# Załącznik nr 3 do SWZ – Szczegółowy OPZ

**Postępowanie o udzielenie zamówienia: Zakup sprzętu i oprogramowania na potrzeby realizacji projektu: Poprawa poziomu Cyberbezpieczeństwa w Urzędzie Miejskim w Boguchwale**

**Opis przedmiotu zamówienia**

1. **Uwagi ogólne:**

Niniejszy dokument prócz zdefiniowania minimalnych wymagań dotyczących przedmiotu zamówienia, będzie również pełnił funkcje przedmiotowego środka dowodowego w rozumieniu ustawy Prawo zamówień publicznych z dnia 11.09.2019 r. (tekst jednolity Dz. U. z 2023 r. poz. 1605 z późniejszymi zmianami). W związku z powyższym Wykonawca zobowiązany jest do dokonania szczegółowej analizy załącznika pod kątem sformułowanych wymogów i wypełnienie stosownych kolumn tabel ujętych w części II i III załącznika (wymóg nie dotyczy cz. XVI Usługa instalacji i konfiguracji środowiska sieciowego w Urzędzie Miejskim w Boguchwale oraz w Centrum Usług Wspólnych). Następnie Wykonawca zobowiązany jest do dołączenia wypełnionego dokumentu do złożonej oferty.

W części II Wykonawca zobowiązany jest do podania oferowanego modelu lub wersji oraz producenta oferowanego asortymentu (w kolumnie 3).

W części III natomiast Wykonawca zobowiązany jest do odniesienia się do opisanego wymogu i wpisanie danych (w kolumnie 3), które będą miały za zadanie jednoznaczne potwierdzenie spełnienie danego wymogu. Wpisy ogólne typu: „zgodne z SWZ” nie będą traktowane przez Zamawiającego jako prawidłowe.

Zamówione urządzenia i oprogramowanie, mają być fabrycznie nowe, kompletne, nieużywane i pozbawione wad fizycznych i prawnych. Zamawiający wyklucza dostawę sprzętu używanego, poleasingowego, powystawowego, po zwrocie itp. Nie dopuszcza się zaoferowania sprzętu refurbished. Nie dopuszcza się modyfikacji na drodze Producent-Zamawiający. Zamawiający nie dopuszcza stosowania licencji używanej, przeniesionej z innego sprzętu oraz licencji typu refurbished. Nie dopuszcza się stosowania adapterów, przejściówek, ani innych urządzeń zewnętrznych w celu osiągnięcia wymaganych portów i funkcjonalności urządzeń. Wyjątek stanowi sytuacja, że dopuszczenie adapterów jest wyraźnie opisane w opisie pozycji przedmiotu zamówienia.

1. **Zestawienie Oferowanego sprzętu lub oprogramowania:**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Przedmiot zamówienia** | **Producent/ Model/Wersja** |
| *1* | *2* | *3* |
| 1. | Macierz, 2 szt. |  |
| 2. | Rozszerzenie funkcjonalności posiadanej macierzy Huawei OceanStore 2600 V5, 1 szt |  |
| 3. | Serwer wirtualizacyjny, 1 szt |  |
| 4. | Serwer dla Centrum Usług Wspólnych (CUW), 1 szt. |  |
| 5. | Switch zarządzalny, 2 szt. |  |
| 6. | Switch dla CUW, 1 szt. |  |
| 7. | Licencja UTM, 1 szt. |  |
| 8. | Pakiet oprogramowania antywirusowego dla CUW, liczba stanowisk: 10, 1 szt. |  |
| 9. | Pakiet oprogramowania z zakresu bezpieczeństwa danych –  licencja na 130 stanowisk, 1 szt |  |
| 10. | Deduplikator – urządzenie dla bezpiecznego składowania danych cyfrowych, 1 szt. |  |
| 11. | Zaawansowana ochrona stacji roboczych – rozbudowa obecnego systemu, 1 szt. |  |
| 12. | System do zarządzania infrastrukturą IT i zasobami ludzkimi –wymagania. System zawierający panel użytkownika dla administratora z możliwością zarządzania urządzeniami końcowymi w ilości 100 szt. |  |
| 13. | Aktualizacja posiadanego programu do backupu i archiwizacji komputerów w sieciach LAN, 1 szt. |  |
| 14. | Wsparcie posiadanego programu do backupu maszyn wirtualnych NAKIVO Backup & Replication Pro Essentials, 1 szt |  |
| 15. | Urządzenie UTM dla CUW, 1 szt |  |
| 16. | Usługa instalacji i konfiguracji środowiska sieciowego w Urzędzie Miejskim w Boguchwale oraz w Centrum Usług Wspólnych (CUW) | **NIE DOTYCZY** |

1. **Wymagane minimalne parametry i funkcjonalności.**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Charakterystyka (wymagania minimalne)** | **Opis oferowanej funkcjonalności lub parametru** |
| ***1*** | ***2*** | ***3*** |
| **I Macierz 2 szt.** | | |
| 1. | Urządzenie musi być przeznaczone do instalacji w szafie technicznej typu RACK 19”, dostarczone ze wszystkimi niezbędnymi komponentami do montażu. |  |
| 2. | Minimum dwa kontrolery pracujące w trybie Symmetrical Active-Active (SAN-only), to znaczy w trybie zapewniającym dostęp do wolumenów logicznych (LUN) utworzonych w macierzy, z wykorzystaniem wszystkich dostępnych ścieżek (path) i portów kontrolerów w trybie bez wymuszania preferowanej ścieżki dostępu oraz z zapewnieniem automatycznego równoważenia obciążenia (load balancing). Kontrolery muszą pozwalać na udostępnianie zasobów protokołem FC, iSCSI w zależności od zastosowanych kart komunikacyjnych. |  |
| 3. | Komunikacja pomiędzy parą kontrolerów (synchronizacja cache) macierzy musi wykorzystywać wewnętrzną, dedykowaną magistralę zapewniającą wysoką przepustowość i niskie opóźnienia; nie dopuszcza się w szczególności komunikacji z wykorzystaniem urządzeń aktywnych FC/Ethernet/Infiniband. |  |
| 4. | Zamawiający dopuszcza komunikację z wykorzystaniem urządzeń aktywnych przy klastrze wielu kontrolerów. Każdy z kontrolerów musi mieć możliwość jednoczesnej prezentacji (aktywny dostęp odczyt i zapis) wszystkich wolumenów utworzonych w logicznych ramach całego systemu dyskowego. |  |
| 5. | Urządzenie musi umożliwiać podniesienie wydajności i niezawodności poprzez rozbudowę do 2 par kontrolerów, tworzących jedną logiczną macierz dyskową. Rozbudowa musi być możliwa bez konieczności wymiany zaoferowanej pary kontrolerów na nowe. Za jedną logiczną macierz uznaje się rozwiązanie, w którym zarządzanie wszystkimi kontrolerami jest możliwe z jednego interfejsu GUI, CLI. Nie dopuszcza się rozwiązań opartych o wirtualizator. |  |
| 6. | Możliwość rozbudowy do co najmniej 4 par kontrolerów dyskowych tworzących jedna logiczną macierz, bez konieczności wymiany zaoferowanej pary kontrolerów. |  |
| 7. | Musi być skonstruowana wyłącznie do obsługi modułów pamięci SSD i w żadnej konfiguracji nie może obsługiwać przestrzeni danych użytkownika na dyskach obrotowych/ talerzowych. |  |
| 8. | Całkowita pojemność brutto (fizyczna) urządzenia (sumaryczna pojemność zainstalowanych dysków) musi wynosić minimum 40 TB i musi być zbudowana wyłącznie w oparciu o moduły pamięci SSD. Rozmiar pojedynczego modułu nie może być większy niż 4 TB. |  |
| 9. | Możliwość rozbudowy do co najmniej 70 sztuk oferowanego typu modułów pamięci, bez wymiany kontrolerów macierzowych oraz bez potrzeby zakupu dodatkowych licencji. (tylko poprzez dodawanie półek i modułów SSD). |  |
| 10. | Kontrolery łącznie muszą być wyposażone w procesory o sumarycznej ilości min. 48 rdzeni (ang.: core). Procesory w macierzy muszą obsługiwać protokół PCI Express Generacji 4. |  |
| 11. | Urządzenie zbudowane z dwóch kontrolerów musi być wyposażone w co najmniej 128 GB pamięci podręcznej cache obsługującej operacje odczytu i zapisu zbudowane w oparciu o wydajną pamięć RAM. Zamawiający nie dopuszcza możliwości zastosowania dysków SSD/NVMe lub kart pamięci FLASH jako rozszerzenia pamięci cache. Pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania poprzez funkcję zapisu zawartości pamięci cache na nieulotną pamięć lub posiadać podtrzymywanie bateryjne min. 48 godzin. |  |
| 12 | Możliwość definiowania dysków SPARE lub odpowiedniej zapasowej przestrzeni dyskowej. |  |
| 13. | Macierz musi posiadać minimum 12 portów 10Gb/s obsługujące protokół iSCSI. Jeśli korzystanie z któregoś z wyżej wymienionych portów wymaga zastosowania wkładek (np. SFP+), wymaga się ich dostarczenia wraz z urządzeniem. |  |
| 14. | Możliwość rozbudowy macierzy o minimum 8 portów 25Gb/s obsługujących protokół iSCSI w ramach zaoferowanej ilości kontrolerów oraz możliwość podłączania serwerów bezpośrednio do tych portów macierzy bez użycia przełączników. Możliwość rozbudowy o wskazane porty nie może ograniczać rozbudowy do wymaganej ilości modułów pamięci. |  |
| 15. | Urządzenie musi obsługiwać poziomy RAID5 i RAID6 (RAID z dystrybuowaną przestrzenią zapasową typu hot-spare) lub równoważne poziomy RAID zabezpieczające przed awarią dwóch dysków jednocześnie. |  |
| 16. | Macierz musi umożliwiać skonfigurowanie poziomu RAID zapewniającego odporność na jednoczesną awarię 3 dysków w grupie RAID. |  |
| 17. | Brak pojedynczego punktu awarii. Wszystkie krytyczne komponenty takie jak adaptery HBA, kontrolery dyskowe, pamięć, zasilacze i wentylatory muszą być zaprojektowane nadmiarowo: tak, aby awaria pojedynczego elementu nie wpływała na ciągłość dostępu do danych całego systemu. Komponenty te muszą być wymienialne w trakcie pracy. |  |
| 18. | Urządzenie musi cechować wsparcie dla zasilania z dwóch niezależnych źródeł prądu jednofazowego o napięciu 200-240V i częstotliwości 50-60Hz poprzez nadmiarowe zasilacze typu Hot-Swap. |  |
| 19. | Wymagana jest funkcjonalność tworzenia i prezentacji dysków logicznych (LUN) o pojemności większej niż zajmowana fizyczna przestrzeń dyskowych (ang. ThinProvisioning). Wymagana funkcjonalność zwrotu skasowanej przestrzeni dyskowej do puli zasobów wspólnych (ang. Space Reclamation). Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania. |  |
| 20. | Zarządzanie macierzą (wszystkimi kontrolerami) z poziomu pojedynczego interfejsu graficznego. Wymagane jest stałe monitorowanie stanu macierzy (w tym monitorowanie wydajności) oraz możliwość konfigurowania jej zasobów. Wymagana możliwość monitorowania stanu żywotności modułów SSD. Konsola graficzna musi być dostępna poprzez przeglądarkę internetową i być elementem systemu operacyjnego macierzy. Wymaga możliwość dostępu do danych wydajnościowych historycznych z poziomu GUI co najmniej 1 rok wstecz lub jako równoważne dostarczenie fizycznego serwera z oprogramowaniem umożlwiającym zbieranie i przeglądanie danych historycznych. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania. |  |
| 21. | Urządzenie musi umożliwiać utworzenie 800 kopii migawkowych (ang. snapshot) w trybie ROW (ang. Redirect on Write) dla pojedynczego wolumenu oraz minimum 2000 dla całej macierzy. Niedopuszczalne jest wykonywanie kopii w technologii COW (ang. Copy-on-Write). Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania. |  |
| 22. | Wymagana jest możliwość utworzenia harmonogramu snapshotów, które będą zabezpieczone przed modyfikacją oraz usunięciem przez wybrany okres czasu bez odpowiednich uprawnień celem przywrócenia danych w przypadku ataku ransomware. Musi być możliwość odtworzenia danych z dowolnej kopii (snapshot) wykonanej w ramach harmonogramu. Odtworzenie danych z jednej kopii nie może uniemożliwiać odtworzenia danych z innej kopii z innego punktu w czasie. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania. |  |
| 23. | Rozwiązanie musi umożliwiać hierarchiczne tworzenie kopii migawkowych (np. kopia z kopii z kopii). |  |
| 24. | Tworzenie na żądanie pełnej kopii danych typu klon w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Funkcjonalność ta musi umożliwiać synchronizację danych z woluminu źródłowego na docelowy oraz resynchronizację danych z woluminu docelowego na źródłowy np. w sytuacji uszkodzenia danych na woluminie źródłowym. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania. |  |
| 25. | Macierz musi mieć możliwość włączenia funkcjonalności deduplikacji i kompresji danych w trybie in-line, a ponadto musi ona umożliwiać:  - włączenie deduplikacji dla poszczególnych wolumenów,  -wyłączenie deduplikacji dla poszczególnych wolumenów na których wcześniej deduplikacja była włączona  -włączenie kompresji dla poszczególnych wolumenów,  -wyłączenie kompresji dla poszczególnych wolumenów na których wcześniej kompresja była włączona |  |
| 26. | Uruchomienia jednocześnie deduplikacji i kompresji dla dowolnego wolumenu |  |
| 27. | Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania**.** |  |
| 28. | Macierz musi umożliwiać uruchomienie mechanizmów zdalnej replikacji danych z innymi macierzami (ten sam model/rodzina modeli) - w trybie synchronicznym i asynchronicznym - po protokołach FC lub iSCSI bez konieczności stosowania zewnętrznych urządzeń konwersji wymienionych protokołów transmisji, główek typu serwer/wirtualizator, itp. Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania. |  |
| 29. | Model oferowanej macierzy musi wspierać rozwiązanie klastra „wysokiej dostępności” tj. zapewnienia wysokiej dostępności zasobów danych macierzy dla podłączonych platform software’owych i sprzętowych z wykorzystaniem synchronicznej replikacji danych po FC lub iSCSI pomiędzy minimum 2 macierzami. Pod użytym pojęciem „wysoka dostępność zasobów dyskowych” należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/ system operacyjny/ serwer) podłączonego do macierzy (macierz podstawowa) w przypadku wystąpienia awarii logicznego połączenia z tą macierzą bądź awarii samej macierzy, powodujących dla danego środowiska brak dostępu do zasobów macierzy podstawowej. Replikacja danych pomiędzy macierzami podstawową i zapasową, wykorzystanych w układzie „wysokiej dostępności”, musi wspierać klastrownie wybranych woluminów bez konieczności stosowania lustrzanej konfiguracji grup dyskowych pomiędzy macierzami podstawową i główną. Musi być możliwość dodawania woluminów objętych zabezpieczeniem w klastrze bez konieczności zatrzymywania replikacji. Funkcjonalność „wysokiej dostępności” musi pozwalać na automatyczne przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową w przypadku awarii macierzy podstawowej (tzw. automated failover). Funkcjonalność „wysokiej dostępności” musi pozwalać na ręczne (zaplanowane) przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową (tzw. manual failover). Funkcjonalność „wysokiej dostępności” musi pozwalać na minimum ręczne przełączanie obsługi środowisk produkcyjnych z macierzy zapasowej na podstawową po usunięciu awarii macierzy podstawowej (tzw. failback). Funkcjonalność „wysokiej dostępności” musi wspierać konfiguracje z macierzą zapasową zainstalowaną w innej fizycznej lokalizacji o ile nadal spełnione są warunki dla realizacji synchronicznej replikacji danych pomiędzy lokalizacjami.  Jeżeli do obsługi tej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania. |  |
| 30. | Macierz musi posiadać funkcjonalność zarządzania wydajnością, która dynamicznie przydziela zasoby macierzy w celu spełnienia określonych celów wydajnościowych aplikacji (QoS). Możliwość ustawiania priorytetów wydajności dla aplikacji w oparciu o zdefiniowane profile wolumenowe, dla wydajności w IOPS i przepustowości danych. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania. |  |
| 31. | Wsparcie dla mechanizmów dynamicznego przełączania zadań I/O pomiędzy kanałami w przypadku awarii jednego z nich (path failover). Wymagane jest wsparcie dla odpowiednich mechanizmów oferowanych przez producentów systemów operacyjnych: Windows, Vmware, Linux, których używa Zamawiający. |  |
| 32. | Macierz musi posiadać wsparcie dla wielościeżkowości dla systemów Windows Server 2016/2019/2022 Vmware 8.0, Vmware 7.0, CentOS, których używa Zamawiający. |  |
| 33. | Wymagane uaktualnianie firmware-u kontrolerów macierzy bez przerywania dostępu do danych. |  |
| 34. | Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta, a także musi być objęte serwisem producenta na terenie RP. |  |
| 35. | Macierz dyskowa musi zostać objęta minimum 2 letnim okresem gwarancji producenta z gwarantowanym czasem reakcji najpóźniej w następnym dniu roboczym od momentu zgłoszenia usterki. Zamawiający dopuszcza realizacje gwarancji przez autoryzowanego partnera serwisowego producenta. |  |
| 36. | Zgłoszenia usterek muszą być akceptowane zarówno drogą email (w ofercie należy podać dedykowany adres email do zgłoszeń serwisowych) jak również drogą telefoniczną (ogólnie dostępna linia telefoniczna, kontakt w języku polskim, linia telefoniczna w polskiej strefie numeracyjnej - telefon stacjonarny. Nie dopuszcza się numerów specjalnych, komórkowych, o podwyższonej płatności itp.). |  |
| 37. | Wymagane jest, aby gwarancja świadczona była z zachowaniem poniższych warunków:  - bezpłatna możliwość aktualizacje firmware;  - dostęp do bazy wiedzy producenta w zakresie dostarczanych urządzeń;  - dostęp do centrum pomocy technicznej producenta;  - otwieranie zgłoszeń serwisowych w przypadku podejrzenia możliwości błędu w oprogramowaniu/hardware;  - otrzymywanie poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z macierzą oraz oprogramowania wewnętrznego macierzy. |  |
| **II Rozszerzenie funkcjonalności posiadanej macierzy Huawei OceanStore 2600 V5,**  **1 szt** | | |
| 1. | Dostawa licencji Smart Series: SmartTier, SmartQoS, SmartPartition, SmartCache, SmartDedupe, SmartCompression, SmartEncryption.  Parametry równoważności:   * Automatyczne przenoszenie danych między warstwami pamięci na podstawie aktywności dla optymalizacji wydajności. * Zarządzanie priorytetami przepustowości dla aplikacji w celu zapewnienia odpowiedniej jakości usług dla kluczowych obciążeń. * Tworzenie logicznych partycji pamięci masowej z możliwością niezależnego zarządzania, co zwiększa bezpieczeństwo i elastyczność. * Buforowanie danych na szybszych dyskach w celu redukcji opóźnień i poprawy dostępu do często używanych danych. * Identyfikacja i eliminacja duplikatów, co pozwala na efektywniejsze wykorzystanie przestrzeni pamięci. * Kompresja danych w czasie rzeczywistym, umożliwiająca przechowywanie większej ilości informacji na mniejszej powierzchni dyskowej. * Szyfrowanie danych w celu zabezpieczenia ich przed nieautoryzowanym dostępem.   Licencje muszą zapewniać bezproblemową współpracę z posiadaną macierzą. |  |
| 2. | Wraz z licencjami wymagane jest dostarczenie wsparcia producenta na okres min. 2 lat. |  |
| **III Serwer wirtualizacyjny,**  **1 szt** | | |
| 1. | **Obudowa** | |
| 1.1 | * Obudowa Rack o wysokości max 1U * Obudowa wyposażone w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. * 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. |  |
| 2. | **Płyta główna** | |
| 2.1 | * Płyta główna z możliwością zainstalowania do dwóch procesorów. * Obsługa procesorów 32 rdzeniowych. * Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. * Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. * Płyta główna powinna obsługiwać do 1TB pamięci RAM. |  |
| 3. | **Chipset** | |
| 3.1 | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych. |  |
| 4. | **Procesor** | |
| 4.1 | Zainstalowane dwa procesory min. 16-rdzeniowe, min. 2.0GHz, klasy x86, dedykowane do pracy z zaoferowanym serwerem, umożliwiające osiągnięcie wyniku min. 280 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. |  |
| 5. | **RAM** | |
| 5.1 | Min.256GB DDR5 RDIMM 5600MT/s, |  |
| 6. | **Funkcjonalność pamięci RAM** | |
| 6.1 | * Demand Scrubing, * Patrol Scrubing, * Permanent Fault Detection |  |
| 7. | **Dyski twarde** | |
| 7.1 | Zainstalowane dwa dyski M.2 NVMe SSD o pojemności min. 480GB z możliwością konfiguracji RAID 1. |  |
| 8. | **Gniazda PCI** | |
| 8.1 | trzy sloty PCIe LP |  |
| 9. | **Interfejsy sieciowe/FC/SAS** | |
| 9.1 | * Wbudowane min. 6 interfejsów sieciowych 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) * Czteroportowa karta sieciowa 25Gb Ethernet SFP28 |  |
| 10. | **Wbudowane porty** | |
| 10.1 | * 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 |  |
| 11 | **Video** | |
| 11.1 | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200 |  |
| 12. | **Zasilacze** | |
| 12.1 | Redundantne, Hot-Plug min. 1100W klasy Titanium |  |
| 13. | **Elementy montażowe** | |
| 13.1 | Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych |  |
| 14. | **System operacyjny/dodatkowe oprogramowanie** | |
| 14.1 | Windows Server 2022 Standard wraz z nośnikiem CD/DVD – licencja dobrana tak, aby przy oferowanych procesorach umożliwić uruchomienie 2 maszyn wirtualnych lub równoważny, tj. obsługujący technologię COM, .NET, posiadający możliwości zarządzania komputerami oraz użytkownikami na poziomie funkcjonalności usługi katalogowej Active Directory kompatybilnej z używaną przez Zamawiającego, opartą o Windows Server 2022. |  |
| 15. | **Bezpieczeństwo** | |
| 15.1 | * Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. * 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). |  |
| 16. | **Karta Zarządzania** | |
| 16.1 | * Niezależna od zainstalowanego na serwerze systemu operacyjnego 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 dynamic 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) |  |
| 17. | **Oprogramowanie do zarządzania** | |
| 17.1 | * 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. |  |
| 18. | **Oprogramowanie do monitorowania** | |
| 18.1 | 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 |  |
| 19. | **Certyfikaty** | |
| 19.1 | * Serwer musi posiadać deklaracja CE. * 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 lub inne równoważne, tj.: Wykonawca musi potwierdzić, ze Oferowany serwer jest zatwierdzony do użytku z systemami operacyjnymi danego producenta oraz spełnia normy zgodności i gwarantuje bezproblemowe działanie i wsparcie techniczne dla używanych systemów operacyjnych. |  |
| 20. | **Dokumentacja użytkownika** | |
| 20.1 | * Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim. * Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |  |
| 21. | **Warunki gwarancji** | |
| 21.1 | * Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres min. 2 lat. * Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. * Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. * Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Naprawa w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. * Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. * Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta * 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.   + Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.   + 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. |  |
| **IV Serwer dla Centrum Usług Wspólnych (CUW), 1 szt.** | | |
| 1 | **Obudowa** | |
| 1.1 | * Obudowa Rack o wysokości max 1U * Obudowa wyposażone w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. * 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. |  |
| 2 | **Płyta główna** | |
| 2.1 | * Płyta główna z możliwością zainstalowania do dwóch procesorów. * Obsługa procesorów 32 rdzeniowych. * Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. * Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. * Płyta główna powinna obsługiwać do 1TB pamięci RAM. |  |
| 3. | **Chipset** | |
| 3.1 | * Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych. |  |
| 4 | **Procesor** | |
| 4.1 | * Zainstalowany jeden procesor min. 16-rdzeniowy, min. 2.0GHz, klasy x86, dedykowany do pracy z zaoferowanym serwerem, umożliwiający osiągnięcie wyniku min. 280 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. |  |
| 5. | **RAM** | |
| 5.1 | * 128GB DDR5 RDIMM 5600MT/s |  |
| 6. | **Funkcjonalność pamięci RAM** | |
| 6.1 | * Demand Scrubing, * Patrol Scrubing, * Permanent Fault Detection |  |
| 7. | **Dyski twarde**  **Kontroler** | |
| 7.1 | * Zainstalowane dwa dyski M.2 NVMe SSD o pojemności min. 480GB z możliwością konfiguracji RAID 1. * Zainstalowane cztery dyski HDD SAS 12Gbps 10krpm o pojemności min. 2.4TB * Kontroler RAID 0, 1, 5, 6, 10, 50, 60, min. 8GB cache |  |
| 8. | **Gniazda PCI** | |
| 8.1 | * trzy sloty PCIe LP |  |
| 9. | **Interfejsy sieciowe/FC/SAS** | |
| 9.1 | * Wbudowane min. 6 interfejsów sieciowych 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) * Dwuportowa karta sieciowa 25Gb Ethernet SFP28 |  |
| 10. | **Wbudowane porty** | |
| 10.1 | * 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 |  |
| 11. | **Video** | |
| 11.1 | * Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200 |  |
| 12. | **Zasilacze** | |
| 12.1 | * Redundantne, Hot-Plug min. 1100W klasy Titanium |  |
| 13. | **Elementy montażowe** | |
| 13.1 | * Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych |  |
| 14. | **System operacyjny/dodatkowe oprogramowanie** | |
| 14.1 | * Windows Server 2022 Standard wraz z nośnikiem CD/DVD – licencja dobrana tak, aby przy oferowanym procesorze umożliwić uruchomienie 2 maszyn wirtualnych., 10x licencja Windows Server 2022/2019 User CAL lub równoważny, tj. obsługujący technologię COM, .NET, posiadający możliwości zarządzania komputerami oraz użytkownikami na poziomie funkcjonalności usługi katalogowej Active Directory kompatybilnej z używaną przez Zamawiającego, opartą o Windows Server 2022. |  |
| 15. | **Bezpieczeństwo** | |
| 15.1 | * Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. * 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). |  |
| 16. | **Karta Zarządzania** | |
| 16.1 | * Niezależna od zainstalowanego na serwerze systemu operacyjnego 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 dynamic 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) |  |
| 17. | **Oprogramowanie do zarządzania** | |
| 17.1 | * 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. |  |
| 18. | **Oprogramowanie do monitorowania** | |
| 18.1 | 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 aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania * możliwość aktualizacji 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:   o Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz An-droid |  |
| 19. | **Certyfikaty** | |
| 19.1 | * Serwer musi posiadać deklaracja CE. * 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 lub inne równoważne, tj.: Serwer musi być zatwierdzony przez producenta systemów jako zgodny z wymienionymi wersjami systemu operacyjnego, oferując pełne wsparcie techniczne oraz zapewniając stabilną i wydajną pracę zgodnie ze standardami producenta. |  |
| 20. | **Dokumentacja użytkownika** | |
| 20.1 | * Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim. * Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |  |
| 21. | **Warunki gwarancji** | |
| 21.1 | * Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres min. 2 lat. * Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. * Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. * Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Naprawa powinna się rozpocząć w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. * Zamawiający wymaga od podmiotu realizującego serwis lub producenta że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. * Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta * 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.   + Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. |  |
| **V Switch zarządzalny,**  **2 szt.** | | |
| 1. | Zarządzalny przełącznik |  |
| 2. | Ilość portów 1Gb RJ45, min. 48 |  |
| 3. | Ilość portów 10Gb SFP+, min. 4 |  |
| 4. | Możliwość łączenia w stos co najmniej 8 urządzeń |  |
| 5. | Pamięć RAM min. 1 GB |  |
| 6. | Obsługa CLI/WEB/SNMP/SSH/LLDP/CDP/VLAN |  |
| 7. | Funkcjonalność QoS, LACP, Voice VLAN, DHCP, SSH, ACL, 802.1X, RADIUS, TACACS+, Jumbo frame, L3 routing statyczny, RIP, IPv4, IPv6 |  |
| 8. | Przepustowość min. 175Gbps |  |
| 9. | Prędkość przekazywania min. 130 Mpps |  |
| 10. | Gwarancja producenta min. 24 miesiące |  |
| **VI SWITCH dla CUW, 1 szt.** | | |
| 1. | Zarządzalny przełącznik |  |
| 2. | Ilość portów 1Gb RJ45, min. 24 |  |
| 3. | Ilość portów 10Gb SFP+, min. 4  Możliwość łączenia w stos co najmniej 8 urządzeń |  |
| 4. | Pamięć RAM min. 1GB |  |
| 5. | Obsługa CLI/WEB/SNMP/SSH/LLDP/CDP/VLAN |  |
| 6. | Funkcjonalność QoS, LACP, VLAN, DHCP, SSH, ACL, RADIUS, Jumbo frame, L3 routing statyczny, IPv4, IPv6, RIP, OSPF |  |
| 7. | Przepustowość min. 120Gbps |  |
| 8. | Prędkość przekazywania min. 90 Mpps |  |
| 9. | Gwarancja producenta min. 24 miesiące |  |
| **VII Licencja UTM, 1 szt** | | |
| 1. | **Przedłużenie posiadanej przez Zamawiającego licencji UTM (support Unified Threat Protection dla urządzenia Fortinet Fortigate FG100f SN: FG100FTK19018781) obejmującej aktualne usługi FortiCare support, IPS. Anivirus, web filtering, firmware and general updates)** lub inne równoważne tj. oferowana licencja musi zapewniać pełen zakres funkcji obejmujących wsparcie techniczne, ochronę przed zagrożeniami (IPS, antivirus), filtrowanie treści internetowych oraz bieżące aktualizacje oprogramowania i firmware’u, aby w pełni odpowiadać posiadanej licencji i zagwarantować nieprzerwaną ochronę oraz wsparcie dla posiadanego urządzenia Fortinet Fortigate FG100f. |  |
| 2. | Wymagany okres ważności supportu: 30.06.2026 |  |
| **VIII Pakiet oprogramowania antywirusowego dla CUW, 1 szt**  **liczba stanowisk: 10**  Dostawa pakietu oprogramowania o wymaganej poniżej funkcjonalności. | | |
| 1. | **Wymagany okres ważności licencji:** do 30.06.2026 |  |
| 2 | **Administracja zdalna w chmurze** | |
| 2.1 | * Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego. * Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW. * Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL. * Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. * Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. * Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM. * Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. * Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak. * Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta. * Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. * Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. * Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej. |  |
| 3 | **Ochrona stacji roboczych** | |
| 3.1 | * Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). * Rozwiązanie musi wspierać architekturę ARM64. * Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. * Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. * Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. * Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. * Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. * Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. * Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku. * Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). * Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. * Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. * Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. * Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia. * Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, * tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, * tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, * tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, * tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach. * Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. * Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. * Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. * Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). * Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. |  |
| 4. | **Ochrona serwera** | |
| 4.1 | * Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux. * Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. * Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. * Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS. * Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. * Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji. * Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. * Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. |  |
| 5. | **Dodatkowe wymagania dla ochrony serwerów Windows** | |
| 5.1 | * Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. * Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS). * Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. * Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. * Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. * Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. * Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych*.* * Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. * Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu. |  |
| 6 | **Dodatkowe wymagania dla ochrony serwerów Linux:** | |
| 6.1 | * Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. * Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. * Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon. * Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu. |  |
| 7. | **Ochrona urządzeń mobilnych opartych o system Android** | |
| 7.1 | * Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. * Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne. * Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). * Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM. * Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi: usunięcie zawartości urządzenia,   + przywrócenie urządzenie do ustawień fabrycznych,   + zablokowania urządzenia,   + uruchomienie sygnału dźwiękowego,   + lokalizację GPS. * Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. * Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: * nazwę aplikacji, * nazwę pakietu, * kategorię sklepu Google Play, * uprawnienia aplikacji, * pochodzenie aplikacji z nieznanego źródła. |  |
| **IX Pakiet oprogramowania z zakresu bezpieczeństwa danych, 1 szt**  **licencja na 130 stanowisk** | | |
| 1. | * Pakiet oprogramowania z zakresu bezpieczeństwa danych – rozbudowa posiadanej licencji ESET do wyższego pakietu ochronnego o większej funkcjonalności. |  |
| 2. | * Rozszerzenie funkcjonalności posiadanej przez Zamawiającego licencji ESET PROTECT Essential ON-PREM na 130 stanowisk (nr licencji 33B-TCR-HB3) do wymaganej funkcjonalności.   lub inne równoważne, tj.: Oferowane rozwiązanie musi zapewniać pełen zakres funkcji bezpieczeństwa i zarządzania równoważny lub wyższy względem posiadanej licencji ESET PROTECT Essential ON-PREM na 130 stanowisk, gwarantując rozbudowaną ochronę, centralne zarządzanie oraz bieżące wsparcie techniczne i gwarantować współprace z ww. obecnie używanymi rozwiązaniami. |  |
| 3. | * **Wymagany okres ważności licencji:**   **do 30.06.2026** |  |
| 4. | **Administracja zdalna w chmurze** | |
| 4.1 | Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.  Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.  Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.  Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.  Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.  Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.  Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.  Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.  Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.  Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.  Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.  Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej. |  |
| 5 | **Ochrona stacji roboczych** | |
| 5.1. | * Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11) obecnie używane u Zamawiającego.   Rozwiązanie musi wspierać architekturę ARM64.   * Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. * Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. * Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. * Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. * Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. * Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. * Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku. * Rozwiązanie musi integrować się z Intel Threat Detection Technology. * Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). * Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. * Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. * Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. * Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia * Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach. * Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux. * Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. * Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. * Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS. * Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. * Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji. * Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. * Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. |  |
| 6 | **Ochrona serwera** | |
| 6.1 | * Dodatkowe wymagania dla ochrony serwerów Windows: * Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. * Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS). * Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. * Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. * Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. * Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. * Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych*.* * Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. * Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu. * Dodatkowe wymagania dla ochrony serwerów Linux:   Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.  Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.  Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.  Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu |  |
| 7. | **Szyfrowanie** | |
| 7.1 | System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10 i Microsoft Windows 11.  System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).  Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.  Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI. |  |
| 8. | **Ochrona urządzeń mobilnych opartych o system Android** | |
| 8.1 | * Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. * Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne. * Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). * Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM. * Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi: usunięcie zawartości urządzenia,   + - * przywrócenie urządzenie do ustawień fabrycznych,       * zablokowania urządzenia,       * uruchomienie sygnału dźwiękowego,       * lokalizację GPS.       * Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.       * Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:       * nazwę aplikacji,       * nazwę pakietu,       * kategorię sklepu Google Play,       * uprawnienia aplikacji,       * pochodzenie aplikacji z nieznanego źródła. |  |
| 9. | **Sandbox w chmurze** | |
| 9.1 | * Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.   Rozwiązanie musi wykorzystywać do działania chmurę producenta.  Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.   * Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta. * Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek. * Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania. * Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów. * Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy. * Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione. * Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych. * Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo. * Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem: Czysty, Podejrzany, Bardzo podejrzany, Szkodliwy.   W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.  W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.  Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia. |  |
| 10. | **Moduł XDR** | |
| 10.1 | Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.  Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.  Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.  Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.  Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”.  Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.  Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.  Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.  Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.  Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.  Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.  Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.  W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.  W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.   * Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji |  |
| **X Deduplikator – urządzenie dla bezpiecznego składowania danych cyfrowych –**  **1 szt.** | | |
| 1 | **Obudowa** | |
| 1.1 | Obudowa do montażu w szafie rack 19” za pomocą dostarczonych dedykowanych elementów. |  |
| 2 | **Kontrolery** | |
| 2.1 | * Deduplikator musi być wyposażony w minimum 2 kontrolery pracujące w trybie active-passive lub active-active. * Deduplikator nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. * W przypadku awarii kontrolera wszystkie procesy musi przejąć drugi kontroler. |  |
| 3 | **Wymagana przestrzeń** | |
| 3.1 | * Deduplikator musi być skonstruowany wyłącznie do obsługi modułów pamięci SSD i w żadnej konfiguracji nie może obsługiwać przestrzeni danych użytkownika na dyskach obrotowych/talerzowych. * Przestrzeń użytkowa po zbudowaniu RAID 6 z min. 1 dyskiem hot-spare lub przestrzenią hot‑spare równą pojemności min. 1 dysku musi wynosić min 41TB. Rozmiar RAW pojedynczego dysku nie może być większy niż 4 TB. * Wymagana pojemność użytkowa rozumiana jest jako pojemność dostępna po konfiguracji RAID i odliczeniu rezerwy na dyski/przestrzeń *spare* i dostępna dla hostów bez uwzględnienia jakichkolwiek mechanizmów kompresji, czy deduplikacji. |  |
| 4 | **Zabezpieczenia RAID** | |
| 4.1 | * Dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6 lub równoważnej, tolerującej jednoczesną awarię 2 dysków bez utraty danych. * Urządzenie musi umożliwiać bezpieczne usuwanie danych zgodnie ze standardem DoD 5220.22-Mpoprzez mechanizm nadpisywania danych. |  |
| 5. | **Pamięć Cache** | |
| 5.1 | * Co najmniej 256GB pamięci cache na cały deduplikator (dwa kontrolery). * Pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania. |  |
| 6. | **Dostępne interfejsy** | |
| 6.1. | * Urządzenie musi posiadać minimum:   12 portów Ethernet 10 Gb/s z możliwością obsługi każdym portem Ethernet protokołów CIFS, NFS, wszystkie porty wyposażone we wkładki optyczne. |  |
| 7. | **Obsługiwane protokoły** | |
| 7.1 | * Wymagane wsparcie dla FC, iSCSI, NFS, CIFS. |  |
| 8. | **Zarządzanie** | |
| 8.1 | * Zarządzanie deduplikatorem (wszystkimi kontrolerami) z poziomu pojedynczego interfejsu graficznego. Wymagane jest stałe monitorowanie stanu deduplikatora w tym monitorowanie wydajności obiektów takich jak: * cały deduplikator * kontrolery * CPU * porty front-end * porty logiczne * dyski * file systemy * Pod kątem parametrów takich jak: * operacje wejścia/wyjścia IOPS * przepustowość (KB/s lub MB/s) * czas odpowiedzi (latency) * średnie użycie (w % dla CPU) * Wymagana możliwość dostępu do historycznych danych wydajnościowych z poziomu GUI urządzenia do co najmniej 2 lat wstecz lub jako równoważne dostarczenie fizycznego serwera z oprogramowaniem umożliwiającym zbieranie i przeglądanie danych historycznych. * Wymagany dostęp do informacji o wykorzystanej przestrzeni. * Wymagana możliwość tworzenia wielu użytkowników deduplikatora w oparciu o wbudowane role. Rozwiązanie musi umożliwiać tworzenie własnych ról. * Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje to ich dostarczenie jest wymagane na tym etapie postępowania oraz należy je uwzględnić w cenie ofertowej. |  |
| 9. | **Redukcja danych** | |
| 9.1 | * Urządzenie musi deduplikować dane inline przed zapisem na nośnik dyskowy. * Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym bloku. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych. * Proces deduplikacji musi odbywać się inline – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. * Dane muszą być poddane także procesowi kompresji. * Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia oraz należy je uwzględnić w cenie ofertowej. * Wymagana także obsługa deduplikacji na źródle, co pozwala ograniczyć zużycie sieci. |  |
| 10. | **Kontrola zasobów plikowych** | |
| 10.1 | * Wymagana możliwość skonfigurowania tzw. quoty ograniczającej wystawione zasoby plikowe. Wymagana możliwość ograniczenia użytkownikom przestrzeni, z której mogą korzystać lub liczby plików jakie mogą być przechowywane na udostępnionej przestrzeni. * Wymagana możliwość skonfigurowania polityki filtrowania zapisywanych plików poprzez wykluczenie ich konkretnych rozszerzeń. * Wymagana możliwość ograniczenia dostępu do udostępnionych udziałów CIFS/NFS poprzez zdefiniowanie adresów IP lub ich przedziałów, które będą miały do nich dostęp. * Dostarczenie powyższych funkcjonalności jest wymagane na tym etapie postępowania oraz należy je uwzględnić w cenie ofertowej. |  |
| 11. | **Ochrona zasobów plikowych** | |
| 11.1 | * Tworzenie na żądanie tzw. migawkowej kopii danych (ang. snapshot) file systemów w ramach deduplikatora do wykorzystania w celu np. wykonywania kopii zapasowych. * Wymagana jest możliwość utworzenia harmonogramu snapshotów, które będą zabezpieczone przed modyfikacją oraz usunięciem przez wybrany okres czasu bez odpowiednich uprawnień celem przywrócenia danych w przypadku ataku ransomware. * Musi być możliwość odtworzenia danych z dowolnej kopii (snapshot) wykonanej w ramach harmonogramu. * Odtworzenie danych z jednej kopii nie może uniemożliwiać odtworzenia danych z innej kopii z innego punktu w czasie. * Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania na całą przestrzeń dyskową i na maksymalną liczbę snapshotów obsługiwanych przez oferowany model deduplikatora oraz należy je uwzględnić w cenie ofertowej. * Wymagana możliwość zablokowania plików przed modyfikacją lub usunięciem (WORM). * Dostarczenie licencji na tą funkcjonalność jest wymagane na tym etapie postępowania oraz należy je uwzględnić w cenie ofertowej. |  |
| 12. | **Replikacja danych** | |
| 12.1 | * Urządzenie musi umożliwiać replikację danych do drugiego urządzenia w ramach tej samej rodziny oferowanego deduplikatora. * Replikacja musi się odbywać w trybie asynchronicznym. Wymagana możliwość ograniczenia ilości przesyłanych danych poprzez ich deduplikację oraz kompresję. * Deduplikator musi umożliwiać konfigurację harmonogramu replikacji poprzez określenie interwału (np. replikacja co 60 min) lub konkretnych okien czasowych (np. w każdą sobotę o godz. 20:00). * Dostarczenie powyższych funkcjonalności jest wymagane na tym etapie postępowania oraz należy je uwzględnić w cenie ofertowej. * Wymagana możliwość zastosowania funkcjonalności typu AirGap czyli fizyczne wyłączanie portów dedykowanych do replikacji w czasie kiedy replikacja nie jest wykonywana. Dopuszcza się realizację tej funkcjonalności poprzez zastosowanie dodatkowego oprogramowania. * Dostarczenie funkcjonalności typu AirGap nie jest wymagane na tym etapie postępowania. |  |
| 13. | **Szyfrowanie danych** | |
| 13.1 | * Wymagane szyfrowanie danych zapisywanych na deduplikatorze algorytmem AES256 lub silniejszym. * Licencja do obsługi tej funkcjonalności nie jest przedmiotem postępowania. |  |
| 14. | **Obsługa serwisowa** | |
| 14.1 | * Deduplikator musi posiadać możliwość upgrade’u firmware-u kontrolerów bez przerywania dostępu do danych. * Urządzenie przystosowane do napraw w miejscu instalacji oraz wymiany elementów bez konieczności jego wyłączania * Urządzenie musi umożliwiać zdalne zarządzanie. * Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta, a także musi być objęte serwisem producenta lub autoryzowanego partnera serwisowego na terenie RP. * Deduplikator musi zostać objęty minimum 2 letnim okresem gwarancji producenta z gwarantowanym czasem reakcji najpóźniej w następnym dniu roboczym od momentu zgłoszenia usterki. Zamawiający dopuszcza realizacje gwarancji przez autoryzowanego partnera serwisowego producenta. |  |
| **XI Zaawansowana ochrona stacji roboczych – rozbudowa obecnego systemu** | | |
| Przedmiotem dostawy jest rozbudowa posiadanego systemu bezpieczeństwa infrastruktury teleinformatycznej typu Fortinet FortiGate 100F o elementy zabezpieczeń dla stacji roboczych używanych w pracy zdalnej, wraz z mechanizmami centralnego zarządzania.  Dostarczone rozwiązanie do ochrony stacji roboczych musi zapewniać wszystkie wymienione poniżej funkcje i mechanizmy. Dopuszcza się aby poszczególne elementy wchodzące w skład rozwiązania były zrealizowane w postaci osobnych, komercyjnych platform lub komercyjnych aplikacji.  Parametry systemu ochrony dla stacji roboczych: | | |
| 1. | **Elementy systemu ochrony dla stacji roboczych powinny zapewniać następujące funkcje i mechanizmy** | |
| 1.1 | * Kontrola antywirusowa. * Funkcja analizy plików w zewnętrznym systemie Sandbox. * Opcja kwarantanny lokalnej plików przesłanych do Sandbox na czas analizy. * URL filtering w oparciu o kategorie stron z opcją definiowania wyjątków. * Kontrola aplikacji - w oparciu o wbudowany Firewall aplikacyjny. * Mechanizmy analizy podatności na stacji roboczej - pozwalające wykryć zagrożenia w systemie operacyjnym oraz zainstalowanych aplikacjach. * Mechanizmy szyfrowanych połączeń typu IPSec VPN z opcją Split tunneling (przekierowanie tylko określonego ruchu do tunelu) oraz możliwością przekierowania całego ruchu do tunelu. * Mechanizmy szyfrowanych połączeń typu SSL VPN z opcją Split tunneling (przekierowanie tylko określonego ruchu do tunelu) oraz możliwością przekierowania całego ruchu do tunelu. * Możliwość zastosowania certyfikatów cyfrowych w procesie uwierzytelnienia przy realizacji szyfrowanych połączeń. * Mechanizmy uwierzytelniania dwuskładnikowego * AntiExploit, * blokowanie dysków przenośnych typu USB, * Poszczególne mechanizmy muszą być dostępne dla następujących systemów operacyjnych: Microsoft Windows 7/8/10/11, Mac OS X, Linux OS * Dostarczony system centralnego zarządzania aplikacjami klienckimi musi zapewniać wszystkie wymienione poniżej funkcje. Wymaga się aby elementy wchodzące w skład systemu były zrealizowane w postaci komercyjnych platform wirtualnych lub aplikacji instalowanych na systemach operacyjnych: Microsoft Windows Server 2019/2022 * System powinien umożliwiać automatyczną aktualizację oprogramowania zabezpieczającego na urządzeniach końcowych oraz musi zapewniać mechanizmy integracji z sieciowymi systemami bezpieczeństwa (Firewall) * Ponadto wymagane jest aby system zapewniał:   + integrację z systemami zarządzania tożsamością użytkowników – co najmniej AD,   + definiowanie różnych profilów (wersji konfiguracji) ochrony dla różnych grup użytkowników czerpanych z AD lub definiowanych lokalnie,   + zautomatyzowany proces zarządzania aplikacja kliencką,   + przygotowywanie paczek instalacyjnych przynajmniej dla systemu Windows 32/64 bit i MacOS w których administrator może określić komponenty dla ochrony stacji roboczych takich jak AV, WebFiler, Skaner Podatności.   + możliwość edycji pliku konfiguracyjnego w zewnętrznym edytorze tekstowym,   + panel, w którym wyświetlane są wyniki analizy podatności na stacjach roboczych,   + panel w którym wyświetlane są informacje o podłączonych i zarządzanych stacjach roboczych,   + możliwość wymuszenia patchowania wykrytych podatności na stacjach roboczych,   + automatyczne wykrywanie stacji klienckich w grupach roboczych,   + logowanie zdarzeń z aplikacji klienckich, możliwość ich przeglądania z funkcja filtrów oraz możliwością pobierania logów przez administratora,   + generowanie alarmów: związanych z zarządzeniem aplikacją kliencką, w przypadku wykrycia ważnych podatności na stacjach oraz w sytuacji zaistnienia zdarzeń związanych z aktywnością złośliwego kodu, aktywności aplikacji botnet z wykorzystaniem komunikacji C&C, nieaktualnej bazy danych dla sygnatur antywirusa.   + definiowanie grup administratorów lokalnie oraz w oparciu o AD z opcja przypisywania uprawnień do elementów panelu konfiguracyjnego,   + zarządzenie certyfikatami na potrzeby połączeń IPSec VPN oraz SSL VPN,   + automatyczne wykrywanie aplikacji zainstalowanych na stacjach klienckich z możliwością filtrowania przynajmniej po producencie i nazwie aplikacji,   + możliwość przeniesienia użytkownika przez administratora do kwarantanny i personalizację komunikatu, który wyświetli się użytkownikowi,   + możliwość wymuszenia przeskanowania stacji klienckiej za pomocą antywirusa i skanera podatności na żądanie jak i cyklicznie,   + możliwość skonfigurowania weryfikacji zgodności (compliance) w celu sprawdzenia czy na stacji końcowej jest aktualna baza sygnatur dla AV, czy jest odpowiednia wersja systemu operacyjnego, czy jest uruchomiony odpowiedni proces. * Administrator musi mieć możliwość wykonywania backupu i odtwarzania bazy danych, w oparciu o którą działają elementy system. * Centralny system zarządzania musi zapewniać możliwość dystrybucji paczek instalacyjnych z lokalnych zasobów w oparciu o adres URL definiowany przez administratora lub w ramach postępowania koniecznym jest dostarczenie odpowiednio zabezpieczonego portalu, za pośrednictwem którego administrator będzie mógł dystrybuować paczki instalacyjne. * W ramach postępowania wraz z konsolą centralnego zarządzania muszą zostać dostarczone niezbędne licencje upoważniające do:   - zainstalowania i centralnego zarządzania aplikacjami klienckimi na 25 stacjach roboczych.  - dla wskazanej powyżej ilości stacji roboczych licencje powinny obejmować:  Web Filtering, Skaner podatności, Remote Access, Centralne zarządzanie przez okres do dnia 30.06.2026r.  System musi być objęty serwisem producenta przez okres do dnia 30.06.2026r., upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7. |  |
| **XII System do zarządzania infrastrukturą IT i zasobami ludzkimi –wymagania**  **System zawierający panel użytkownika dla administratora z możliwością zarządzania urządzeniami końcowymi w ilości 100 szt.** | | |
| 1. | * Wymagania licencyjne: * licencja wieczysta * Zakres asysty technicznej: * bezpłatna aktualizacja do najnowszych wersji programu w trakcie trwania asysty * aktualizacji bazy wzorców * pomoc techniczna producenta systemu w języku polskim |  |
| 2 | **Zarządzanie zasobami**  **Pozyskiwanie informacji o sprzęcie, zarządzanie widokami, funkcje ogólne** | |
| 2.1 | Centralne zarządzanie wynikami skanowania sprzętu i oprogramowania |  |
| 2.2 | Zdalne wykrywanie urządzeń w sieci za pomocą protokołów PING, ARP oraz SNMP |  |
| 2.3 | Automatyczne wykrywanie adresów IP, MAC, DNS, Systemu Operacyjnego wraz z informacją o aktualizacji |  |
| 2.4 | Automatyczne wykrywanie, czy komputer jest członkiem domeny oraz do jakiej domeny lub grupy roboczej należy |  |
| 2.5 | Odwzorowanie struktury organizacji w oparciu o Active Directory |  |
| 2.6 | Jednostronna synchronizacja komputerów oraz drukarek z AD oraz AAD (Odwzorowanie wszystkich wprowadzonych zmian w rekordach Active Directory) |  |
| 2.7 | Automatyczne skanowanie całości lub wybranych grup Active Directory (oraz AAD) oraz sieci |  |
| 2.8 | Mapowanie atrybutów obiektów AD (oraz AAD) do obiektów w programie |  |
| 2.9 | Grupowanie wyposażenia z podziałem na jednostki organizacyjne w firmie (np. względem działów, lokalizacji, statusów) |  |
| 2.10 | Utworzenie własnych typów elementów wyposażenia |  |
| 2.11 | Grupowanie, sortowanie i filtrowanie po dowolnie nadanych atrybutach |  |
| 2.12 | Podpięcie dowolnych załączników, np. skany faktur, gwarancji oraz wszelkich innych plików |  |
| 2.13 | Przypisywanie sprzętu do konkretnych osób |  |
| 2.14 | Przypisywanie sprzętu do dowolnej lokalizacji |  |
| 2.15 | Definiowanie własnych, dowolnych atrybutów sprzętu |  |
| 2.16 | Wydruk etykiet z kodami kreskowymi do inwentaryzacji wyposażenia |  |
| 2.17 | Grupowa zmiana domeny/grupy roboczej zasobu |  |
| 3 | **Informacje o sprzęcie** | |
| 3.1 | Automatyczne wykrywanie typu komputera (Desktop\Notebook\Serwer\Kontroler domeny) na podstawie wyników skanowania sprzętu |  |
| 3.2 | Automatyczne uzupełnianie informacji o procesorze, liczbie rdzeni, ilości pamięci RAM, rozmiarze dysku, nazwie karty graficznej i rozdzielczości monitora w obiekcie zasobu po wykonaniu skanowania sprzętu |  |
| 3.3 | Odczytywanie indeksów wydajności poszczególnych komponentów komputera: CPU, GPU, HDD, RAM |  |
| 3.4 | Automatyczna aktualizacja nazwy komputera w przypadku jej zmiany |  |
| 3.5 | Definiowanie statusów dla sprzętu (Nowy, Do kasacji, W serwisie, itd. ) |  |
| 3.6 | Szczegółowa informacja na temat podzespołów sprzętu (procesor, bios, płyta główna, pamięć, dyski twarde, monitory, karty graficzne i muzyczne, etc. ) |  |
| 3.7 | Odczyt informacji o module TPM |  |
| 3.8 | Inwentaryzacja osprzętu komputerowego (monitory, drukarki, myszki, urządzenia sieciowe: Switch, Router, Access Point, Bridge, Modem, NAS, UPS, itd.) |  |
| 3.9 | Automatyczne wykrywanie lokalnych drukarek (USB) na podstawie wyników skanowania sprzętu |  |
| 3.10. | Automatyczne tworzenie zestawów: Komputer + Monitor |  |
| 3.11 | Automatyczne utworzenie zestawów: Komputer + drukarka lokalna |  |
| 3.12 | Określanie informacji o wykorzystywanej wirtualizacji |  |
| 3.13 | Cykliczne wykonywanie skanowania sprzętu z różnymi ustawieniami |  |
| 3.14 | Automatyczne odczytywanie ServiceTag oraz modelu komputera (na podstawie wyników skanowania sprzętu) |  |
| 3.15 | Automatyczna aktualizacja adresów IP komputerów bez zainstalowanego agenta |  |
| 3.16 | Agent odczytuje identyfikator SID komputera |  |
| 3.17 | Określanie adresu interfejsu webowego urządzenia sieciowego |  |
| 3.18 | Wyszukiwanie i identyfikacja duplikatów zasobów |  |
| 4. | **Raporty zasobów** | |
| 4.1 | Automatyczne tworzenie historii zmian sprzętu |  |
| 4.2 | Raport zbiorczy historii zmian w sprzęcie |  |
| 4.3 | Ewidencja zdarzeń serwisowych |  |
| 4.4 | Informacja na temat pojemności dysków twardych oraz wolnego miejsca |  |
| 4.5 | Wydruk\dodawanie jako załącznik protokołu przekazania\zwrotu\utylizacji sprzętu |  |
| 4.6 | Wydruk\dodawanie jako załącznik protokołu przekazania dla całego zestawu |  |
| 4.7 | Wydruk\dodawanie jako załącznik Karty informacyjnej do elementu wyposażenia |  |
| 4.8 | Wydruk lub zapis do pliku raportów ze szczegółami sprzętu |  |
| 4.9 | Porównywarka wyników skanowania sprzętu |  |
| 4.10 | Dzienniki zdarzeń systemu Windows |  |
| 4.11 | Automatyczny monitoring i raportowanie zmian w podzespołach sprzętu |  |
| 4.12 | Geolokalizacja komputerów z agentem |  |
| 5 | **Funkcje dodatkowe** | |
| 5.1 | Zdalne wykonywanie skryptów (batch/powershell) - Obsługa zadań jednorazowych i cyklicznych |  |
| 5.2 | Wykonywanie skryptów w kontekście sesji użytkownika lub usługi |  |
| 5.3 | Skrypty wykonywane po uruchomieniu komputera lub zalogowaniu użytkownika |  |
| 5.4 | Import informacji o wyposażeniu z pliku CSV |  |
| 5.5 | Wyszukiwanie sterowników, informacji o komputerze, informacji o gwarancji w bazie producenta (DELL) |  |
| 5.6 | Mechanizm automatycznego tworzenia rekordów producenta sprzętu (na podstawie wyników skanowania sprzętu) |  |
| 5.7 | Generowanie kodów paskowych, QR dla każdego elementu wyposażenia |  |
| 5.8 | Powiadomienia o kończącej się gwarancji\umowie serwisowej dla zasobu |  |
| 5.9 | Zachowanie ostatniego skanu sprzętu podczas konserwacji bazy danych |  |
| 6. | **Zarządzanie oprogramowaniem**  **Licencje** | |
| 6.1 | Inwentaryzacja licencji |  |
| 6.2 | Automatyczne tworzenie licencji na podstawie kluczy produktów |  |
| 6.3 | Odczytu OriginalProductKey (BIOS/UEFI) dla systemu operacyjnego |  |
| 6.4 | Import licencji z pliku tekstowego |  |
| 6.5 | Tworzenie licencji z poziomu raportu kluczy licencji |  |
| 6.6 | Tworzenie zestawów licencji |  |
| 6.7 | Kompletna informacja na temat posiadanych licencji (typ, producent, program licencjonowania, czas ważności, informacje finansowe) |  |
| 6.8 | Przypisywanie licencji do komputera |  |
| 7. | **Skanowanie oprogramowania** | |
| 7.1 | Skanowanie oprogramowania na podstawie harmonogramu oraz definicji skanera |  |
| 7.2 | Automatyczna kontrola zmian w stanie zainstalowanego oprogramowania bez zlecania skanów |  |
| 7.3. | Śledzenie zmian w stanie zainstalowanego oprogramowania |  |
| 7.4 | Zdalny skan komputerów (bieżący lub okresowy) |  |
| 7.5 | Identyfikacja zainstalowanych aplikacji na podstawie wzorców oprogramowania |  |
| 7.6 | Prawidłowe rozpoznanie aplikacji nawet mimo zmiany jej nazwy |  |
| 7.7 | Skan oraz identyfikacja zawartości archiwów zapisanych w formatach: 7z, arj, bz2, bzip2, cab, gz, gzip, img, iso, jar, lha, lzh, lzma, msi, nrg, rar, tar, taz |  |
| 7.8 | Wykrywanie plików multimedialnych |  |
| 7.9 | Wykrywanie i inwentaryzacja plików dowolnego typu (np. multimedia, czcionki, grafika) |  |
| 7.10 | Bezpłatna, automatycznie aktualizowana baza wzorców aplikacji\pakietów\systemów operacyjnych |  |
| 8 | **Kontrola wykorzystania sprzętu i oprogramowania**  **Pozyskiwanie informacji o użytkownikach, zarządzanie widokami, funkcje ogólne** | |
| 8.1 | Dane gromadzone dla konkretnych użytkowników (na bazie kont Windows) - jeden użytkownik może mieć przypisanych wiele kont Windows i pracować na różnych komputerach |  |
| 8.2 | Odczyt informacji o kontach lokalnych komputera, wraz z odczytem grup do, których konto należy |  |
| 8.3 | Odczytywanie informacji o użytkownikach z Active Directory oraz AAD |  |
| 8.4 | Pełna synchronizacja rekordów użytkowników (Odwzorowanie wszystkich wprowadzonych zmian w rekordach Active Directory oraz AAD) |  |
| 8.5 | Baza danych teleadresowych użytkowników z możliwością tworzenia raportów i zestawień |  |
| 8.6 | Automatyczne tworzenie działów na podstawie informacji odczytanych z Active Directory |  |
| 9 | **Raporty** | |
| 9.1 | Analiza aktywności użytkowników |  |
| 9.2 | Grupowanie danych według komputerów jeśli użytkownik wykorzystywał więcej niż jedno stanowisko |  |
| 9.3 | Analiza zdarzeń sesji użytkownika (Logowanie, Wylogowanie, Zablokowanie, Odblokowanie, Nawiązanie połączenia RDP, Zakończenie połączenia RDP ) |  |
| 9.4 | Analiza jakości pracy (liczba kliknięć myszą, liczba wpisanych znaków) |  |
| 9.5 | Analiza wykorzystania poszczególnych aplikacji w czasie |  |
| 9.6. | Analiza czasu działania aplikacji, na pierwszym planie oraz sumarycznie |  |
| 9.7 | Statystyki wykorzystania komputerów przez poszczególnych użytkowników |  |
| 9.8 | Statystyki aktywności użytkownika i grup użytkowników |  |
| 9.9 | Informacje o drukowanych dokumentach (osoba, nazwa pliku, ilość stron, ilość kopii, cz-b/kolor, dpi) |  |
| 9.10 | Monitoring wydruków na drukarkach sieciowych |  |
| 9.11 | Informacja o operacjach na nośnikach zewnętrznych (CD/DVD, HDD, FDD, Pen Drive, etc.) |  |
| 10. | **Kontrola wykorzystania Internetu**  **Funkcje** | |
| 10.11 | Blokada stron internetowych dla poszczególnych użytkowników, możliwość zastosowania filtrów, blokada WWW po zawartości (ContentType) |  |
| 10.12 | Blokada stron internetowych dla protokołu http \ https w najpopularniejszych przeglądarkach WWW |  |
| 10.13 | Kategoryzacja stron internetowych |  |
| 10.14 | Blokada dostępu do witryn zgodnie z harmonogramem |  |
| 10.15 | Blokada trybu incognito w przeglądarce Google Chrome |  |
| 11. | **Raporty** | |
| 11.1 | Raporty dotyczące aktywności użytkowników w Internecie |  |
| 11.2 | Analiza czasu przebywania na poszczególnych stronach lub domenach (z uwzględnieniem informacji o tytule strony i wersji przeglądarki ) |  |
| 11.3 | Analiza liczby wejść na poszczególne strony lub domeny |  |
| 11.4 | Kategoryzacja odwiedzanych domen i stron |  |
| 11.5 | Raport informujący o plikach pobranych przez przeglądarki WWW |  |
| 11.6 | Raport informujący o danych wysłanych przez przeglądarki (bez Firefox) |  |
| 11.7 | Monitoring plików pobieranych przez przeglądarki internetowe |  |
| **XIII Aktualizacja posiadanego programu do backupu i archiwizacji komputerów w sieciach LAN, 1 szt** | | |
| 1. | Aktualizacja ma objąć obecnie posiadany Ferro Backup System 5 (uprawniający do używania produktu na następującej liczbie komputerów: stacje robocze: 100, serwery: 6 do wersji aktualnej |  |
| **XIV Wsparcie posiadanego programu do backupu maszyn wirtualnych NAKIVO Backup & Replication Pro Essentials, 1 szt** | | |
| 1. | Wsparcie dla obecnie posiadanej licencji NAKIVO Backup & Replication Pro Essentials, 6 sockets do 30.06.2026r  Opis równoważności: Oferowane rozwiązanie musi zapewniać funkcje backupu, replikacji, odzyskiwania i wsparcia technicznego na poziomie co najmniej równym do NAKIVO Backup & Replication Pro Essentials dla 6 socketów, gwarantując pełne wsparcie i ochronę danych Zamawiającego do 30.06.2026 r. |  |
| **XV Urządzenie UTM dla CUW, 1 szt**  ***Wymagania ogólne*** | | |
| 1. | * Urządzenie ma współpracować z posiadanym przez Zamawiającego urządzeniem Fortigate FG100f i być zarządzane ze wspólnego panelu administracyjnego. * Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. * Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa 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. * System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. * W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji System musi wspierać IPv4 oraz IPv6 w zakresie: Firewall, Ochrony w warstwie aplikacji, Protokołów routingu dynamicznego |  |
| 2 | **Redundancja, monitoring i wykrywanie awarii** | |
| 2.1 | * 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. * Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. * Monitoring stanu realizowanych połączeń VPN. * System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych. |  |
| 3 | **Interfejsy, Dysk, Zasilanie** | |
| 3.1 | * System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: 5 portami Gigabit Ethernet RJ-45. * System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. * System jest wyposażony w zasilanie AC |  |
| 4. | **Parametry wydajnościowe** | |
| 4.1 | * W zakresie Firewall’a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę. * Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B. * Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps. * Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 Gbps. * Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1 Gbps. * Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps. * Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps. |  |
| 5. | **Funkcje Systemu Bezpieczeństwa:** | |
| 5.1 | * W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: * Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. * Kontrola Aplikacji. * Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. * Ochrona przed malware. * Ochrona przed atakami - Intrusion Prevention System. * Kontrola stron WWW. * Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. * Zarządzanie pasmem (QoS, Traffic shaping). * Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). * Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. * Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. * Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.   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). |  |
| 6. | **Polityki, Firewall** | |
| 6.1 | * Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. * System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:   + Translację jeden do jeden oraz jeden do wielu.   + Dedykowany ALG (Application Level Gateway) dla protokołu SIP. * W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. * Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. * Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. * Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. * Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. * Amazon Web Services (AWS).   + Microsoft Azure.   + Cisco ACI.   + Google Cloud Platform (GCP).   + OpenStack. * VMware NSX |  |
| 7. | **Połączenia VPN** | |
| 7.1 | * System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: * Wsparcie dla IKE v1 oraz v2. * Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). * Obsługa protokołu Diffie-Hellman grup 19, 20. * Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. * Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. * Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. * Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. * Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. * Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. * Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. * Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. * Mechanizm „Split tunneling” dla połączeń Client-to-Site. * System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia: * Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0. * Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. * Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji. |  |
| 8. | **Routing i obsługa łączy WAN** | |
| 8.1 | W zakresie routingu rozwiązanie zapewnia obsługę:   * Routingu statycznego. * Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). * Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. * Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. * ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. * BFD (Bidirectional Forwarding Detection). * Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu. |  |
| 9. | **Funkcje SD-WAN** | |
| 9.1 | * System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. * SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec). |  |
| 10. | **Zarządzanie pasmem** | |
| 10.1 | * System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. * System daje możliwość określania pasma dla poszczególnych aplikacji. * System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. * System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL. |  |
| 11. | **Ochrona przed malware** | |
| 11.1 | * Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). * Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. * System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości. * System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. * System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). * Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. * System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze. * System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. * Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. * Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu. |  |
| 12. | **Ochrona przed atakami** | |
| 12.1 | * Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. * System chroni przed atakami na aplikacje pracujące na niestandardowych portach. * Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. * Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. * System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. * Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). * Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. * Wykrywanie i blokowanie komunikacji C&C do sieci botnet. * Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie. |  |
| 13. | **Kontrola aplikacji** | |
| 13.1 | * Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. * Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. * Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. * Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. * Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. * Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). * System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80). |  |
| 14. | **Kontrola WWW** | |
| 14.1 | * Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. * W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. * Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. * Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. * Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). * Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. * Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. * Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. * System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji. |  |
| 15. | **Uwierzytelnianie użytkowników w ramach sesji** | |
| 15.1 | * System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: * Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. * Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. * Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. * System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. * System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. * Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. |  |
| 16. | **Zarządzanie** | |
| 16.1 | * 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. * Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. * Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. * System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. * System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. * Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. * Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. * Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). * Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP. |  |
| 17. | **Logowanie** | |
| 17.1 | * 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. * W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. * Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. * Możliwość włączenia logowania per reguła w polityce firewall. * System zapewnia możliwość logowania do serwera SYSLOG. * Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS. |  |
| 18. | **Testy wydajnościowe oraz funkcjonalne** | |
| 18.1 | Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy. |  |
| 19. | **Serwisy i licencje** | |
| 19.1 | 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 na okres do 30.06.2026r. |  |
| **XVI Usługa instalacji i konfiguracji środowiska sieciowego w Urzędzie Miejskim w Boguchwale oraz w Centrum Usług Wspólnych (CUW)** | | |
| 1. | * Prace polegające na instalacji, konfiguracji oraz integracji dostarczonego sprzętu i oprogramowania z obecną infrastrukturą. * Instalacja we wskazanych lokalizacjach przez Zamawiającego. Obejmuje to również migracje maszyn wirtualnych do nowych zasobów. * Wymagana jest pełna instalacja i konfiguracja dostarczonych urządzeń i oprogramowania oraz integracja ze środowiskiem informatycznym Zamawiającego. Czynności te dotyczą zarówno Urzędu Miejskiego w Boguchwale jak i Centrum Usług Wspólnych w Boguchwale. * Wykonawca zobowiązany jest zainstalować, uruchomić i skonfigurować wszystkie elementy dostawy zgodnie z wytycznymi Zamawiającego a w szczególności wykonać następujące prace:   + - montaż urządzeń we wskazanym przez Zamawiającego miejsca.     - uruchomienie i konfiguracja wysokodostępnego klastra macierzy w trybie HA     - integracja dostarczonych macierzy z istniejącym środowiskiem VSphere, połączona z migracją danych     - migracja danych w trybie bezprzerwowym     - uruchomienie dostępnych usług bezpieczeństwa danych na istniejących i nowych macierzach zgodnie z aktualnymi najlepszymi praktykami i zaleceniami producenta     - wymiana jednego z serwerów esxi w pracującym klastrze VSphere na nowy (prace w trybie bezprzerwowym, Zamawiający gwarantuje zasoby na pozostałych węzłach na czas wymiany)     - Podniesienie klastra Vmware do aktualnej wersji zgodnie z posiadaną licencją na VMWare (v.8)     - instalacja i uruchomienie środowiska na potrzeby dostarczonego oprogramowania na klastrze wirtualizacyjnym     - uruchomienie wraz z konfiguracją dostarczonego urządzenia UTM     - uruchomienie i konfiguracja (integracja z istniejącym środowiskiem) klastra sieciowych przełączników zarządzalnych     - aktualizacja polityk backupu dla zabezpieczenia nowych obiektów w środowisku     - instalacja i wdrożenie dostarczonego oprogramowania oraz systemów, podniesienie ich wersji do obecnie aktualnych     - dostawa, uruchomienie i wdrożenie dostarczonego deduplikatora danych     - integracja deduplikatora ze środowiskiem sieci i backupu jako miejsce składowania kopii zapasowych     - konfiguracja zabezpieczeń danych na deduplikatorze zgodnie z zaleceniami producenta/najlepszymi praktykami mająca na celu zabezpieczenie ich na wypadek usunięcia/zaszyfrowania     - ustawienie polityk przechowywania i retencji danych na deduplikatorze     - instalacja i konfiguracja istniejącego środowiska domenowego AD na nowych serwerach     - instalacja oraz konfiguracja pozostałych elementów dostawy zgodnie z wytycznymi Zamawiającego     - świadczenie wsparcia technicznego dla wdrożonych rozwiązań do dnia 30.06.2026 * Wykonawca zobowiązany jest zapewnić wszystkie niezbędne dla zestawienia urządzeń elementy połączeniowe (kable, wkładki światłowodowe, itp.) | **Nie dotyczy** |