Norma w zakresie akustyki – określanie poziomów mocy dźwięku oraz energii dźwiękowej.
	PN-EN ISO 3744:2011	Akustyka -- Wyznaczanie poziomów mocy akustycznej i poziomów energii akustycznej źródeł hałasu na podstawie pomiarów ciśnienia akustycznego. Metody techniczne stosowane w warunkach zbliżonych do pola swobodnego nad płaszczyzną odbijającą dźwięk. Metodyka pomiarowo obliczeniowa w zakresie wyznaczania poziomu mocy akustycznej i ciśnienia akustycznego
	PN-EN ISO 3745:2012/A1:2017-07	Akustyka -- Wyznaczanie poziomów mocy akustycznej i poziomów energii akustycznej źródeł hałasu na podstawie pomiarów ciśnienia akustycznego. Metody dokładne w komorach bezechowych i w komorach bezechowych z odbijającą podłogą
	PN-EN ISO 11469:2016 wg. ISO 1043	Tworzywa sztuczne -- Identyfikacja rodzaju tworzywa i znakowanie wyrobów z tworzyw sztucznych
	ISO/EIC 28360-1:2018	Informatyka - Sprzęt biurowy - Oznaczanie wskaźników emisji chemicznej ze sprzętu elektronicznego - Część 1: Materiały eksploatacyjne

	PN-EN IEC 61249-2-45:2018	Materiały na płytki drukowane i inne struktury wzajemnych połączeń -- Część 2-45: Wzmocnione materiały podłoża z pokryciem i bez pokrycia -- Płyty z bezhalogenowej żywicy epoksydowej, o wzmocnieniu nietkanym/tkanym ze szkła typu E, foliowane miedzią, o przewodności cieplnej (1,0 W/mK) i określonej palności (pionowa próba palności), do lutowania bezołowiowego Norma w zakresie wytwarzania laminatów drukowanych, bezhalogenowych oraz bez wykorzystania związków ołowiu
	PN-EN IEC 63000:2019	Dokumentacja techniczna do oceny produktów elektrycznych i elektronicznych w odniesieniu do ograniczenia substancji niebezpiecznych Norma w zakresie tworzenia oraz prowadzenia dokumentacji technicznej do oceny produktów elektrycznych i elektronicznych w odniesieniu do ograniczenia substancji niebezpiecznych
	Badania zgodności z Dyrektywami EMC i LVD przez podmiot akredytowany wg PN-EN ISO/IEC 17025:2018	Badanie kompatybilności elektromagnetycznej urządzeń elektronicznych i elektrycznych przeprowadzone przez akredytowane laboratorium
	Dyrektywa RoHS w sprawie ograniczenia stosowania niektórych niebezpiecznych substancji w sprzęcie elektrycznym i elektronicznym	Deklaracja w zakresie spełnienia wymogów dyrektywy ROHS dotycząca ograniczania substancji niebezpiecznych w produktach elektronicznych