Załącznik numer 6

Cześć 1 : Serwer wraz z oprogramowaniem : w ilości 2 sztuk

Parametr	Wymagania
Obudowa	Obudowa Rack o wysokości max 2U bez slotów na dyski twarde Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, pozwalający jednoznacznie stwierdzić, czy system działa poprawnie i pokazujący podstawowe stany działania serwera w tym adres IP karty zarządzającej Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	Płyta główna z możliwością zainstalowania minimum jednego procesora. Możliwość obsługi procesorów 128 rdzeniowych Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. Na płycie głównej powinno znajdować się minimum 12 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do min. 3TB pamięci RAM.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych
Procesor	Zainstalowany jeden procesor, min. 16-rdzeniowy, min. 4.1GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 221 w teście SPECrate2017_int_base w konfiguracji jedno procesorowej, dostępnym na stronie www.spec.org.
RAM	Minimum 256GB DDR5 RDIMM 5600MT/s, w modułach o pojemności 64GB
Kontroler RAID	Brak sprzętowego kontrolera dyskowego
Dyski twarde	Brak zainstalowanych dysków twardych Zainstalowane w dedykowanym slocie dwa dyski M.2 NVMe o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1.
Gniazda PCI	Cztery sloty PCIe w tym jeden min. Gen 5.
Interfejsy sieciowe/FC/SAS	~~Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT~~ ~~Wbudowane 2 karty sieciowe, każda z 2 interfejsami sieciowymi 10/25Gb Ethernet w standardzie SFP28.~~

	~~Dodatkowa karta sieciowa z 2 interfejsami 100GB Ethernet w standardzie QSFP56 z obsługą RoCE v1/v2.~~ Wbudowane min. 2 interfejsy sieciowe 1 Gb Ethernet w standardzie Base-T. Dodatkowe 2 karty sieciowe, każda z 2 interfejsami sieciowymi 10/25Gb Ethernet w standardzie SFP28. Dodatkowa karta sieciowa z 2 interfejsami 100GB Ethernet w standardzie QSFP56 z obsługą RoCE v1/v2.
Wbudowane porty	4 porty USB w tym min: 1 port USB 3.0 z tyłu obudowy, 1 port micro USB z przodu obudowy 2 port VGA z czego jeden z przodu obudowy Możliwość rozbudowy o port RS232
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1080
Wentylatory	Redundantne
Zasilacze	Redundantne, Hot-Plug min. 1100W klasy Titanium
Elementy montażowe	Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych
Bezpieczeństwo	Zatrzask górnej pokrywy oraz blokada na ramce panelu zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. Moduł TPM 2.0 Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).

Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego, karta zarządzająca, posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: zdalny dostęp do graficznego interfejsu Web karty zarządzającej; zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; możliwość podmontowania zdalnych wirtualnych napędów; wirtualną konsolę z dostępem do myszy, klawiatury; wsparcie dla IPv6; wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; integracja z Active Directory; możliwość obsługi przez dwóch administratorów jednocześnie; wsparcie dla automatycznej rejestracji DNS wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności o: Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej Przesyłanie danych telemetrycznych w czasie rzeczywistym Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze Automatyczna rejestracja certyfikatów (ACE)
Oprogramowanie do zarządzania	Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych integracja z Active Directory Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram Szczegółowy opis wykrytych systemów oraz ich komponentów Możliwość eksportu raportu do CSV, HTML, XLS, PDF Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. Grupowanie urządzeń w oparciu o kryteria użytkownika Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji

	Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach Szybki podgląd stanu środowiska Podsumowanie stanu dla każdego urządzenia Szczegółowy status urządzenia/elementu/komponentu Generowanie alertów przy zmianie stanu urządzenia. Filtry raportów umożliwiające podgląd najważniejszych zdarzeń Integracja z service desk producenta dostarczonej platformy sprzętowej Możliwość przejęcia zdalnego pulpitu Możliwość podmontowania wirtualnego napędu Kreator umożliwiający dostosowanie akcji dla wybranych alertów Możliwość importu plików MIB Przesyłanie alertów „as-is" do innych konsol firm trzecich Możliwość definiowania ról administratorów Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. Zdalne uruchamianie diagnostyki serwera. Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Oprogramowanie do monitorowania	Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności: Monitoring: ilość podłączonych oraz rozłączonych systemów

	stan podłączonych urządzeń informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia informacje o statusie gwarancji dla poszczególnych urządzeń informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. Monitoring parametrów serwerów z informacją o minimum: Obciążeniu procesora Zużyciu pamięci RAM Temperaturze procesorów Temperaturze powietrza wlotowego Zużyciu prądu Zmianach w fizycznej konfiguracji serwera Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. Monitoring parametrów pamięci masowych z informacją o minimum: Opóźnieniach IOPS Przepustowości Utylizacji kontrolerów Pojemność całkowita i dostępna Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów. Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata Informacje o poziomie redukcji danych Informacje o statusie replikacji oraz snapshotów

	Monitoring parametrów przełączników sieciowych z informacją o minimum: Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny Stanie komponentów: zasilacze, wentylatory Podłączonych hostach Ilości i statusu portów Utylizacji procesora Utylizacji poszczególnych portów Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. Aktualizacja firmware możliwość aktualizcji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania możliwość aktualizcji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania możliwość aktualizcji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania możliwość aktualizcji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania możliwość aktualizcji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania Raporty Możliwość generowania raportów dla serwerów zawierających informację o: Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej Średnim obciążeniu: procesorów, pamięci RAM, IO, Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji Generowanie raportów do plików CSV i PDF Cyberbezpieczeństwo Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. Wspierane urządzenia

	Urządzenie Producenta dostarczane w ramach postępowania Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) Wirtualny asystent Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; Możliwość rozszerzenia funkcjonalności Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. Inne Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 Serwer musi posiadać deklaracja CE. Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku – **Wykonawca złoży dokument potwierdzający spełnianie wymogu.** Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022, Windows Server 2025.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 5 lat.

	Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu.

	Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.
System operacyjny	Licencje na serwerowy system operacyjny muszą uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i nielimitowanej liczbie wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. Dodatkowo musi pozwalać na wykorzystanie tej licencji w usłudze hostowanej platformy producenta serwerowego systemu operacyjnego. Możliwość wykorzystania nielimitowanej liczby rdzenie logicznych procesorów oraz co najmniej 24 TB pamięci RAM w środowisku fizycznym. Możliwość wykorzystywania 64 procesorów wirtualnych oraz minimum 1TB pamięci RAM i dysku o pojemności minimum 64TB przez każdy wirtualny serwerowy system operacyjny. Możliwość budowania klastrów składających się z 64 węzłów. Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. Ochrona firmware przed atakami poprzez izolację hypervisora technologią Dynamic Root of Trust of Measurement (DRTM). Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Wbudowane wsparcie instalacji i pracy na wolumenach, które: • pozwalają na zmianę rozmiaru w czasie pracy systemu, • umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, • umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, • umożliwiają zdefiniowanie list kontroli dostępu (ACL).

	Wbudowany asystent aktualizacji obejmujący możliwość upgrade z trzech ostatnich wersji systemu. Narzędzie wiersza poleceń, które umożliwia użytkownikom monitorowanie i rozwiązywanie problemów z wydajnością systemu w czasie rzeczywistym, pozwalające dynamicznie instrumentować zarówno jądro, jak i kod w przestrzeni użytkownika bez konieczności modyfikowania samego kodu. Wbudowana możliwość zakładania kont w systemie: • Microsoft Entra ID • Microsoft account • Work or school account. Rozbudowane schematy Active Directory obejmujące sch89.ldf, sch90.ldf i sch91.ldf. Poziom funkcjonalności domeny i lasu dostosowany rozmiaru strony bazy danych 32k, odwzorowywany na wartość DomainLevel 10 i ForestLevel 10 dla instalacji nienadzorowanych. Wystąpienia kontrolerów domeny i usług LDS w usłudze AD zezwalają protokołowi LDAP na dodawanie, wyszukiwanie i modyfikowanie operacji obejmujących atrybuty poufne tylko wtedy, gdy połączenie jest szyfrowane. Narzędzia wspierające tworzenie klastra hiperkonwergentnego (łączącego magazyn i zasoby obliczeniowe w węzłach klastra). Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. Możliwość wykorzystania standardu http/2. Wbudowana obsługa TLS 1.3 włączona jako ustawienie standardowe. Możliwość przechowywania wrażliwych danych i kluczy pod ochroną TPM 2.0. Izolacja kernela od pozostałych komponentów systemu w oparciu zabezpieczenia bazujące na wirtualizacji (VBS)

	chroniąca przed metodami ataków wykorzystujących podatności używane przy „kopaniu" kryptowalut. Dostępność usługi DNS-over-HTTPS (DoH) szyfrujących zapytania DNS przy użyciu HTTPS. Dostępność usługi Server Message Block (SMB) z szyfrowaniem AES-256 (AES-256-GCM and AES-256-CCM), automatycznie wykorzystywanych przy połączeniach z urządzeniami wspierającymi te metody. Szyfrowanie komunikacji i wspólnych zasobów wewnątrz klastra niezawodnościowego. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. Wsparcie dla technologii Azure Arc pozwalające na traktowanie serwera zainstalowanego we własnym centrum przetwarzania jako zarządzalnego zasobu Azure. Dostępne dwa rodzaje graficznego interfejsu użytkownika: • Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, • Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. Zlokalizowane w języku polskim, co najmniej następujące elementy: • menu, • przeglądarka internetowa, • pomoc, • komunikaty systemowe. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. Mechanizmy logowania w oparciu o: • Login i hasło, • Karty z certyfikatami (smartcard), • Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), • PIN zdefiniowany dla urządzenia, • Rozpoznawanie twarzy.

	Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji. Podstawowe usługi sieciowe DHCP oraz DNS wspierający DNSSEC, Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1. Zdalna dystrybucja oprogramowania na stacje robocze.

	Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: Dystrybucję certyfikatów poprzez http Konsolidację CA dla wielu lasów domeny, Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. Szyfrowanie plików i folderów. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). Szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. Serwis udostępniania stron WWW. Wsparcie dla protokołu IP w wersji 6 (IPv6), Wsparcie dla algorytmów Suite B (RFC 4869), Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. Możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mające wsparcie dla: Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,

	Obsługi ramek typu jumbo frames dla maszyn wirtualnych. Obsługi 4-KB sektorów dysków Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) Możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego. Możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów. Wsparcie dla rozwiązania dla rozwiązań kontenerowych dla aplikacji zgodnych z Kubernetes... Możliwość wykorzystywania aplikacji kontenerowych wymagających wykorzystania Azure Active Directory bez dołączania hosta kontenerów do domeny. Wsparcie migracji zasobów na dyskach do Azure. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). Mechanizmy deduplikacji i kompresji na wolumenach do 64 TB. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. Mechanizm konfiguracji połączenia VPN do platformy Azure. Wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.

	Mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.
Licencje / Ilość	Proxmox VE Community Subscription 1 CPU/year lub równoważnej, zapewniającej pełną kompatybilność i współpracę z istniejącą infrastrukturą serwerową Zamawiającego, opartą na Proxmox VE Cluster

Cześć 2 : Licencja do zapory antyspamowej

Parametr	Wymagania
Wymagania ogólne	Roczna licencja FortiCare oraz ATP dla Fortimail VM-01 SN: FEVM01TM24001326
	Licencje muszą pochodzić od oficjalnego polskiego dystrybutora
Licencje / Ilość	Zamawiający wymaga dostarczenia ww. produkt w ilości 1 sztuki

Cześć 3 : Licencja do zapory sieciowej

Parametr	Wymagania
Wymagania ogólne	Roczna licencja UTP Bundle dla dwóch urządzeń FortiGate 121G SN: FG121GTK24000360 SN: FG121GTK24000061
	Licencje muszą pochodzić od oficjalnego polskiego dystrybutora
Licencje / Ilość	Zamawiający wymaga dostarczenia ww. produkt w ilości 2 sztuk (po jednej dla każdego urządzenia)

Cześć 4 : Przedłużenie licencji dla Veeam Data Platform Essentials

Parametr	Wymagania
Wymagania ogólne	Przedłużenie obecnych licencji o 1 rok ID: #03501343 ID: #02918247
	Licencje muszą pochodzić od oficjalnego polskiego dystrybutora
Licencje / Ilość	Zamawiający wymaga dostarczenia ww. produkt w ilości 2 sztuk (po jednej dla każdej licencji)

Cześć 5 : Przedłużenie gwarancji i wsparcia technicznego dla macierzy NetAPP E2824

Parametr	Wymagania
Wymagania ogólne	Przedłużenie obecnie trwającej gwarancji oraz wsparcia technicznego producenta o 2 lata SN : 952052001969
	Licencje muszą pochodzić od oficjalnego polskiego dystrybutora
Licencje / Ilość	Zamawiający wymaga dostarczenia ww. produktu w ilości 1 sztuki

Cześć 6 : Oprogramowanie typu – skaner podatności

Parametr	Wymagania
Wymagania ogólne	1. Rozwiązanie typu vulnerability manager musi być dostępne w wersji chmurowej (jako SaaS). 2. Rozwiązanie w wersji chmurowej musi posiadać swoje centrum danych (data center) na terenie Unii Europejskiej. 3. Centralna konsola zarządzania musi posiadać możliwość uruchomienia dodatkowego uwierzytelnienia użytkowników, za pomocą MFA/2FA wysyłanych w postaci wiadomości SMS 4. Rozwiązanie musi posiadać możliwość integracji z systemami ticketowymi: Jira, TopDesk i ServiceNow. 5. Rozwiązanie musi posiadać możliwość wysyłania powiadomień do następujących systemów: Slack, Microsoft Teams i Webhooks. 6. Administrator w centralnej konsoli zarządzania musi posiadać możliwość dodania dodatkowych użytkowników zarządzających. 7. Rozwiązanie musi posiadać możliwość dodania dodatkowych zestawów uprawnień (ról), które mogą być przypisane do użytkowników systemu. 8. Rozwiązanie musi posiadać możliwość zarządzania systemem przy użyciu interfejsu API.
Skanowanie usług chmurowych	1. Rozwiązanie musi posiadać możliwość wykrywania i raportowania błędnej konfiguracji usług chmurowych Amazon Web Services (AWS), Microsoft Azure oraz Google Cloud. 2. Rozwiązanie musi posiadać możliwość dodawania nowych profili skanowania usług chmurowych. 3. Administrator musi posiadać możliwość uruchomienia zadania skanowania usługi chmurowej jednorazowo, lub z harmonogramem.
Monitorowanie serwerów pocztowych i stron internetowych	1. Rozwiązanie musi posiadać mechanizm weryfikacji powiązany z rejestrami typu „black list" synchronizowanymi z serwerami pocztowymi i stronami internetowymi.

Menadżer podatności i panel główny	1. Platforma zarządzania podatnościami musi być w stanie zapewnić funkcje pulpitu nawigacyjnego (i konfigurowalne) z następującymi widżetami: a. wyniki skanowania podatności sieci według ważności (z opcjami wykresu: słupkowy i kołowy) b. wyniki skanowania podatności aplikacji internetowych według ważności (z opcjami wykresu: słupkowy i kołowy) c. otwarte zgłoszenia według ważności (z opcjami wykresu: słupkowy i kołowy) d. top 10 wyników skanowania sieci (dostępna opcja ustawienia celu zasobu jako wszystkich lub wybranych adresów IP/tagów) e. 10 największych podatności w aplikacjach sieciowych (dostępna opcja ustawienia celu zasobu jako wszystkie lub wybrane aplikacje sieciowe/etykiety) f. zgodność z OWASP (z opcjami wykresów: słupkowy i kołowy oraz dostępną opcją ustawienia dla wszystkich lub wybranych aplikacji internetowych) g. ostatnie skanowania h. nadchodzące skanowania i. ostatnie 10 raportów j. liczba podatności w zabezpieczeniach w czasie (dostępna opcja ustawienia celu zasobu jako wszystkich lub wybranych aplikacji IPS/web/tagów wraz z ustawieniem czasu, aby ustawić czas trwania i interwał) k. ocena wyników kampanii phishingowych l. ciągłe monitorowanie alertów (dostępna opcja ustawienia okresu na dzień/tydzień 2. Platforma zarządzania podatnościami musi mieć możliwość sortowania, grupowania i priorytetyzacji podatności a. możliwość tworzenia wielu zakładek w celu filtrowania następujących kryteriów: b. według stanu: wszystkie, nie ignorowane/wyłączone i ignorowane/wyłączone c. według typu: host i aplikacja internetowa d. według statusu: nowy, aktywny, ponownie otwarty, naprawiony e. według ważności: informacja, niski, średni, wysoki, krytyczny f. według tagów (opcja uwzględnienia/wykluczenia tagu) g. według pierwszego i ostatniego wykrycia h. według kategorii: podatności w skanowaniu sieci i podatności w aplikacjach internetowych i. możliwość filtrowania listy podatności według podatności lub aplikacji internetowych/hosta j. możliwość tworzenia raportów bezpośrednio z menedżera podatności poprzez wybranie jednej lub więcej podatności k. możliwość dalszego administrowania/zarządzania listą luk w zabezpieczeniach za pomocą następujących funkcji: l. co ignorować: wyłącz tę podatność dla wszystkich hostów/aplikacji internetowych i ignoruj tę podatność m. powód ignorowania: fałszywie dodatni, ryzyko zaakceptowane, nieistotny

	n. opcja ustawienia czasu wygaśnięcia dla ignorowanych podatności o. możliwość tworzenia notatek do celów uwag i notatek, które pojawią się w raporcie po jego wygenerowaniu p. możliwość tworzenia czatu konwersacyjnego do celów współpracy między użytkownikami q. opcja wyświetlania następujących informacji na temat podatności: • wpływ • rozwiązanie • podsumowanie • wgląd • wykrywanie • odniesienie • łatki • możliwość utworzenia zgłoszenia bezpośrednio ze wskazanych luk w zabezpieczeniach • środki zaradcze 3. Platforma zapewnia wbudowany system ticketowy dla procesu naprawczego. 4. Możliwość dostarczania informacji o zgłoszeniach, takich jak: a. numerowanie ich w celu łatwego śledzenia i powiadamiania za pośrednictwem poczty elektronicznej b. możliwość podawania i aktualizowania statusu zgłoszenia, takiego jak: otwarte, zamknięte lub rozwiązane c. możliwość podania nazwy powiązanej podatności w zabezpieczeniach wraz z jej zasobami d. możliwość podania wagi podatności w zabezpieczeniach zarejestrowanego zgłoszenia e. możliwość przypisania do wyznaczonego właściciela i terminu f. możliwość tworzenia wielu zakładek do utrzymywania i zarządzania zgłoszeniami zgodnie z poniższymi zasadami: • status • typ zasobu • kategoria usługi • tagi • termin kategoria skanowania sieci i aplikacji internetowych • Istotność • system operacyjny • porty • właściciel g. możliwość zapewnienia proaktywnej obsługi zgłoszeń. 5. Rozwiązanie musi posiadać możliwość ciągłego monitorowania oraz szybkiego i łatwego ustawiania w profilu monitorowania zmian za pomocą powiadomień i alarmów. 6. W menedżerze podatności musi istnieć możliwość utworzenia własnego widoku podatności zawierającego

	13. Możliwość tworzenia skryptów co najmniej w C# i PowerShell. 14. Funkcja automatycznego nanoszenia na przetwarzany dokument podpisu cyfrowego przy wykorzystaniu certyfikatu. 15. Funkcja kompresji plików w celu zmniejszenia ich rozmiaru.
Licencje / Ilość	Dostawa dostarczy licencje stałe (perpetual), nieprzenoszalne do dyspozycji w zakresie posiadanej ilości. Wymagana edycja Government dedykowana dla sektora publicznego, z pełną zgodnością z wymaganiami bezpieczeństwa i regulacjami rządowymi jak RODO, NIS2. Zgodność systemu z regulacją WCAG oraz normą EN 301549. Dostawca zobowiązany jest przedstawić wyniki testu wykonanego przez niezależną organizację. System ma pozwolić na podłączenie do systemu 10 szt. urządzeń wielofunkcyjnych bez stosowania zewnętrznych terminali. Wsparcie i maintenance: Obowiązkowe 3 letnie wsparcie dla każdej licencji, z możliwością przedłużenia. Wsparcie obejmuje aktualizacje oprogramowania, poprawki bezpieczeństwa i helpdesk dedykowany dla edycji Government. Dostawca dostarczy czytnik podłączany na USB lub RS-232 obsługujący standardy RFID, NFC, BLE w ilości 10 sztuk Dostawca odpowiada za prawidłowe wdrożenie i szkolenie Zgodność i dokumentacja: Dostawca zobowiązany dostarczyć pełną dokumentację licencyjną (EULA w języku polskim/angielskim) oraz potwierdzenie liczby urządzeń (lista z numerami seryjnymi). Brak sublicencji lub OEM – wyłącznie oryginalne licencje producenta.

Zgodność z wymaganiami dal przeciwdziałania wykluczeniu technologicznemu dla osób z niepełnosprawnościami (WCAG)	1. Zgodność systemu z regulacją WCAG oraz normą EN 301549. Dostawca zobowiązany jest przedstawić wyniki testu wykonanego przez niezależną organizację. 2. Obsługa dedykowanej klawiatury adaptacyjnej lub jednoręcznej 3. Interfejs w dedykowanej czytelnej formie teksu 4. Obsługa czytników ekranu – konwersja tekstu na dźwięk 5. Funkcja obsługi poprzez ustny wskaźnik 6. Funkcja rozpoznawania mowy 7. Szablon kolorów interfejsu webowego – wysoki kontrast
Okołounijne przepisy na rzecz wysokiego cyberbezpieczeństwa NIS 2	1. Zarządzanie prawami użytkowników 2. Reagowanie i rejestrowanie incydentów 3. Raportowanie incydentów 4. Bezpieczne uwierzytelnianie dwuskładnikowe 5. Przydzielanie i usuwanie dostępu dla użytkownika 6. Dzienniki w czasie rzeczywistym oraz dzienniki audytu
Współpraca z systemem elektronicznego zarządzania dokumentacją NASK EZD RP	1. System zarządzania wydrukiem i urządzeniami musi posiadać integrację z systemem NASK EZD RP. 2. W ramach integracji system ma pozwolić na automatyczne przetwarzanie korespondencji przychodzącej w zakresie rejestracji korespondencji przychodzącej oraz skanowania dokumentacji użytkownika. 3. W przypadku dokumentacji użytkownika rozwiązanie ma umożliwić wprowadzenie nazwy dla skanowanych dokumentów. 4. Rozwiązanie musi realizować funkcje skanowania w jednym stosie (jeden cykl skanowania) dla korespondencji przychodzącej oraz dokumentacji użytkownika.
Funkcje OCR	1. Możliwość pobierania dokumentu z Hot Folderu, poczty e-mail, serwera FTP. 2. Wsparcie dla nielimitowanej ilości Hot Folderów. 3. Funkcja OCR do formatów co najmniej doc, docx, xls, xlsx, RTF, PDF przeszukiwalny, PNG,BMP, JPEG, TIFF, XPS 4. Funkcja podziału dokumentu poprzez puste strony lub co określoną ilość stron. 5. Funkcja czytania kodów kreskowych 1D i 2D. 6. Funkcja nanoszenia kodów kreskowych na dokument. 7. Możliwość przetworzenia OCR nielimitowanej ilości stron bez limitów miesięcznych/rocznych. 8. Wsparcie dla OCR dla języka polskiego. 9. Funkcja obróbki obrazu w zakresie co najmniej: usuwania pustych stron, usuwania białych miejsc, rotacji obrazu, prostowania obrazu, wygładzania obrazu, usuwania linii, usuwania zaczernień po dziurkaczu. 10. Możliwość wysłania przetworzonego dokumentu/danych do systemu plików, na adres e-mail, WebDAV, FTP, baz danych, SharePoint. 11. Możliwość nanoszenia komentarzy na dokument. 12. Funkcja powiadamiania o statusie pracy.

	6. Możliwość generowania bezpośrednio raportów do formatów PDF, CSV, XLSX, XML, ODS. 7. Możliwość wykorzystania wbudowanych szablonów raportów jak i funkcja kreatora raportów. 8. Możliwość nadawania uprawnień do raportu dla użytkownika lub użytkowników. 9. Możliwość tworzenia harmonogramu dla automatycznego generowania i dystrybucji raportów. 10. Możliwość generowania raportów ilościowych jak i wartościowych. 11. Możliwość tworzenia cenników w postaci kosztu wydruku jednej strony dla funkcji drukowania, kopiowania i skanowania. 12. Możliwość tworzenia cenników dla papieru dla formatu A4 i A3. 13. Możliwość nakładania filtrów na raporty w celu doprecyzowania prezentowanych danych. 14. Możliwość kopiowania/klonowania tj. zapisywania już gotowych raportów jako nowy/szablon w celu przyśpieszenia modyfikacji, np.: zamawiający posiada raporty cykliczne, który zawiera obszerny wykaz użytkowników z całej organizacji i musi dokonać pojedynczych korekt bez konieczności modyfikowania lub przygotowywania pozostałych elementów raportu.
Zgodność z rozporządzeniem o ochronie danych osobowych	1. Funkcja automatycznego usuwania pracy z urządzenia zaraz po jego wydrukowaniu. 2. Funkcja anonimizacji danych użytkownika – prawo do bycia zapomnianym. 3. Funkcja automatycznego usuwania pracy z urządzenia w przypadku jej przerwania. 4. Szyfrowana komunikacja pomiędzy komponentami systemu a urządzeniem drukującym. 5. Szyfrowana funkcja drukowania i skanowania w schemacie End to End. 6. Funkcja nanoszenia znaku wodnego w postaci tekstu, kodu kreskowego. Możliwość wybory miejsca na dokumencie, w którym ma być naniesiony znak wodny, możliwość wyboru rozmiaru znaku wodnego oraz przeźroczystości. Możliwość wyboru jakie informacje mają być zawarte w znaku wodnym. Do wyboru: nazwa użytkownika, data, nazwa kolejki, nazwa pracy, nazwa komputera. 7. Komunikat dla użytkownika kto jest administratorem danych osobowych w organizacji. 8. Podgląd dla użytkownika jakie dane osobowe są przetwarzane przez system.

	urządzenia. W przypadku dodania nowych przycisków bez ograniczeń co do ich liczby. Możliwość tworzenia folderów i przypisywania do nich przycisków. 8. Możliwość nadawania uprawnień do przycisków/procesów prezentowanych na panelu urządzenia dla użytkownika, grup użytkowników i urządzeń. 9. Funkcja generowania alertu w postaci wiadomości e-mail do wskazanych przez administratora osób w przypadku wystąpienia błędu podczas skanowania – błąd wysłała. 10. Możliwość nadania użytkownikom praw do zmiany parametrów pracy skanowanej bezpośrednio przy urządzeniu w zakresie co najmniej: rozdzielczość, kolor, format, duplex, skanowanie ciągłe, nasycenie bezpośrednio poprzez terminal aplikacyjny systemu. 11. Możliwość przegląda bezpośrednio na panelu urządzenia przez zalogowanego użytkownika folderów sieciowych, zasobów chmurowych w celu wskazania miejsca zapisu skanowanego dokumentu wraz z możliwością zmiany nazwy pliku. Administrator zarządza prawami dostępu użytkownika do funkcji. 12. Funkcja kopiowania dowodu osobistego na jednej stronie. 13. Funkcja pomijania pustych stron w procesie kopiowania
Raportowanie	1. Funkcja generowania raportów w podziale na: a) Użytkowników lub grupy użytkowników b) Lokalizacje c) Projekty d) Urządzenia e) Najbardziej aktywni użytkownicy f) Najbardziej obciążane urządzenia g) Alerty urządzeń 2. Możliwość generowania raportów środowiskowych. 3. Możliwość generowania raportów serwisowych bezpośrednio przez interfejs systemu druku bez konieczności zastosowania dodatkowych aplikacji i/lub narzędzi, zawierających informacje: a) Model urządzenia b) Nazwa usterki c) Data powstania d) Data zakończenia 4. Możliwość generowania raportu serwisowego z informacją o wymianie tonerów. Raport musi zamierać informacje co najmniej o: a) Nazwa drukarki b) Toner c) Data instalacji d) Data wymiany e) Ilość wydrukowanych stron 5. Możliwość generowania raportu serwisowego z podsumowaniem zdarzeń poprzez interfejs systemu druku zawierający co najmniej informacje o: nazwie zdarzenia, kodzie zdarzenia, częstotliwości wystąpienia.

Zarządzanie wydrukiem urządzenie mobilne	1. Możliwość zwolnienia wszystkich wydruków. 2. Możliwość dodania pracy do wydruku. 3. Funkcja zarządzania pracami oczekującymi na wydruk, ulubionymi lub już wydrukowanymi. 4. Możliwość dodawania prac do ulubionych. 5. Funkcja wyboru konkretnej pracy do wydruku. 6. Możliwość zmiany parametrów pracy co najmniej w zakresie simplex/duplex, tryb eko, tryb monochromatyczny, ilość kopii. 7. Możliwość odblokowania urządzenia drukującego. 8. Możliwość wygenerowania przez użytkownika kodu PIN. 9. Możliwość zgłoszenia przez użytkownika usterki urządzenia.
Zarządzanie skanowaniem	1. Możliwość skanowania dokumentów na co najmniej: a) E-mail zalogowanego użytkownika b) E-mail innego użytkownika c) Folder użytkownika d) FTP e) Możliwość określenia kilku miejsc dla skanowanego dokumentu w jednym procesie np. E-mail zalogowanego użytkownika i Folder użytkownika 2. Możliwość skanowania dokumentów do zasobu chmurowego co najmniej: OneDrive for Business, DropBox, Sharpoint Online, AWS. 3. Możliwość ograniczenia rozmiaru skanowanego dokumentu na e-mail zalogowanego użytkownika i zapisanie go na serwerze. Do użytkownika inicjującego proces skanowania zostanie wysłana wiadomość z zaszyfrowanym linkiem HTTPS do pobrania pracy z serwera. Administrator systemu może określić rozmiar pracy po przekroczeniu którego będzie ona zapisywana na serwerze do pobrania poprzez wysłany bezpieczny link HTTPS do użytkownika. 4. Możliwość dokończenia przerwanej pracy na innym urządzeniu poprzez oznaczenie zakresu stron do wydruku. 5. Możliwość personalizacji przycisków wyświetlanych na panelu dotykanym urządzenia pod względem realizowanych funkcji, układu, nazw, kolorów, przez administratora bezpośrednio przez interfejs webowy systemu. 6. Administrator poprzez panel webowy systemu musi posiadać możliwość modyfikacji przycisków wyświetlanych na panelu dotykowym urządzenia, dodawania nowych przycisków bez ograniczeń, przypisywania funkcji do przycisków, określania nazwy, uprawnień jak i lokalizacji przycisku na panelu urządzenia. 7. Administrator poprzez panel webowy systemy musi mieć możliwość dodawania, usuwania lub modyfikacji przycisków wyświetlanych na panelu dotykowym

	4. Możliwość przyjmowania prac do wydruku wysłanych przez pocztę elektroniczną. 5. Możliwość załadowania pracy do wydruku poprzez portal systemu dostępny dla użytkownika. 6. Możliwość przyjmowania prac w formatach: PCL 5,PCL 6, PostScript, Prescribe, PDF, XPS, JPEG, ESC/P. 7. Możliwość delegowania prac drukowanych do innych użytkowników systemu definiowana z poziomu administratora systemu. 8. Obsługa protokołów IPPS, LPR, RAW. 9. Możliwość zarządzania pracami bezpośrednio na panelu urządzenia w zakresie wybory pracy do wydruku, kasowania, dodawania do ulubionych. 10. Możliwość zmiany parametrów pracy bezpośrednio na urządzeniu w zakresie mono/kolor, simplex/duplex, ilość kopii, dziurkowanie, zszywanie – do wyboru: górny róg, dolny róg, broszura. 11. Możliwość włączenia lub wyłączenia wydruku pracy w kolorze na urządzeniu monochromatycznym. 12. Możliwość wstrzymania prac drukowanych na stacji roboczej do momentu ich odebrania na urządzeniu wielofunkcyjnym z wykorzystaniem wydruku podążającego. 13. Możliwość wydruku pracy w systemie druku poprzez załadowanie pliku do Hot Folderu, bezpośrednie wsparcia co najmniej dla formatów PDF, JPG, BMP, TIF, PNG, TXT. 14. Możliwość przegląda bezpośrednio na panelu urządzenia przez zalogowanego użytkownika katalogów lokalnych, sieciowych, zasobów chmurowych w celu wyboru pracy do wydruku i jej fizycznego wydrukowania. Administrator zarządza prawami dostępu użytkownika do funkcji. 15. W przypadku przerwania wydruku pracy w związku z np. brakiem tonera, brakiem papieru, zacięciem papieru, użytkownik ma mieć możliwość dokończenia jej wydruku na innym urządzenia od następnej strony bez konieczności ponownego zlecenia jej wydruku na stacji roboczej. 16. System musi posiadać możliwość automatycznej dystrybucji kolejek wydruków na stacje robocze użytkowników z ich personalizacją w obszarze domyślnej konfiguracji i przypisania do poszczególnych podsieci. 17. Funkcja pomijania pustych stron. 18. System musi pozwalać na integrację z urządzeniami drukującymi jednofunkcyjnymi bez stosowania zewnętrznych terminali. Obsługa wydruku podążającego oraz bezpiecznego ma odbywać się poprzez wbudowaną w urządzenie klawiaturę oraz wyświetlacz. W zakresie zarządzania koleją wydruku użytkownik ma mieć możliwość wybory kolejności drukowanych dokumentów oraz ich usuwania. Wszystkie czynności mają być dostępne poprzez wbudowany w drukarek wyświetlacz oraz klawiaturę.

	offline, odblokowania urządzenia i udostępnienia funkcji kopiowania, skanowania na USB i drukowania. 7. Możliwość ustawienia przez administratora czasu przechowywania poświadczeń użytkowników na urządzeniu. 8. Funkcja monitorowania zajętości dysku w lokalizacji gdzie są przechowywane prace. Możliwość ustawienia przez administratora wartości dla poziomu ostrzeżenia oraz poziomu krytycznego. W przypadku osiągniecia wartości poziomu krytycznego, system ma wygenerować powiadomienie mailowe do administratora. 9. Funkcja usuwania historii co najmniej dla zdarzeń: a) Prace starsze niż, b) Lokalne skany starsze niż, c) Historia starsza niż, d) Zarchiwizowane raporty starsze niż, 10. Funkcja archiwizacji prac drukowanych, kopiowanych i skanowanych. Możliwość podglądu zarchiwizowanego dokumentu.
Autentykacja użytkowników	1. Dostęp do funkcji urządzenia po uprzedniej pozytywnej weryfikacji użytkownika. 2. Funkcja bezpośredniej rejestracji karty zbliżeniowej przez użytkownika przy urządzeniu wielofunkcyjnym. 3. Możliwość włączenia lub wyłączenia funkcji rejestracji wielu kart zbliżeniowych dla jednego użytkownika. 4. Możliwość określenia czasu ważności dla karty zbliżeniowej, tzw. karta tymczasowa. 5. Jednoczesny dostęp do 3 form autoryzacji użytkownika: a) Karta zbliżeniowa b) Kod PIN c) Login i hasło 6. Możliwość włączenia dwuetapowej autoryzacji np. karta zbliżeniowa i kod PIN. 7. Funkcja logowania za pomocą kodu QR i urządzenia mobilnego. 8. Możliwość włączenia lub wyłączenia przez administratora funkcji logowania za pomocą QR. 9. Dostęp do nielimitowanej ilości terminali mobilnych dla systemów Android i iOS. 10. Możliwość rejestracji przez użytkownika nieznanej karty i powiązanie jej z kontem
Zarządzanie drukowaniem	1. Wsparcie dla drukowania z systemów klasy ERP, np. SAP z zachowaniem wydruku poufnego i podążającego. 2. Wsparcie dla drukowania z systemów Windows, Linux, Novell, iOS. 3. Możliwość drukowania dokumentów z urządzeń mobilnych np. poprzez Mopria, AirPrint wraz ze zliczaniem wydruków na użytkownika bez konieczności instalacji dodatkowych aplikacji na urządzeniu mobilnym.

	9. Funkcja generowania alertów w przypadku powstania usterki lub w przypadku konieczności wymiany komponentu po uzyskaniu jego wydajności. Alerty będą wysyłane w postaci wiadomości e-mail do wskazanych przez administratora odbiorców. 10. Funkcja automatycznego zgłaszania konieczności wymiany materiałów eksploatacyjnych. Możliwość określenia przez administratora systemu procentowego (%) poziomu, przy osiągnięciu którego zostanie wygenerowany alert i przesłany w postaci wiadomości e-mail do wskazanych przez administratora systemu odbiorców. 11. Funkcja automatycznego zamawiania materiałów eksploatacyjnych w przypadku osiągnięcia ich niskiego poziomu. 12. System musi posiadać funkcje generowania powiadomienia o przewidywanym terminie wymiany tonerów. Administrator ma możliwość określenia czasu w dniach, z jakim wyprzedzeniem system ma wygenerować powiadomienie o przewidywanym terminie wymiany tonerów. Jeśli określony przez administratora czas wynosi np. 10 dni , to system na podstawie analizy zużycia tonerów przez urządzenia, wygeneruje odpowiednie powiadomienie z 10-dniowym wyprzedzeniem zawierające informacje o urządzeniu oraz tonerze, którego dotyczy planowana wymiana. 13. Funkcja zarządzania alertami o zdarzeniach i automatyzacja zamawiania materiałów eksploatacyjnych dostępna bezpośrednio poprzez interfejs systemu druku bez potrzeby stosowania dodatkowych aplikacji i systemów. 14. Dostęp do stanu urządzeń w czasie rzeczywistym. 15. Możliwość zgłaszania usterki bezpośrednio na panelu dotykowym urządzenia poprzez wybór z listy zdefiniowanych opisów awarii wraz z możliwością dołączenia kopii strony, której awaria dotyczy. Zgłoszenie powinno być wysłane na wskazany adres e-mail i powinno zawierać co najmniej: nazwa urządzenia, numer seryjny, stan licznika, opis usterki wraz ze wskazaniem funkcji urządzenia, której usterka dotyczy, imię i nazwisko osoby zgłaszającej awarie, numer telefonu, adres e-mail.
Bezpieczeństwo	1. Szyfrowana komunikacja pomiędzy komponentami systemu. 2. Blokowanie dostępu do panelu urządzenia do momentu autoryzacji użytkownika. 3. Funkcja szyfrowania bazy danych. 4. Funkcja szyfrowania prac drukowanych i skanowanych. 5. Funkcja bezpiecznego dostarczania prac drukowanych i skanowanych do urządzenia i użytkownika. 6. W przypadku braku połączenia urządzenia wielofunkcyjnego z systemem możliwość logowania

	i) Licznik urządzenia j) Poziom materiałów eksploatacyjnych 8. Możliwość załadowania do systemu własnego logo przez Administratora w celu personalizacji interfejsu systemu i generowanych raportów oraz personalizacji terminala prezentowanego na urządzeniu wielofunkcyjnym. 9. Funkcja monitorowania wymian tonerów.
Zarządzanie użytkownikami	1. Współpraca z usługą katalogową MS Active Directory, eDirectory, Azure Active Directory, Open LDAP, Novell, Lotus Domino. 2. Funkcja pobierania informacji o użytkownikach z wybranych kontenerów i grup użytkowników. 3. Funkcja wsparcia dla wielu domen. 4. Funkcja tworzenia użytkowników lokalnych. 5. Funkcja importu użytkowników poprzez plik CSV. 6. Funkcja ręcznego lub automatycznego powiązywania aliasów do istniejących loginów. 7. Automatyczne generowanie kodu PIN dla nowo zarejestrowanych użytkowników. 8. Funkcja określenia złożoności hasła co najmniej dla: duża litera, mała litera, cyfra, znak specjalnych. 9. Funkcja określenia ilości nieudanych prób logowania, po których nastąpi zablokowanie konta użytkownika na określony przez administratora czas. 10. Funkcja limitu z możliwością konfiguracji dla użytkownika, członków grupy lub grup zliczania z określeniem okresu rozliczeniowego. Możliwość określenia limitu dla wydruków i kopii całkowitych, wydruków i kopii kolorowych, wydruków i kopii monochromatycznych oraz skanów. Możliwość określenia limitu zarówno w postaci wolumenu jaki wartości. 11. Możliwość rejestracji przez użytkownika nieznanej karty i powiązanie jej z kontem.
Zarządzanie urządzeniami	1. Funkcja zarządzania urządzeniami poprzez portal systemu (jeden interfejs). 2. Funkcja aktywacji i dezaktywacji urządzenia w systemie. 3. Funkcja automatycznej konfiguracji urządzenia w systemie. 4. Funkcja kreatora profili konfiguracji urządzeń co najmniej w zakresie: cennik wydruku, kopii, skanu, typ terminala aplikacyjnego, metoda logowania. Profil konfiguracji ma pozwolić na automatyczne skonfigurowanie urządzenia podłączonego do systemu wraz z instalacją terminala. 5. Funkcja zdalnej instalacji terminala na urządzeniu wielofunkcyjnym poprzez portal systemu. 6. Funkcja konfiguracji większej liczby urządzeń na podstawie przygotowanego szablonu. 7. Funkcja ręcznego dodania urządzenia do systemu. 8. Funkcja monitorowania stanu urządzeń.

	w urządzenie wielofunkcyjne panelem dotykowym bez stosowania zewnętrznych komponentów. 3. Możliwość tworzenia drzewiastej struktury projektów na potrzeby rozliczania prac. 4. Możliwość włączenia lub wyłączenia funkcji rozliczania projektów dla funkcji skanowania. 5. Możliwość obsługi lokalizacji bezserwerowych. 6. Współpraca systemu z Microsoft Exchange Online, Gmail, AmazonS3, Microsoft Universal Print 7. Możliwość integracji systemu z rozwiązaniami zewnętrznymi poprzez funkcję REST API. 8. Oferent musi przedstawić aktualne potwierdzenie od producenta systemy potwierdzające uprawnienia oferenta do świadczenia usług przedsprzedaży, sprzedaży, odsprzedaży, sublicencjonowania oraz świadczenia usług serwisowych i gwarancyjnych dla zaoferowanego systemu.
Zarządzenie systemem	1. Logowanie do portalu systemu poprzez przeglądarkę z wykorzystaniem mechanizmu SSO 2. Funkcja przydzielania różnych poziomów praw dostępu użytkownikom do webowego interfejsu systemu. 3. Funkcja podglądu logów poprzez interfejs systemu. 4. Funkcja tworzenia automatycznych harmonogramów dla: a) kopii zapasowej systemu, b) konserwacji systemu, c) wykrywania urządzeń, d) kontroli stanu systemu, e) raportów, f) synchronizacji użytkowników 5. Możliwość personalizacji pulpitu początkowego systemu, tzw. zarządzanie widżetami, w zakresie prezentowanych informacji, co najmniej dla: a) Najbardziej obciążane urządzenia b) Najbardziej aktywni użytkownicy c) Najbardziej aktywne grupy d) Informacja o licencjach e) Status konfiguracji systemu f) Urządzenia z problemem g) Podgląd graficzny stron za ostatnie 30 dni 6. Funkcja kontroli stanu systemu 7. Podgląd urządzeń podłączonych do systemu wraz z informacją co najmniej o: a) Status urządzenia b) Nazwa urządzenia c) Adres IP d) Lokalizacja e) Marka urządzenia f) Numer seryjny g) Typ usterki h) Status terminala (w przypadku gdy urządzenie jest wyposażone w terminal)

	(według podatności i hosta) z opcjami wglądu, podsumowania, wykrywania, odniesień i ograniczenia tekstu. 15. Filtrowanie: selektywne raportowanie podatności (pełne i niestandardowe) i wykluczenia, uwzględnione systemy operacyjne, filtry zasobów, filtry podatności. 16. Możliwość tworzenia "raportów skróconych" wysyłanych w formie podsumowania. Częstotliwość raportów można ustawić na: tygodniowe raporty skrócone i miesięczne raporty skrócone. Raporty są dostarczane kanałem e-mail.
Licencje / Ilość	Licencja musi obejmować skanowanie : - 100 aktywnych adresów IP, - 80 stacji roboczych - 1 webaplikacji - 10 skrzynek mailowych pod kątem phishingu Licencja musi zapewnić - wsparcie producenta, w tym bezpośredni kontakt z pomocą techniczną producenta za pomocą maila / ticketu oraz połączenia telefonicznego Zamawiający wymaga dostarczenia ww. produktu w ilości 1 sztuki Czas trwania licencji: 12 m-cy

Cześć 7 : Oprogramowanie do zarządzania wydrukiem

Parametr	Wymagania
Architektura	1. Obsługa instalacji w architekturze centralnej jak i rozproszonej. 2. Wsparcie dla instalacji w architekturze wysokiej dostępności. 3. Nielimitowana ilość monitorowanych urządzeń w nieograniczonej ilości lokalizacji. 4. Brak ograniczeń pod względem ilości użytkowników korzystających z systemu. 5. Możliwość instalacji na serwerach z systemem operacyjnym Windows Server 2012 lub nowszym. 6. Możliwość współpracy z bazą danych MS SQL lub wbudowaną bazą danych. 7. Swobodne dysponowanie licencjami w zakresie posiadanej ilości i przemieszczanie ich pomiędzy lokalizacjami.
Funkcje ogólne	1. Interfejs systemu w języku polskim lub angielskim administratora, w języku polskim dla użytkownika. 2. Współpraca systemu z co najmniej z 10 producentami urządzeń biurowych poprzez integrację z wbudowanym

	odfiltrowane dane zgodnie z konfiguracją administratora danych. 7. Rozwiązanie musi posiadać możliwość zignorowania wykrytych podatności na określony czas.
System raportujący	System raportujący musi zawierać następujące typy raportów: 1. Skanowanie sieci 2. Aplikacja sieciowa 3. Łatki 4. Środki zaradcze 5. Ocena phishingu e-mail 6. Porównanie (raport typu delta) 7. Zgodność 8. Raporty zgodności – musi być w stanie wygenerować następujący typ zgodności: a. ustawa Sarbanes-Oxley b. ustawa o przenośności i rozliczalności ubezpieczeń zdrowotnych c. OWASP Top 10 d. ustawa o ochronie danych osobowych e. ISO / IEC 27001 f. ogólne rozporządzenie o ochronie danych g. bezpieczeństwo sieci i informacji h. PCI DSS. 9. System powinien mieć możliwość dostarczania nowych niestandardowych raportów zgodności, które mogą być zalecane przez rząd, gdy ma to zastosowanie. 10. Rozwiązanie musi posiadać możliwość tworzenia i dostosowywania szablonów raportów sieciowych z następującymi opcjami: i. raport oparty na określonym czasie skanowania j. raport oparty na wszystkich bieżących informacjach o podatnościach k. raport trendów z historią podatności l. zawartość raportu: szczegóły raportu, przegląd podatności, podsumowanie podatności, lista podatności (według podatności i hosta) z opcjami wglądu, podsumowania, wykrywania, odniesień i ograniczenia tekstu m. sposób prezentacji raportu: podatności według ważności w czasie, podatności według statusu, podatności według ważności, 5 najbardziej narażonych kategorii n. filtrowanie: selektywne raportowanie podatności (pełne i niestandardowe) i wykluczenia, uwzględnione systemy operacyjne, filtry zasobów, filtry podatności. 11. Możliwość utworzenia i dostosowania szablonu raportu aplikacji internetowej. 12. Raport oparty na określonym czasie skanowania. 13. Raport oparty na wszystkich bieżących informacjach o podatnościach. 14. Zawartość raportu: szczegóły raportu, przegląd podatności, podsumowanie podatności, lista podatności