Załącznik do SWZ nr 8

OPIS PRZEDMIOTU ZAMÓWIENIA

Na potrzeby postępowania pn.: „Cyberbezpieczny Samorząd w Gminie Bierawa - dostawa systemów cyberbezpieczeństwa" w ramach Projektu Cyberbezpieczny Samorząd realizowanego w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa.

Wymagania ogólne

W przypadkach, kiedy w szczegółowym opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego Wykonawcę, co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne". Dostarczany sprzęt musi być fabrycznie nowy, nieużywany, nieregenerowany, kompletny, wyprodukowany nie wcześniej niż w 2024 r., wolny od jakichkolwiek wad fizycznych i prawnych, sprawny technicznie, pochodzić z oficjalnego kanału dystrybucyjnego. Przez stwierdzenie "fabrycznie nowy" należy rozumieć sprzęt opakowany oryginalnie (opakowanie musi być nienaruszone i posiadać zabezpieczenie zastosowane przez producenta). Przez "wadę fizyczną" należy rozumieć również jakąkolwiek niezgodność ze szczegółowym opisem przedmiotu zamówienia. Sprzęt musi być wyposażony we wszystkie niezbędne do jego działania i zapewnienia wymaganych funkcjonalności Sprzętu standardowe rozwiązania softwarowe wraz z prawem do bezterminowego korzystania przez Zamawiającego z tych rozwiązań w takiej funkcji, jednakże w każdym przypadku nie krócej, niż przez czas, w jakim będzie technicznie możliwe używanie Sprzętu. O ile inaczej nie zaznaczono, wszelkie zapisy SOPZ zawierające parametry techniczne należy odczytywać jako parametry minimalne.

---

1. Biblioteka Taśmowa – 1 szt.

L.p.	Element konfiguracji	Wymagane minimalne parametry techniczne
1.	**Wykorzystana technologia**	LTO Ultrium wspierająca technologię partycjonowania nośników.
2.	**Obudowa**	Typu rack 19". Wysokość maksymalnie 1U - wszystkie elementy do montażu muszą być dostarczone wraz z urządzeniem. Urządzenie musi mieć możliwość instalowania w tej samej obudowie różnych generacji napędów LTO (minimum od LTO-6 wzwyż).
3.	**Zainstalowany napęd**	Jeden napęd LTO-8 wyposażony w dwa złącza mSAS SFF-8088. Urządzenie musi mieć możliwość instalowania w tej samej obudowie także napędów LTO z interfejsem FC oraz wspierać technologię LTFS (Linear Tape File System). Prędkość zapisu napędu bez kompresji – minimum 300 MB/sek. Zainstalowany napęd musi mieć możliwość dynamicznego i płynnego dopasowania prędkości do napływających danych (speed matching) w przedziale od 100 do 300 MB/sek. oferować funkcję SkipSync zapewniającą dużą szybkość zapisu małych plików bez konieczności zatrzymywania i przewijania kasety oraz stosować szyfrowanie danych metodą AES 256-bit zgodną ze standardem FIPS 140-2

4.	**Ilość slotów i magazynki**	Minimum 8 kieszeni na taśmy podzielone na dwa magazynki (urządzenie musi być dostarczone z kompletem magazynków). Wymagana ilość mail slot (I/E): min. 1. Wymiana taśm przez MailSlot musi odbywać się bez konieczności wysuwania całego magazynka.
5.	**Pojemność**	Pojemność bez kompresji – minimum 96TB przy obsadzeniu wszystkich slotów na taśmy wyłącznie nośnikami LTO-8
6.	**Zarządzanie**	Za pomocą panelu kontrolnego znajdującego się na froncie urządzenia oraz zdalne przez sieć poprzez przeglądarkę internetową (web GUI) za pomocą interfejsu FastEthernet. Wymagane wsparcie SNTP, protokołów SSL/TLS i IPv6 oraz definiowanie minimum 4 poziomów zarządzania urządzeniem i dostępem do niego. Urządzenie musi mieć możliwość zabezpieczania swojej konfiguracji na podłączony, poprzez slot USB, PenDrive. Operacja powinna być możliwa zarówna poprzez web GUI jak i poprzez panel kontrolny urządzenia. Wymagana możliwość zdalnego wysuwania magazynków, restartowania biblioteki oraz wyłączania zasilania napędów poprzez webGUI.
7.	**Dodatkowe interfejsy**	Biblioteka musi być wyposażone w interfejs sieciowy, interfejs USB oraz interfejs ADI
8.	**Obsługa urządzenia**	Wymagana możliwość wymiany napędu, zasilacza, modułu portów zarządzania u użytkownika bez konieczności demontażu urządzenia z szafy przemysłowej oraz bez konieczności zdejmowania pokrywy głównej. Możliwość wyjmowania magazynków z urządzenia nawet przy braku zasilania. Zarówno napęd jak i zasilacz oraz moduł portów zarządzania powinny być wyposażone w lamki kontrolne, informujące o stanie technicznym i widoczne na tylnej stronie biblioteki.
9.	**Wyposażenie**	Urządzenie musi być standardowo wyposażone w czytnik kodów kreskowych, zestaw kabli: 1x zasilając, 1x sieciowy oraz 1x komunikacyjny konieczny do podłączenia urządzenia do odpowiedniego kontrolera serwera umożliwiającego komunikację z urządzeniem – długość kabla min. 2m. oraz kontroler SAS do podłączenia biblioteki z posiadanym przez zamawiającego serwerem - interfejs kontrolera: minimum single SAS 12Gb. Wraz z urządzeniem należy dostarczyć także zestaw 4 identycznych nośników na dane o pojemności natywnej pojedynczego nośnika min. 12TB oraz jeden nośnik czyszczący wyposażonych w unikalne naklejki z kodem kreskowym. Wszystkie dostarczone nośniki muszą być kompatybilne i dedykowane do współpracy z oferowanym urządzeniem – Instrukcja instalacji w języku polskim lub angielskim.
11.	**Gwarancja i oświadczenia**	36 miesięcy z czasem reakcji do 72 godz. (dni robocze) od momentu zgłoszenia uszkodzenia. Czas przyjmowania zgłoszeń serwisowych w trybie 24x7. Możliwość rozszerzenia oferowanego serwisu do 84 miesięcy. Zgłaszania awarii wyłącznie poprzez ogólnopolską linię telefoniczną producenta lub autoryzowany serwis producenta posiadający certyfikat ISO-9001 na usługi serwisowe – kontakt z serwisem wyłącznie w języku polskim. Firma serwisująca musi posiada ISO9001 na usługi serwisowe.

2. Oprogramowanie do badania podatności

LICENCJA	W ramach postępowania Wykonawca jest zobowiązany dostarczyć Oprogramowanie wraz z licencją. Wykonawca musi dostarczyć licencje czasową na okres do 30.06.2026 r. Oprogramowanie musi posiadać możliwość aktualizacji do najnowszej dostępnej wersji w okresie gwarancji. W ramach gwarancji Zamawiający ma prawo zgłaszać błędy w Oprogramowaniu do serwisu producenta. Licencje na Oprogramowanie dostarczone będą do siedziby Zamawiającego w formie papierowej lub elektronicznej. Dostarczona licencja na Oprogramowanie Systemu nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji z zgromadzonych danych. Ilość licencji dla hostów (IP address): **5 szt.**
Zaawansowany skaner podatności – w	1. Rozwiązanie zapewnia wykrywanie oraz zarządzanie podatnościami bezpieczeństwa, w środowisku informatycznym.

formularzu oferty należy podać pełną nazwę oferowanego oprogramowania	2. Architektura rozwiązania składa się z systemu zarządzania oraz osobnego, dedykowanego oprogramowania wykonującego skanowania podatności, które jest zarządzane za pomocą jednej centralnej konsoli zarządzania. 3. Dostęp do konsoli centralnego zarządzania odbywa się z poziomu interfejsu WWW, niezależnie od zastosowanej platformy sprzętowej i programowej. 4. Konsola zarządzania jest dostępna w postaci usługi hostowanej na serwerach producenta 5. Konsola zarządzania oferuje dostęp za pomocą następujących wspieranych przeglądarek internetowych: • Microsoft Edge • Mozilla Firefox • Google Chrome • Safari 6. Konsola zarządzająca dostępna jest w języku polskim. 7. Poza językiem polskim konsola wspiera języki: angielski, niemiecki, francuski, hiszpański, fiński, włoski. 8. Logowanie do konsoli umożliwia wykorzystanie mechanizmów wieloskładnikowego uwierzytelniania (2FA) dla kont posiadających dostęp do konsoli zarządzającej. 9. Mechanizm 2FA służący zabezpieczeniu dostępu do konsoli zarządzającej w swoim działaniu wykorzystuje mechanizmy: powiadomień SMS oraz tokenów jednorazowych generowanych w aplikacjach mobilnych (np. Google Authenticator, Microsoft Authenticator). 10. Konsola wyposażona jest w panel kontrolny, w którym wyświetlane są informacje podsumowujące dotyczące poziomu bezpieczeństwa chronionej organizacji. 11. Rozwiązanie realizuje skanowania podatności za pomocą dedykowanego oprogramowania, instalowanego w środowisku, zarządzanego z poziomu konsoli centralnego zarządzania. 12. Ta sama konsola umożliwia zarządzanie innymi produktami w przypadku posiadania odpowiedniej licencji w tym co najmniej ochrony antymalware, systemem EDR, ochroną usług Microsoft 365 13. Konsola pozwala na podgląd posiadanych licencji oraz ich wykorzystania. 14. Oprogramowanie skanujące podatności bez agentowo (lokalny scan node) dostępne jest w postaci aplikacji instalowanej lokalnie i wspiera poniższe systemy operacyjne: • Windows Server 2016 i nowsze • Ubuntu server (wersje 64 bitowe 16.x 18.x, 20.x) • Debian (wersje 64 bitowe 9,10,11) 15. Rozwiązanie umożliwia również agentowe skanowanie w poszukiwaniu podatności na komputerach z systemem Windows. 16. Agent instalowany na systemach Windows wspiera systemy MS Windows 10 i 11 oraz systemy serwerowe MS Windows Server 2016 i nowsze. 17. Ten sam agent zainstalowany na wspieranych systemach Windows w przypadku posiadania odpowiedniej licencji może dodatkowo zapewniać również ochronę antymalware i funkcjonalność systemu EDR. 18. Skanowanie agentowe odbywać się może w cyklach co:4,6,12,24 godzin 19. Istnieje możliwość włączenia i wyłączenia funkcji skanowania agentowego. 20. Wyłączenie funkcji skanowania agentowego nie powoduje deinstalacji agenta na danym hoście. 21. Rozwiązanie umożliwia przeprowadzenie skanowania, wykrywającego urządzenia pracujące w skanowanej sieci komputerowej. 22. Skanowanie wykrywające urządzenia pracujące w skanowanej sieci umożliwia: a) wykrywanie urządzeń pracujących w skanowanej sieci na podstawie protokołów: ARP, ICMP PING, SSH, HTTP, HTTPS, RDP. b) wykrycie pracujących urządzeń w oparciu o analizę wszystkich dostępnych otwartych portów sieciowych. c) Pozwala na konfigurację parametrów skanowania takich jak: a. zakres przeszukiwanych portów (osobne wartości dla TCP i UDP)

	b. wydajność skanowania (6 poziomów), c. liczbę jednoczesnych wątków skanowania (1,2,4,8,16,24,32) d. możliwość wykrycia wersji systemu operacyjnego. d) konfigurację harmonogramu uruchamiania skanu (np. dziennie, tygodniowo, w określony dzień miesiąca, kwartalnie oraz wskazanie godziny rozpoczęcia skanowania) e) określenia maksymalnej ilości wykonanych skanowań (1-100) lub bez ograniczenia. f) konfigurację wysyłania powiadomień na wskazane adresy e-mail g) powiadomienia dotyczyć mogą: informacji o rozpoczęciu skanowania, jego zakończeniu, zmiany ilości hostów w stosunku do poprzedniego skanowania, zmiany ilości portów w stosunku do poprzedniego skanowania. 23. Konsola zarządzająca umożliwia podgląd listy skonfigurowanych skanów wykrywających dostępne hosty w sieci, wraz z informacją o zmianach w stosunku do ostatniego przeprowadzonego skanu. 24. Widok listy dostępnych skanowań wykrywających obiekty pozwala na zaawansowane filtrowanie. 25. Konsola pozwala na uruchomienie z poziomu listy dostępnych skanowań, wskazanego skanowania wykrywającego obiekty na żądanie z pominięciem harmonogramu. 26. Trwające zadanie skanowania w poszukiwaniu obiektów może zostać przerwane na żądanie. 27. Konsola zarządzania umożliwia eksport wyniku skanu wykrywającego dostępne urządzenia w sieci do pliku XLSX oraz XML. 28. Rozwiązanie umożliwia uruchomienie skanowania wykrywającego znane podatności bezpieczeństwa na urządzeniach sieciowych. 29. Skan wykrywający znane podatności bezpieczeństwa na urządzeniach sieciowych umożliwia: a) określenie skanowanego celu za pomocą adresu IP, oraz grupy celów za pomocą adresu podsieci IP. b) masowe wprowadzenie listy skanowanych celów (adresów IP), za pomocą ustrukturyzowanego pliku z rozszerzeniem CSV. c) konfigurację parametrów skanowania, takich jak: a. zakres skanowanych portów sieciowych TCP/UDP, b. parametr wydajności skanowania (6 poziomów) c. rodzaj uwierzytelniania na skanowanej stacji. d) konfigurację harmonogramu uruchamiania skanu: dziennie, tygodniowo, w określony dzień miesiąca, oraz wskazanie godziny rozpoczęcia. e) konfigurację wysyłania powiadomień na wskazane adresy e-mail informujących o momencie rozpoczęcia skanowania oraz jego zakończeniu. 30. W przypadku tworzonego zadania skanowania administrator posiada możliwość określenia czy do celu skanowania mają zostać wykorzystane wszystkie dostępne pluginy skanujące, tylko wybrane, wszystkie pluginy poza wskazanymi. 31. Administrator posiada możliwość podglądu dostępnych pluginów skanujących podatności i przeszukiwania ich listy. 32. Konsola zarządzania umożliwia podgląd listy skonfigurowanych skanów wykrywających znane podatności bezpieczeństwa. 33. Konsola pozwala na uruchomienie i zatrzymanie skanowania w poszukiwaniu znanych podatności na żądanie. 34. Konsola zarządzania umożliwia eksport wyniku skanu wykrywającego znane podatności bezpieczeństwa do pliku docx i xml 35. Dla danego hosta widoczne są wyniki skanowania w poszukiwaniu podatności. 36. Wyniki zawierają listę wykrytych podatności wraz z poziomem ich krytyczności 37. Dla danej wykrytej podatności dostępny jest: jej opis, poziom krytyczności w oparciu o punktację CVSS, datę wykrycia, wersję pluginu który wykrył podatność, sugestię rozwiązania (jeśli jest dostępna), informację o publicznie dostępnym exploicie (jeśli jest dostępna), zewnętrzne referencje (jeśli są dostępne).

	38. Dla wybranych przez administratora wykrytych podatności, w celu ich obsługi istnieje możliwość stworzenia zgłoszenia we wbudowanym w rozwiązanie systemie zgłoszeń. 39. Podczas tworzenia zgłoszenia administrator ma możliwość określenia: nazwy zgłoszenia, wskazania konta osoby, do której zgłoszenie zostanie przypisane, priorytetu, tzw. „dedline" do którego zgłoszenie powinno zostać rozwiązane, dodatkowego opisu. 40. Lista wszystkich stworzonych zgłoszeń wraz z ich statusem widoczna jest z poziomu konsoli zarządzającej. 41. Administrator posiada możliwość sortowania oraz filtrowania stworzonych zgłoszeń. 42. Osoba, dla której zostało przypisane zgłoszenie ma możliwość dodawania komentarzy, w celu informowania o etapach procesu rozwiązywania zgłoszenia. 43. Dla zgłoszenia istnieje możliwość zmiany jego statusu. 44. Rozwiązanie umożliwia uruchomienie skanu wykrywającego luki bezpieczeństwa w aplikacjach webowych. 45. Skanowanie wykrywające luki bezpieczeństwa w aplikacjach webowych umożliwia: a) określenie skanowanego celu za pomocą adresu URL. b) konfigurację parametrów skanowania takich jak: a. rodzaje testowanych ataków, b. wyjątki ze skanowania (adresy URL omijane podczas testowania aplikacji web), c. parametr wydajności skanowania (ilość jednoczesnych zapytań przesyłanych do skanowanej aplikacji). c) konfigurację uwierzytelniania w testowanej aplikacji web. d) konfigurację harmonogramu uruchamiania skanowania: dziennie, tygodniowo, w określony dzień miesiąca, oraz wskazanie godziny rozpoczęcia skanowania. e) konfigurację wysyłania powiadomień na wskazany adres e-mail informujących o momencie rozpoczęcia skanowania oraz jego zakończeniu. 46. Konsola zarządzania umożliwia podgląd listy skonfigurowanych skanów wykrywających luki w aplikacjach webowych 47. Rozwiązanie umożliwia skorzystanie z narzędzia do identyfikacji zasobów informatycznych dostępnych z publicznej sieci Internet. 48. Narzędzie do identyfikacji zasobów informatycznych dostępnych z publicznej sieci Internet umożliwia: a) przeszukiwanie adresów internetowych, skatalogowanych przez automatyczne systemy producenta, spełniających wskazane warunki wyszukiwania. b) zapisywanie wskazanych warunków wyszukiwania jako szablony. c) podgląd listy wyników wyszukiwania z informacją o wykrytym adresie IP, nazwie oraz słowach kluczowych. d) dodanie wybranych wyników wyszukiwania do grupy skanowania podatności bezpieczeństwa. 49. Rozwiązanie umożliwia podgląd listy wszystkich wykrytych podatności bezpieczeństwa z wszystkich przeprowadzonych skanowań. 50. Lista wszystkich wykrytych podatności musi umożliwiać: a) filtrowanie podatności ze względu na ich rodzaj, przypisany znacznik (tag), urządzenie sieciowe na którym została znaleziona podatność, stopień zagrożenia, status jego naprawy. b) wyświetlenie szczegółów poszczególnych podatności bezpieczeństwa wraz z informacjami na jakich urządzeniach sieciowych dana podatność została wykryta. c) eksport listy urządzeń na których została wykryta dana podatność bezpieczeństwa do pliku CSV. 51. Rozwiązanie umożliwia utworzenie nowego raportu podsumowującego. 52. Rozwiązanie umożliwia podgląd listy wygenerowanych raportów 53. Raport podsumowujący umożliwia: a) konfigurację szablonu jaki będzie wykorzystany do przygotowania raportu, b) wybranie grup urządzeń, które będą znajdowały się w raporcie, c) wybranie poszczególnych statusów oraz poziomu zagrożenia podatności, które będą znajdowały się w raporcie, d) Utworzenie harmonogramu generowania raportu

	e) Wskazanie adresu email na który zostanie wysłany link udostępniający wygenerowany raport, wraz z określeniem czasu ważności linku 54. Lista wygenerowanych raportów musi umożliwiać: a) Wygenerowanie raportu na żądanie b) eksport wyniku raportu do pliku XML(pogrupowany hostami), DOCX(pogrupowany hostami lub wykrytymi podatnościami lub podsumowujący), XLSX (pogrupowany wykrytymi podatnościami) 55. Administrator ma możliwość określenia: strefy czasowej dla swojej organizacji, długości przetrzymywania raportów (miesiąc, kwartał, pół roku, rok, 2 lata) 56. Dostęp do konsoli może być ograniczony na podstawie adresów IP lub ich zakresu.
Moduł sztucznej inteligencji (GenAI) do zarządzania incydentami oraz rozszerzone usługi wsparcia technicznego	• Monitorowanie krytycznych wykryć skanera podatności oraz modułów EDR/XDR przez certyfikowanych ekspertów producenta oprogramowania • Walidacja i dochodzenie czy wykrycia są prawdziwe oraz czy wymagają natychmiastowej akcji by zatrzymać incydent, bądź czy są fałszywymi wykryciami • Eskalacja incydentu do adekwatnego reprezentanta klienta mającego możliwość i autorytet aby odpowiedzieć na incydent • Porada ekspertów jak zatrzymać i naprawić incydent – na przykład, rekomendując izolację systemów bądź zatrzymanie złośliwych procesów • Przygotowywanie raportów dla klienta wraz z sugestiami rozwiązań. Zawartość raportu : Szczegóły raportu, Przegląd podatności, Podsumowanie podatności, Lista podatności (według podatności i hosta) z opcjami Wglądu, Podsumowania, Wykrywania, Odniesień i Ograniczenia tekstu do 500 znaków. Filtrowanie: Selektywne raportowanie podatności (pełne i niestandardowe) i wykluczenia, Uwzględnione systemy operacyjne, Filtry zasobów, Filtry podatności Możliwość tworzenia "raportów skróconych" wysyłanych w sposób podsumowujący. Częstotliwość raportów w trybie miesięcznym (minimum raz w miesiącu). Raporty dostarczane kanałem e-mail lub w inny bezpieczny sposób komunikacji ustalony z Zamawiającym. System musi zawierać zaawansowany moduł wykorzystujący generatywną sztuczną inteligencję (GenAI) do wspierania zespołów IT i cyberbezpieczeństwa w zarządzaniu incydentami bezpieczeństwa. Integruje się z platformami chmurowymi, oferując funkcjonalności związane z analizą zagrożeń, raportowaniem oraz asystowaniem w dochodzeniach bezpieczeństwa. 2. Kluczowe funkcjonalności 2.1. Asystent dochodzeniowy • Analizuje wykrycia w szerokim kontekście, integrując dane z różnych źródeł. • Dostarcza czytelne raporty i rekomendacje w języku użytkownika. • Integruje informacje zewnętrzne o zagrożeniach w czasie rzeczywistym. • Automatyzuje proces analizy incydentów, skracając czas reakcji zespołu bezpieczeństwa. 2.2. Asystent świadomości bezpieczeństwa • Generuje cotygodniowe raporty dotyczące zdarzeń bezpieczeństwa. • Raporty zawierają podsumowanie incydentów i zalecane działania. • Zapewnia interaktywny dostęp do szczegółowych danych, umożliwiając szybką weryfikację zagrożeń. • Obsługuje wielojęzyczność, dostarczając raporty w lokalnym języku użytkownika. 3. Wymagania przetargowe 3.1. Integracja i kompatybilność • System musi być w pełni zintegrowany z platformą chmurową. • Powinien umożliwiać automatyczne zbieranie, analizowanie i raportowanie zdarzeń. • Musi wspierać wieloplatformowe środowiska IT, w tym systemy Windows, macOS oraz Linux. 3.2. Wymagania dotyczące AI • System powinien wykorzystywać generatywną sztuczną inteligencję do analizy zagrożeń.

	• Musi zapewniać predefiniowane opcje podpowiedzi minimalizujące ryzyko błędnych rekomendacji. • Powinien umożliwiać uczenie maszynowe na podstawie wcześniejszych incydentów w celu optymalizacji przyszłych działań. 3.3. Bezpieczeństwo danych i prywatność • Dane użytkowników nie mogą być wykorzystywane do trenowania modeli AI poza organizacją. • System musi działać zgodnie z RODO (GDPR) i posiadać mechanizmy ochrony prywatności. • Dostęp do danych musi być regulowany poprzez mechanizmy autoryzacji i kontroli dostępu. 3.4. Raportowanie i analiza • System powinien generować automatyczne raporty w formacie tekstowym i wizualnym. • Raporty powinny obejmować historię incydentów oraz rekomendacje działań naprawczych. • Powinien umożliwiać eksport danych do systemów SIEM oraz integrację z innymi narzędziami analitycznymi.
Certyfikaty i standardy – dokumenty załączyć wraz z ofertą lub na wezwanie Zamawiającego	System musi posiadać normy i certyfikaty: • OPSWAT (dla EDR/XDR na poziomie min. Platinium), • AV-TEST (ochrona w 2023 na poziomie min.6) • Rozwiązanie wyróżnione przez AV-Test jako "najlepszy wykonawca" w testach Advanced EDR Test 2024 na podstawie scenariuszy cyberataków - APT18, TA577, Turla i FIN6 • producent systemu lub autoryzowany dystrybutor producenta musi posiadać certyfikat ISO 9001 oraz 27001 oraz usługi związane z cyberbezpieczeństwem. • Producent systemu lub autoryzowany dystrybutor producenta musi posiadać certyfikację ISAE 3000 assurance-based SOC 2 Type 2, potwierdzającymi zaawansowane zarządzanie bezpieczeństwem informacji • Producent systemu lub autoryzowany dystrybutor producenta musi być aktywnym członkiem Cloud Security Alliance, co podkreśla zaangażowanie w rozwój najlepszych praktyk dla cybernetyncznych środowisk chmurowych. • Zespół reagowania na incydenty od producenta systemu lub autoryzowany dystrybutor producenta musi posiadać certyfikację CREST i NCSC, które potwierdzają zdolność do skutecznego reagowania na zagrożenia cybernetyczne. • Producent lub oferowany produkt/rozwiązanie musi być uznane za lidera (np. "Champion" w raportach Software Reviews Emotional Footprint) w co najmniej jednej kategorii, takich jak zarządzanie punktami końcowymi (Endpoint Management) lub zarządzanie podatnościami (Vulnerability Management).
Rozszerzone wsparcie serwisowe	System jest objęty rozszerzonym wsparciem technicznym gwarantującym czas reakcji wsparcia technicznego do 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres [**24**] miesięcy. System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie: • Wsparcie telefoniczne zespołu certyfikowanych inżynierów. • Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu. • Doradztwo w zakresie konfiguracji. • Zdalne wsparcie techniczne. • Pomoc w zakładaniu zgłoszeń serwisowych u producenta. • Przygotowanie do zdalnej konfiguracji. • Zdalna konfiguracja (połączenia szyfrowane) zgodnie z wymaganiami użytkownika. • Minimum 5 zdalnych rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań użytkownika. • Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.

	• Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich. **Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 oraz 27001 w zakresie świadczenia usług wsparcia technicznego oraz usług związanych z cyberbezpieczeństwem. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7.** Oferent winien przedłożyć dokumenty: •Oświadczanie Producenta lub Autoryzowanego Dystrybutora producenta świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). **(dołączyć do oferty).** •Certyfikat ISO 9001 oraz 27001 autoryzowanego podmiotu serwisującego. **(dołączyć do oferty).** • Certyfikat inżynierski potwierdzony przez Producenta dla min. dwóch osób w zakresie produktów: EDR/XDR oraz skaner podatności **(dołączyć do oferty).** • Certyfikat potwierdzający posiadany status partnerski, potwierdzony przez Producenta rozwiązania. **(dołączyć do oferty).**

3. Oprogramowanie do zarządzania zasobami IT

Zamawiający oczekuje dostawy 35 licencji oprogramowania w formie bezterminowej z serwisem i wsparciem na 12 miesiące, zgodnego z poniższą specyfikacją

1. Oprogramowanie posiada budowę modułową, składa się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Komunikacja pomiędzy Serwerem a Agentami i Konsolami nawiązywana jest przy użyciu szyfrowanego protokołu TLS 1.2. Program umożliwia zmianę portu komunikacyjnego wykorzystywanego przez konsolą zarządzającą.
2. Moduły umożliwiają kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem. Program wykorzystuje darmowy silnik bazy danych z kodem źródłowym dostępnym na licencji open-source (PostgreSQL w wersji 12) dzięki czemu nie jest objęty limitem ilości danych, baza danych jest rozwiązaniem darmowym niewymagającym dodatkowego licencjonowania. Instalacja Serwera oraz Konsol zarządzających wymaga 64-bitowego systemu operacyjnego Windows.
3. Dane, które dotyczą działań pracownika na komputerze, a więc: historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., są odseparowane od danych stricte technicznych tj. informacji o stacji roboczej. Są one również grupowane w osobnym, dedykowanym oknie. Pozwala to na, zgodne z RODO, usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej.
4. Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, objęty jest kontrolą na poziomie wybranych Administratorów – w programie można nadawać kontom administracyjnym różne poziomy dostępu oraz uprawnień zarówno do funkcji Programu, grup urządzeń, jak i użytkowników. Główny Administrator ma możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną np. może wyłączyć możliwość zdalnej deinstalacji Agenta, ograniczyć dostęp do Opcji programu oraz logów działań innych administratorów. Działania administratorów są logowane oznacza to, że program posiada dziennik z listą czynności wykonanych przez administratorów, które zmodyfikowały obiekty znajdujące się w systemie w tym m.in. logowanie dostępu do Opcji programu, logowanie dostępu do informacji o aktywności użytkownika, logowanie poleceń deinstalacji Agenta. Działania administratorów mogą być automatycznie eksportowane do zewnętrznego kolektora Syslog. Lista kont użytkowników, w tym administratorów, może być synchronizowana z Active Directory, również przez szyfrowane połączenie LDAPS.
5. Program umożliwia konfigurację polityki haseł do lokalnych kont użytkowników konsoli. Polityk pozawala na określenie: minimalnej długości hasła, liter, cyfr, znaków specjalnych oraz automatycznie wymusza dostosowanie bieżących haseł do obowiązujących zasad.
6. Program zawiera mechanizmy uwierzytelniania logowań administratorów do konsoli z wykorzystaniem weryfikacji dwuskładnikowej (MFA). Kod autoryzacyjny może być wysyłany za pomocą e-mail i/lub SMS. W weryfikacji MFA można

skonfigurować okres, po którym należy ponownie zautoryzować logowanie. W przypadku awarii autoryzacja logowania może być pominięta tylko w lokalnej konsoli serwera.

7. Producent został wyróżniony znakiem jakości CYBERSECURITY MADE IN EUROPE przyznawanym przez Europejską Organizację ds. Cyberbezpieczeństwa (ECSO).

1. **MONITOROWANIE INFRASTRUKTURY (BEZAGENTOWO)** obejmuje serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:
   - wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping
   - wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją OU)
   - wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci
   - wizualizacji urządzeń na mapach z funkcją siatki umożliwiającej korygowanie pozycji ikon na mapie do najbliższej linii siatki
   - wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła.
   - wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku
   - wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach o dowolnym rozmiarze i kolorze
   - wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie
   - wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny
   - zablokowania mapy urządzeń przed przypadkową edycją
   - serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów
   - serwerów pocztowych:
     - program monitoruje czas logowania do serwisu odbierającego oraz czas wysyłania poczty
     - program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem)
     - program ma możliwość wykonywania operacji testowych
     - program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa
   - monitorowania serwerów WWW i adresów URL
   - cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS
   - obsługi szyfrowania SSL/TLS w powiadomieniach e-mail
   - obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID
   - obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych
   - monitoringu routerów i przełączników wg:
     - zmian stanu interfejsów sieciowych
     - ruchu sieciowego
     - podłączonych stacji roboczych – graficzna prezentacja panelu switcha
     - ruchu generowanego przez podłączone do portów stacje robocze
   - serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie
   - wyświetlania statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu
   - monitorowania stanu maszyn wirtualnych Vmware: działa, nie działa, wstrzymano
   - zarządzania stanem maszyn wirtualnych Vmware: wysyłanie poleceń włączenia, wstrzymania i wyłączenia zasilania do każdej maszyny
   - wydajności systemów Windows:
     - obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy

2. Program posiada Inteligentne Mapy i Oddziały, które służą do lepszego zarządzania logiczną strukturą urządzeń w przedsiębiorstwie (Oddziały) oraz tworzą dynamiczne mapy wg własnych filtrów (Mapy Inteligentne). Kryteria automatycznego filtrowania dotyczyć mogą m.in. statusu Agenta, wygenerowanych alarmów, zainstalowanych aplikacji, przynależności do oddziału, serwisów sieciowych, danych z SNMP, danych z inwentaryzacji urządzenia itp. Program posiada również funkcję kompilatora plików MIB, który umożliwia dodawanie definicji dla modułów SNMP.
3. Program umożliwia również nakładanie na urządzenia liczników wydajności WMI oraz SNMP wg szablonów definiowanie alarmów z wykorzystaniem akcji związanych ze zdarzeniami w systemie, m.in.: wysłanie komunikatu pulpitowego, wysłanie wiadomości e-mail, wysłanie SMS, wysłanie wiadomości SMS poprzez integrację z serwisem smsapi.pl, wysłanie wiadomości przez Microsoft Teams oraz Slack, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi Windows, wyłączenie/restart komputera. Alarmy budowane są przez administratora z wykorzystaniem ciągu przyczynowo skutkowego – oznacza to, że administrator samodzielnie może wskazać dowolne zdarzenie z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie. Wykonywanie akcji alarmów można skonfigurować automatycznie po wykryciu zdarzenia, z opóźnieniem, na końcu zdarzenia oraz cyklicznie np. co 5 minut. Dla akcji można nałożyć ograniczenie czasowe np. nie wykonuj między 8:00-16:00. Alarmy pozwalają na priorytetyzację urządzeń, grupowanie wg. ważności i typu urządzenia. Oprogramowanie umożliwia wykorzystanie w alarmowaniu skrzynek e-mail z wykorzystaniem autoryzacji OAuth 2.0
4. Program ma możliwość integracji ze sprzętową bramką GSM w celu wysyłania powiadomień SMS z wykorzystaniem protokołu netGSM (SOAP).

WZAKRESIE INWENTARYZACJI program automatycznie gromadzi informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz:

- Prezentuje szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.
- Umożliwia odczyt parametrów S.M.A.R.T. dysków twardych, dysków SSD, w tym NVMe.
- Obejmuje m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.
- Informuje o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio
- umożliwia audytowanie i weryfikację użytkowania licencji w organizacji.
- Zbiera informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.
- Posiada możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania
- programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera.
- Umożliwia odczytanie numeru seryjnego (klucze licencyjne).
- Umożliwia automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.
- Umożliwia przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych
- środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.
- Umożliwia utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu).
- Umożliwia wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji są logowane.

Moduł inwentaryzacji zasobów umożliwia prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania:

- przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji,

- przydzielania dostępu administratorów do zasobów na podstawie praw do oddziałów,
- tworzenia powiązań między zasobami a urządzeniami,
- tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych,
- wskazania osób uprawnionych do użycia zasobów poprzez rozbudowane mechanizmy,
- definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz,
- określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów,
- określenia atrybutów dodatkowych tylko dla wybranych typów zasobów,
- masową edycję atrybutów zasobów,
- definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie,
- importu danych z zewnętrznego źródła (.CSV),
- przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp.,
- tworzenia powiązań między zasobami a dokumentami w relacji 1:N,
- oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp.,
- ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności,
- generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania,
- przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji,
- konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca,
- konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca,
- archiwizacji i porównywania audytów zasobów,
- tworzenia kodów kreskowych dla zasobów,
- drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy,
- inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet,
- możliwość zmiany portu komunikacyjnego wykorzystywanego przez aplikację mobilną dla systemu Android,
- inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline),
- definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja”).

Inwentaryzacja oprogramowania zapewnia funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:

1. Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP.
2. Informacje o aplikacjach używanych w organizacji.
3. Tworzenie własnych wzorców aplikacji.
4. Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.
5. Informacje o komputerach, na których aplikacja została wykryta.
6. Zarządzanie posiadanymi licencjami.
7. Wskazywanie osób odpowiedzialnych za licencję.
8. Wskazanie użytkowników licencji.

9. Tworzenia powiązań między licencjami a dokumentami w relacji 1:N.
10. Rozbudowane i konfigurowalne scenariusze zarządzania licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu.
11. Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych.
12. Zarządzanie posiadanymi licencjami: raport zgodności licencji.
13. Możliwość przypisania do programów numerów seryjnych, wartości itp.

Okna audytowe posiadają możliwość filtrowania elementów per oddział.

W ZAKRESIE OBSŁUGI UŻYTKOWNIKÓW program umożliwia monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie:

- Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy),
- Procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach,
- Rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność,
- Informacji o edytowanych przez użytkownika dokumentach,
- Historii pracy (cykliczne zrzuty ekranowe),
- Listy odwiedzanych stron WWW (tytuły, adresy, liczba i czas wizyt),
- Transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika),
- Wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program ma możliwość monitorowania kosztów wydruków,
- Nagłówków przesyłanej w aplikacjach klienckich poczty e-mail.

Program ponadto posiada możliwość:

- wykrywania podejrzanej aktywności przez popularne „jigglery", mającej na celu symulowanie faktycznej pracy.
- zdefiniowania czasu (min. 15 minut) gdy wykrywana będzie symulowana aktywność wyłącznie przez ruch myszą bez kliknięcia lub wprowadzanie tego samego znaku z klawiatury.
- wyszczególnienia podejrzanej aktywności w raportach.
- wygenerowania alarmu i wykonania akcji po wykryciu podejrzanej aktywności.
- automatycznego włączenia zapisywania zrzutów ekranowych po wykryciu podejrzanej aktywności.
- blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. *.domena.pl). Reguły w postaci listy domen tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane lub współdzielone pomiędzy grupami lub kontami.
- integracji list stron w formie plików .TXT z dowolnego adresu zewnętrznego np. CERT.
- skorzystania z wbudowanej listy stron sklasyfikowanych jako zagrożenia.
- automatycznego odświeżania list stron zintegrowanych z adresów zewnętrznych.
- blokowania ruchu na wskazanych portach TCP/IP,
- blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem,
- prowadzenia rejestru naruszeń blokad,

- wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia, naruszy skonfigurowane blokady,
- przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika),
- definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone.

Możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie.
Mechanizm blokowania uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku. Reguły w postaci listy blokowanych plików lub lokalizacji tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami.
Program posiada Grupy użytkowników oraz Grupy Inteligentne, które służą do lepszego zarządzania użytkownikami, polityką monitorowania oraz blokowania aplikacji i stron internetowych.

PROGRAM UMOŻLIWIA REALIZACJĘ ZDALNEJ POMOCY UŻYTKOWNIKOM. W ramach kontroli stacji użytkownika dostępny jest podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połącznie i opcją odrzucenia takiego połącznia przez użytkownika (np. w przypadku pracowników wysokiego szczebla). Podczas dostępu zdalnego, zarówno użytkownik jak i administrator widzą ten sam ekran. Administrator w trakcie zdalnego dostępu ma możliwość wyboru dowolnego ekranu (monitora) oraz zablokowania działania myszy oraz klawiatury dla użytkownika. Funkcja zdalnego dostępu umożliwia równoczesne podłączenie do tego samego komputera kilku administratorom.

W niniejszym module znajduje się baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych poprzez dedykowany portal oraz przetwarzanie wiadomości e-mail, które są przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie. Oprogramowanie pozwala na integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0. Moduł umożliwia również przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o sygnalistach") oraz zawiera dokumenty prawne dot. ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę. Kolejną ważną funkcjonalnością jest umożliwienie użytkownikom monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron. System umożliwia użycie pośredniego statusu „zgłoszenie rozwiązane" przed ostatecznym zamknięciem zgłoszenia.

Moduł ten zawiera również komunikator (czat), który umożliwia prowadzenie rozmów w czasie rzeczywistym oraz archiwizację historii wiadomości pomiędzy zalogowanymi użytkownikami, pracownikami pomocy technicznej i administratorami (wraz z wyszukiwarką rozmów i wiadomości wg słów kluczowych oraz automatycznym oczyszczaniem historii rozmów). Ponadto czat pozwala na:

- zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej
- rozmowy również między „zwykłymi" użytkownikami
- przesyłanie plików między rozmówcami w trybie online
- tworzenie pokojów tematycznych, rozmów grupowych
- oznaczanie kontaktów jako „ulubionych" na liście kontaktów
- uruchomienie z poziomu ikony dostępowej Agenta oraz bezpośrednio w interfejsie WWW heldpesku
- może być wyświetlany w trybie jasnym lub ciemnym

W module zawarta jest również baza wiedzy pomagająca użytkownikom samodzielnie rozwiązywać

najprostsze, powtarzające się problemy wraz z możliwością nadawania artykułom 1 z 3 statusów (opublikowany, wewnętrzny, szkic). Program umożliwia informowanie pracowników o zdarzeniach, np. planowanych przestojach w dostępie do usług, przez komunikaty z graficznym formatowaniem treści oraz łączami do artykułów w bazie wiedzy. Użytkownik ma możliwość przeglądnięcia historii odczytanych komunikatów bezpośrednio z poziomu ikony Agenta. Administrator ma możliwość tworzenia szkiców i archiwizowania komunikatów.

Dostęp do systemu zgłoszeń oraz bazy wiedzy realizowany jest przez dedykowany portal dostępny przez przeglądarkę internetową, który może być wyświetlany w trybie jasnym lub ciemnym.

Funkcjonalność modułu umożliwia również uzyskanie dostępu z prywatnego komputera tylko do swojego komputera firmowego, który pozostał w organizacji, za pomocą funkcji zdalnego dostępu przez każdego pracownika.

Moduł pomocy zdalnej umożliwia również:

1. pobieranie listy użytkowników z Active Directory,
2. wyświetlanie w systemie zgłoszeń wizytówki użytkownika wraz z jego numerem telefonu, adresem e-mail oraz informacją o przełożonym,
3. zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont,
4. zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez rozbudowany system zarządzania regułami widoczności zgłoszeń,
5. zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii zgłoszeń,
6. zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii artykułów bazy wiedzy,
7. tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO,
8. automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników,
9. definiowanie ścieżek akceptacji zgłoszeń – procesu, w którym użytkownik uzyskuje akceptację na realizację zgłoszenia od wyznaczonych osób w organizacji,
10. przypisywanie ścieżek akceptacji zgłoszeń do określonych kategorii,
11. procesowanie zgłoszeń użytkowników z wiadomości e-mail,
12. eksportowania listy zgłoszeń do plików CSV i XLSX,
13. integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0,
14. tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń,
15. wykonywanie operacji na wielu zgłoszeniach równocześnie,
16. dołączanie załączników do zgłoszeń,
17. rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy,
18. szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników,
19. wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia,
20. zrzuty ekranowe (podgląd pulpitu),
21. zdalną modyfikację rejestrów,
22. dystrybucję oprogramowania przez Agenty,
23. definiowanie aplikacji dozwolonych do samodzielnej instalacji przez użytkowników z pakietów MSI w postaci Kiosku z Aplikacjami,
24. przypisywanie dostępnych w Kiosku instalatorów do grup użytkowników,
25. dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI),

26. zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku,
27. możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu,
28. możliwość skonfigurowania automatyzacji dodających komentarze publiczne wraz z załącznikami i odnośnikami do artykułów w Bazie Wiedzy,
29. planowanie nieobecności pracowników helpdesk,
30. obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem,
31. generowanie raportów obsługi helpdesk,
32. zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu),
33. zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami),
34. wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików bez blokowania interfejsu programu podczas przesyłania plików.

Kolejną funkcją oprogramowania jest **MOŻLIWOŚĆ OCHRONY DANYCH PRZED WYCIEKIEM** poprzez blokowanie urządzeń.

1. Blokowanie urządzeń i nośników danych. Program ma możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny.
2. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek.
3. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.
4. Blokownie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane.
5. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych.
6. Funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender.
7. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker.
8. Funkcje wspierające bezpieczeństwo systemu: zdalne szyfrowanie dysków za pomocą BitLocker.
9. Funkcje wspierające bezpieczeństwo systemu: zapisywanie klucza odzyskiwania do pliku oraz jako zasób w bazie danych programu.
10. Funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu.
11. Funkcje wspierające bezpieczeństwo systemu: odczytanie informacji o aktywnym oprogramowaniu antywirusowym firm trzecich, innym niż Windows Defender.
12. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM.

Zarządzanie prawami dostępu do urządzeń:

1. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.
2. Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive'ów, dysków itp. - urządzenia prywatne są blokowane.
3. Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników.
4. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci.
5. Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane.

Audyt operacji na plikach na urządzeniach przenośnych:

1. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.
2. Podłączenie/odłączenie urządzenia przenośnego.

Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika.

Definiowanie reguł monitorowanych folderów w postaci list.

Monitorowanie operacji na plikach na udostępnionych zasobach sieciowych (udziałach) na urządzeniach nieobsługiwanych przez Agenta (np. macierze, NAS itp.)

Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. Przydzielanie uprawnień również do kont użytkowników lokalnych.

Program umożliwia prowadzenie rejestru naruszeń blokad podłączanych nośników.

Wdrożenie

Przedmiotem wdrożenia systemu monitorowania i zarządzania infrastrukturą IT obejmującego instalację, konfigurację i uruchomienie oprogramowania wraz z agentami na wskazanych stacjach roboczych. W ramach realizacji należy skonfigurować bezpieczny dostęp administracyjny, politykę retencji danych, automatyczne kopie zapasowe oraz zasady monitorowania zasobów sieciowych i systemowych. Wykonawca zobowiązany jest do przeprowadzenia skanowania i klasyfikacji urządzeń sieciowych, opracowania map logicznych sieci oraz wdrożenia polityk alarmowych. W dalszym etapie należy skonfigurować inwentaryzację sprzętu i oprogramowania, uruchomić mechanizmy powiadamiania o zmianach konfiguracji, ustalić zasady klasyfikacji i aktualizacji aplikacji, a także wdrożyć polityki monitorowania aktywności użytkowników, zarządzania dostępem do danych i kontroli nośników wymiennych. Całość zostanie zintegrowana w centralnym panelu administracyjnym, który umożliwi monitorowanie stanu infrastruktury, aktywności użytkowników i wydajności systemu. Wymaga się, aby wdrożenie było przeprowadzone przez producenta lub autoryzowanego dystrybutora oferowanego rozwiązania.

4. Serwer do cyberbezpieczeństwa na potrzeby HA – 1 szt.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	• Obudowa Rack o wysokości max 1U • 8 slotów na dyski 2.5” • Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, umożliwiający jednoznacznie stwierdzić, czy system działa poprawnie i pokazujący podstawowe stany działania serwera w tym adres IP karty zarządzającej.
Płyta główna	• Płyta główna z możliwością zainstalowania jednego procesora. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Płyta powinna obsługiwać do min. 128GB, na płycie głównej powinno znajdować się minimum 4 sloty przeznaczone dla pamięci
Chipset	• Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych
Procesor	• Zainstalowany jeden procesor 8-rdzeniowy, 2.7GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku 84.5 w teście SPECrate®2017_int_base w konfiguracji jednoprocesorowej, dostępnym na stronie www.spec.org dla oferowanego serwera.
Pamięć RAM	• 128GB DDR5 UDIMM, 5600MT/s.
Kontroler RAID	• Sprzętowy kontroler dyskowy, posiadający możliwość konfiguracji poziomów RAID: 0, 1, 10
Dyski twarde	• Zainstalowane ○ 5x dysk SSD SATA o pojemności min. 480GB, Hot-Plug. • Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1.
Interfejsy sieciowe/FC/SAS	• Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT

Wbudowane porty	• min. 4 porty USB w tym min:
	  ○ 1 port USB 3.0 z tyłu obudowy,
	  ○ 1 port micro USB z przodu obudowy
	• 1 port VGA na tylnym panelu,
	• 1 port RS232

Karta graficzna	• Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200
Zasilacze	• Redundantne, o mocy maks. 700W klasy Titanium
Elementy montażowe	• Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych • Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.

	• Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 V3 • 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). Wymagane dołączenie do oferty oświadczenia Producenta potwierdzającego spełnienie powyższych zaleceń.
System operacyjny	• Windows Server Standard 2025 – 1 szt.
Karta Zarządzania	• Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca: ○ zdalny dostęp do graficznego interfejsu Web karty zarządzającej ○ 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 SNMP; IPMI2.0, VLAN tagging, SSH ○ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz. ○ możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer ○ integracja z Active Directory ○ możliwość obsługi przez ośmiu administratorów jednocześnie ○ Wsparcie dla automatycznej rejestracji DNS ○ wsparcie dla LLDP ○ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej ○ możliwość podłączenia lokalnego poprzez złącze RS-232. ○ możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy. ○ Monitorowanie zużycia dysków SSD ○ możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi, ○ Automatyczne zgłaszanie alertów do centrum serwisowego producenta ○ Automatyczne update firmware dla wszystkich komponentów serwera ○ Możliwość przywrócenia poprzednich wersji firmware ○ Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON

	○ Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych ○ Automatyczne tworzenie kopii ustawień serwera w opraciu o harmonogram. ○ Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera ○ Serwer musi posiadać możliwość uruchomienia funkcjonalności umożliwiającej 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 lub WIFI. Możliwość rozszerzenia funkcjonalności karty o: ○ możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych narzędzi analitycznych jak Splunk, Grafana, ElasticSearch ○ kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania ○ Automatyczne odświeżanie certyfikatów SSL ○ możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielkoskładnikowego przy logowaniu do karty zarządzającej ○ możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień ○ możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera ○ możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer ○ możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe ○ monitorowanie przepływu powietrza na bieżąco (w CFM)
Oprogramowanie do zarządzania	• Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: ○ Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych ○ integracja z Active Directory ○ Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta ○ Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish ○ Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram ○ Szczegółowy opis wykrytych systemów oraz ich komponentów ○ Możliwość eksportu raportu do CSV, HTML, XLS, PDF ○ Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. ○ Grupowanie urządzeń w oparciu o kryteria użytkownika

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

	▪ wykonać zautomatyzowaną aktualizację firmware serwerów w klastrze Vmware do zdefiniowanej polityki poziomu mikrokodów ▪ wykonać/zweryfikować konfigurację serwera zgodną ze zdefiniowaną polityka konfiguracji ▪ z konsoli vCenter uruchomić zdalną konsolę graficzną serwera (nawet gdy nie jest uruchomiony na serwerze system operacyjny) ▪ inwentaryzacja komponentów w serwerze i ich mikrokodów ▪ historia poboru mocy i temperatury serwera ▪ zbieranie danych diagnostycznych serwera do paczki serwisowej
Oprogramowanie do monitorowania	Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z platformą wirtualizacji VMware. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności: • Monitoring: ○ ilość podłączonych oraz rozłączonych systemów ○ stan podłączonych urządzeń ○ informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów ○ Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia ○ informacje o statusie gwarancji dla poszczególnych urządzeń ○ informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń ○ informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. ○ Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych ○ Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. ○ Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. ○ Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. ○ Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. ○ Monitoring parametrów serwerów z informacją o minimum: ▪ Obciążeniu procesora ▪ Zużyciu pamięci RAM ▪ Temperaturze procesorów ▪ Temperaturze powietrza wlotowego ▪ Zużyciu prądu

	▪ Zmianach w fizycznej konfiguracji serwera ▪ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ○ Monitoring parametrów pamięci masowych z informacją o minimum: ▪ Opóźnieniach ▪ IOPS ▪ Przepustowości ▪ Utylizacji kontrolerów ▪ Pojemność całkowita i dostępna ▪ Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów. ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ▪ Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata ▪ Informacje o poziomie redukcji danych ▪ Informacje o statusie replikacji oraz snapshotów ○ Monitoring parametrów przełączników sieciowych z informacją o minimum: ▪ Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny ▪ Stanie komponentów: zasilacze, wentylatory ▪ Podłączonych hostach ▪ Ilości i statusu portów ▪ Utylizacji procesora ▪ Utylizacji poszczególnych portów ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. • Aktualizacja firmware ○ możliwość aktualizcji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania • Raporty ○ Możliwość generowania raportów dla serwerów zawierających informację o: ▪ Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym

	systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej ▪ Średnim obciążeniu: procesorów, pamięci RAM, IO, ○ Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: ▪ Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji ○ Generowanie raportów do plików CSV i PDF • Cyberbezpieczeństwo ○ Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. ○ Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. ○ Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. ○ Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. • Wspierane urządzenia ○ Urządzenie Producenta dostarczane w ramach postępowania ○ Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) • Wirtualny asystent ○ Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; • Możliwość rozszerzenia funkcjonalności ○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. • Inne ○ Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami. • Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów

	powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver, dla kraju, w którym produkt będzie użytkowany, według normy wprowadzonej w 2019 roku - **Wykonawca złoży dokument potwierdzający spełnianie wymogu.** • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2022, Microsoft Windows Server 2025.
Dokumentacja użytkownika	• Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

Warunki gwarancji	• Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat.
	• Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet.
	• Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.
	• Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.
	• Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki.
	• Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.
	• Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego.
	• Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.
	• Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:
	  ○ Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.
	  ○ Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania

	problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. ○ Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. ○ Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. ○ Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – **dokumenty potwierdzające należy załączyć do oferty.**

5. Zasilacz awaryjny UPS – 1 szt.

L.p.	Nazwa komponentu	Wymagane parametry techniczne
1.	Model, symbol, producent urządzenia	Należy podać w formularzu ofertowym
2.	Technologia	online, VFI-SS-111,
3.	Moc wyjściowa	2kVA/2kW; PF=1
4.	Obudowa	Rack - Zestaw do montażu w szafie rack na wyposażeniu
5.	Napięcie wejściowe	110 ÷ 300 V AC ± 2 %
6.	Napięcie znamionowe (wartość skuteczna)	230V AC
7.	Prąd znamionowy (wejście)	10,7A
8.	Częstotliwość napięcia wejściowego (zakres oraz tolerancja)	45 ÷ 55 / 55 ÷ 65 Hz ± 1 Hz
9.	Częstotliwość znamionowa napięcia wejściowego	50Hz / 60Hz
10.	Zniekształcenia prądu wejściowego THDi	< 5%

11.	Zakres napięcia wyjściowego	200/208/220/230/240V AC konfigurowalne z poziomu oprogramowania oraz z menu zasilacza na wyświetlaczu LCD (domyślnie 230V AC
12.	Zniekształcenia napięcia wyjściowego THDu	< 1% dla Pmax (liniowe) < 5% (nieliniowe wg PN EN 62040-3)
13.	Gniazda wyjściowe	4x IEC320 C13 (10A) sterowalne + 4x IEC320 C13 (10A)
14.	Akumulatory wewnętrzne UPS	Minimum 6szt akumulatorów 12V9Ah
15.	Moduły bateryjne	Opcja – możliwość podpięcia do 4szt modułów (każdy z minimum 12szt akumulatorów 12V9Ah)
16.	Czas podtrzymania z baterii wewnętrznych w UPS dla obciążenia 2kW/1,6kW/1kW	6 / 8,5 / 16 min
17.	Przeciążalność	105-125% - 5min / 125-150% - 30s / >150% - 500ms
18.	EPO	Wymagane – standard NC
19.	Sygnalizacja	akustyczno-diodowa, wyświetlacz LCD oraz diody sygnalizujące usterkę, pracę bateryjną, pracę w trybie online, obejście bypass
20.	Język oprogramowania	polski i angielski do wyboru z poziomu interfejsu użytkownika
21.	Konfiguracja minimalnego poziomu naładowania baterii po powrocie zasilania sieciowego (po rozładowaniu baterii przed ponownym samoczynnym załączeniem zasilania na wyjściu)	Wymagane, konfigurowalne z poziomu oprogramowania (przez USB)
22.	Wymagane certyfikaty	CE, ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisu
23.	Komunikacja z urządzeniem	RS232, USB HID, styki bezpotencjałowe 1-wejście; 1-wyjście; SNMP – wymagana na wyposażeniu
24.	Wymiary UPS (rack) (wys x szer x gł)	Nie więcej niż 86 x 439 x 600 mm
25.	Oprogramowanie do monitorowania pracy zasilacza UPS	Tego samego producenta co UPS, bezpłatne bez ograniczeń funkcjonalności oraz ilości podłączonych stanowisk komputerowych; pod Windows 10, Windows 11, Windows Server 2019, Windows Server 2022, Linux - możliwość pobierania ze strony producenta i dokonywania aktualizacji przez użytkownika bez dodatkowych kosztów

26.	Oprogramowanie - funkcjonalność	możliwość nadawania unikalnych nazw dla kilku tych samych modeli UPS'ów w oprogramowaniu
27.	Oprogramowanie - funkcjonalność	Konfiguracja minimalnego poziomu naładowania baterii. UPS po rozładowaniu baterii przed samoczynnym załączeniem zasilania wyjść (po powrocie zasilania sieciowego) będzie musiał naładować baterie do tego poziomu. Parametr ten ma zastosowanie w przypadku, gdy załączenie zasilania wyjść może nastąpić tylko wtedy, gdy UPS zgromadzi niezbędny zapasa energii na wypadek kolejnego zaniku.
28.	Oprogramowanie - funkcjonalność	Uruchom poprzez Bypass - Aktywacja tej funkcji powoduje, że UPS zawsze przed załączeniem zasilania wyjść na kilka sekund załączy zasilanie poprzez Bypass i po chwili przełączy się w zasilanie wyjść poprzez falownik (normalny tryb pracy). Funkcja ta umożliwia załączenie urządzeń o zwiększonym prądzie rozruchowym bez przeciążania falownika UPS.
29.	Serwis producenta	wymagany, zlokalizowany na terenie Polski, autoryzacja serwisowa lub oświadczenie producenta
30.	Gwarancja	Minimum 24 miesiące elektronika, 24 miesiące akumulatory, serwis door to door, czas naprawy 5 dni roboczych
31.	Dokumentacja	Instrukcja w języku polskim

6. Oprogramowanie do zarządzania systemem bezpieczeństwa informacji – 1 szt. licencji

Oprogramowanie wspomagającego zarządzanie w zakresie bezpieczeństwa informacji i ochrony danych osobowych. Oprogramowanie ma być dostarczone w najnowszej wersji w języku polskim. Oprogramowanie powinno posiadać dokumentację użytkownika opisującą funkcjonalność każdego z modułów oprogramowania oraz dokumentację administratora opisującą sposób administrowania programem w tym jego instalowania, konfiguracji, sposobu tworzenia kopii zapasowych oraz odtwarzania w przypadku awarii,

1. Koszt zakupu oprogramowania powinien uwzględniać koszt wszystkich składników oprogramowania (poza systemem operacyjnym zainstalowanym na serwerze Zamawiającego), które są niezbędne do jego pracy zgodnie z niniejszą specyfikacją.
2. W ramach zamówienia Zamawiający otrzyma wersję instalacyjną oprogramowania oraz licencję uprawniającą do korzystania z przedmiotowego oprogramowania.
3. Program powinien pracować jako aplikacja intranetowa uruchamiana i prawidłowo pracująca w aktualnych wersjach przeglądarek internetowych (MS Edge, Google Chrome, FireFox).
4. Wszystkie dane gromadzone w oprogramowaniu powinny być zapisywane wyłącznie centralnie, na komputerze pełniącym rolę serwera pracującego w trybie ciągłym przez 24 godziny na dobę.
5. Serwer będzie dostarczony przez Zamawiającego i będzie znajdował się w jego siedzibie.
6. Program powinien poprawnie pracować na serwerze z procesorem 8-rdzeniowy w architekturze 64 bit, 1TB SSD, 16GB RAM z zainstalowanym systemem operacyjny Windows lub Linux (inne składniki oprogramowania niezbędne do pracy programu dostarcza Wykonawca).
7. Aplikacja powinna mieć możliwość uruchomienia na serwerze pracującym pod systemem Linux (konfiguracja instalacji niestandardowych powinna być określona w dokumentacji programu).
8. Oprogramowanie musi:

- posiadać rejestr zidentyfikowanych procesów w tym procesów z zakresu ochrony danych,
- posiadać rejestr komórek organizacyjnych, który będzie oparty na regulaminie organizacyjnym,

- posiadać możliwość opisu komórki organizacyjnej poprzez określenie jej podrzędności w strukturze organizacyjnej, przypisania do niej stanowisk pracy oraz zakresu zadań jaki realizuje,
- posiadać rejestr wszystkich pracowników, praktykantów i stażystów oraz osób świadczących pracę na umowach cywilnoprawnych,
- umożliwiać prowadzenie rejestru zidentyfikowanych aktywów informacyjnych oraz zasobów wspomagających,
- wspomagać opisywanie aktywów m.in. poprzez wskazanie procesów przetwarzających informacje oraz istotności informacji dla realizacji danego procesu, wskazanie zasobów wykorzystywanych przy przetwarzaniu informacji oraz określenie poziomu istotności zasobu dla informacji,
- umożliwiać ustalenie wymaganego poziomu podstawowych oraz dodatkowych atrybutów informacji i adekwatnie do tego ustalać klasyfikacje aktywów.
- umożliwiać prowadzenie zgodnie z przepisami prawa rejestru czynności przetwarzania i kategorii czynności przetwarzania danych osobowych w Urzędzie,
- posiadać możliwość rejestrowania klauzul informacyjnych
- posiadać możliwość ewidencji zawartych umów powierzenia przetwarzania danych osobowych,
- wspomagać wystawianie upoważnień do przetwarzania danych osobowych oraz prowadzić rejestr osób upoważnionych do przetwarzania danych osobowych,
- Wspomagać wystawianie uprawnień do systemów informatycznych
- Generować zestawienie uprawnień do systemów informatycznych z kryterium użytkownik lub program.
- posiadać rejestr zidentyfikowanych ryzyk w zakresie m.in. bezpieczeństwa informacji i ochrony danych osobowych,
- posiadać możliwość identyfikacji i ewidencji czynników ryzyka, podatności na zagrożenia lub szanse, opisania skutków ryzyka, estymację i ocenę ryzyka, ustalenia reakcji na ryzyko oraz monitorowania i raportowania ryzyka,
- posiadać możliwość przeprowadzania cyklicznej oceny ryzyka,
- prezentować ryzyka w formie graficznych zestawień m.in. mapy ryzyka,
- posiadać rejestr wszystkich użytkowanych aplikacji,
- posiadać możliwość elektronicznego wnioskowania o nadanie właściwych uprawnień dla pracowników zgodnie z ich zakresem obowiązków do obsługi programów komputerowych,
- posiadać rejestr zaistniałych incydentów oraz słabości systemu,
- wspomagać obsługę incydentów bezpieczeństwa informacji w tym określenia operatora incydentu oraz ewidencjonować podejmowane działania,
- posiadać stosowne zestawienia dotyczące zidentyfikowanych incydentów i słabości systemów,
- posiadać rejestr certyfikatów bezpieczeństwa,
- posiadać możliwość wnioskowania o nadanie certyfikatu bezpieczeństwa,
- umożliwiać ewidencjonowanie certyfikatów bezpieczeństwa,
- posiadać rejestr przeprowadzonych audytów wewnętrznych w tym auditów w zakresie bezpieczeństwa informacji i ochrony danych osobowych,
- posiadać rejestr wszystkich zidentyfikowanych nieprawidłowości (niezgodności) w zakresie bezpieczeństwa informacji i ochrony danych osobowych,
- możliwość określenia działań korygujących i korekcyjnych względem zidentyfikowanej nieprawidłowości oraz głoszenia wykonania działań korygujących,
- posiadać rejestr przeprowadzanych w Urzędzie cyklicznych przeglądów zarządzania w zakresie m.in. bezpieczeństwa informacji i ochrony danych osobowych,
- możliwość automatycznego przygotowania raportu do analizy z zakresu m.in. bezpieczeństwa informacji i ochrony danych osobowych.

9. Wszystkie moduły programu muszą być ze sobą kompatybilne i wzajemnie powiązane (moduły powinny korzystać z danych wprowadzanych w innych modułach bez konieczności ponownego ewidencjonowania tych samych danych).

Licencja

1. Licencja ma zezwalać na jednoczesną pracę w programie wszystkich pracowników Urzędu w formacie licencji wieczystej.
2. Licencja nie może ograniczać liczby końcówek jednocześnie korzystających z oprogramowania.

3. Licencja musi dopuszczać tworzenie przez Zamawiającego dowolnej ilości kopii oprogramowania dla celów testowych lub szkoleniowych.
4. Od dnia przekazania do 30.06.2026 r Wykonawca zapewnia wsparcie, w ramach którego Zamawiający zostanie uprawniony do nieodpłatnego pobierania poprawek i aktualizacji oraz na bieżąco pomocy (nadzoru) w obsłudze programu.
5. Pomoc techniczna powinna być świadczona co najmniej w dni robocze w godzinach pracy Urzędu

Zamawiający wymaga by oprogramowanie było nowe, nieużywane, nieaktywowane wcześniej na innym urządzeniu, dostarczone w najnowszej stabilnej wersji pochodzącej z oficjalnego kanału dystrybucyjnego producenta oprogramowania nieobciążone prawami na rzecz osób trzecich. Dostarczone oprogramowanie i wszelkie jego nośniki (o ile występują) musi być wolne od wad fizycznych i prawnych