



OPIS PRZEDMIOTU ZAMÓWIENIA

„Dostawa oprogramowania oraz monitorów”

– nr postępowania FH/02/10/24

Oferowany przedmiot zamówienia musi spełniać wymagania określone przez Zamawiającego, tj. posiadać parametry i funkcjonalności nie gorsze (co najmniej takie same lub lepsze) od określonych poniżej.

Zamówienie podzielone jest na 11 części. Zamawiający dopuszcza składanie ofert częściowych.

Część nr 1 - Oprogramowanie do nadzorowania 25 sesji uprzywilejowanych

OPOGRAMOWANIE DO NADZOROWANIA SESJI UPRZYWILEJOWANYCH

Opis oprogramowania	Oprogramowanie do nadzorowania sesji uprzywilejowanych
Warunki licencji	<ol style="list-style-type: none">1. Licencja nie może ograniczać ilości użytkowników, których w danym momencie sesje są nadzorowane,2. Licencja powinna umożliwiać nadzorowanie dostęp do co najmniej 25 usług,3. Wsparcie producenta, które obejmuje roczne aktualizacje oraz wsparcie liczone od dnia 31.12.2024.4. Zamawiający posiada u siebie wdrożone rozwiązanie BeyondTrust Privilege Remote Access, zatem zaproponowane licencje mogą tyczyć się przedłużenia działania tego rozwiązania lub całkowicie nowego, równoważnego, spełniające opisywane funkcjonalności wraz z wdrożeniem
Cechy oprogramowania równoważnego	Architektura <ol style="list-style-type: none">1. System musi być dostarczany w formie zamkniętej platformy wirtualnej przygotowanej do implementacji w infrastrukturze. Przez zamkniętą platformę rozumiemy wyspecjalizowane rozwiązanie, w ramach którego zainstalowana jest całość oprogramowania (system operacyjny, baza danych, aplikacja), realizujące funkcjonalności systemu.2. System musi być zaprojektowany i przygotowany

- do umieszczenia w DMZ (hardening producenta).
3. System na potrzeby realizacji swoich funkcji nie może wymagać zestawienia tunelu VPN pomiędzy siecią LAN organizacji, a komputerem zewnętrznego dostawcy. Nie może też wykorzystywać technologii chmurowej do nawiązania połączenia.
 4. System musi umożliwiać tryb pracy awaryjnej zapewniający synchronizację danych między dwoma urządzeniami do uprzywilejowanego dostępu zdalnego, tworząc uproszczony proces bezpiecznej wymiany uszkodzonego urządzenia na zapasowe.
 5. System musi umożliwiać nawiązywanie sesji przynajmniej w dwóch trybach:
 - a) Z wykorzystaniem instalowanego agenta na systemie, do którego będzie nawiązywana sesja,
 - b) Z wykorzystaniem serwerów proxy bez potrzeby instalacji agenta na systemie, do którego będzie nawiązywana sesja.
 6. Serwery proxy (nawiązywanie sesji w sposób bezagentowy) muszą być zarządzane w sposób centralny z poziomu oprogramowania do uprzywilejowanego dostępu zdalnego (konfiguracja minimalnie w zakresie: nadawania uprawnień dostępowych do serwera proxy dla zewnętrznych dostawców, utworzenie serwera proxy, wyłączenie serwera proxy).
 7. Komunikacja między elementami systemu do uprzywilejowanego dostępu zdalnego (tj. oprogramowaniem uprzywilejowanego dostępu zdalnego, agentami instalowanymi na urządzeniach końcowych oraz serwerami proxy) musi być szyfrowana (TLS) i odbywać się na jednym porcie 443.
 8. Elementy systemu (agenci, serwery proxy, klienci) instalowani na zasobach i stacjach roboczych muszą umożliwiać pracę w trybie aktywnego nawiązywania połączenia z systemem uprzywilejowanego dostępu zdalnego, tj. bez pozostawiania otwartych portów nasłuchujących na urządzeniach końcowych.
 9. System musi posiadać wsparcie dla protokołów

SSH, RDP oraz VNC.

10. System musi posiadać możliwość rozbudowy o moduł obsługi sesji do aplikacji WEB (wbudowana przeglądarka WWW).
11. Systemu musi posiadać możliwość uruchomienia sesji aplikacyjnych (uruchomienie wskazanej aplikacji z serwera usług terminalowych lub uruchomienie aplikacji za pomocą dedykowanego agenta)
12. Systemu musi posiadać możliwość tunelowania protokołów TCP na zdefiniowanym porcie między komputerem zewnętrznego dostawcy a zarządzanym systemem.
13. System ma być dostarczony w polskiej wersji językowej (zarówno menu konfiguracyjne systemu jak i interfejs klientów, za pomocą których realizowane są sesje).

Funkcje operacyjne systemu uprzywilejowanego dostępu zdalnego

1. Logowanie do systemu uprzywilejowanego dostępu zdalnego musi odbywać się poprzez konta lokalne (tworzone na poziomie systemu do uprzywilejowanego dostępu zdalnego) lub konta i grupy importowane z Active Directory.
2. Logowanie dostawców zewnętrznych do systemu uprzywilejowanego dostępu zdalnego musi być zabezpieczone drugim składnikiem (2FA).
3. System musi realizować następujące scenariusze nawiązywania sesji przez zewnętrznego dostawcę:
 - a) za pomocą klienta zainstalowanego na komputerze zewnętrznego dostawcy (gruby klient),
 - b) za pomocą przeglądarki WWW z komputera zewnętrznego dostawcy (bez potrzeby instalacji klienta),
 - c) za pomocą klienta zainstalowanego na urządzeniu mobilnym (minimum wsparcie dla systemu Android).
4. System musi umożliwiać opcję zastosowania przez kontraktora własnych klientów RDP i SSH.
5. System musi umożliwiać realizację sesji do stacji roboczych (przynajmniej Windows i Linux) i współdzielenie tej samej sesji między

kontraktorem a operatorem pracującym przy stacji roboczej.

6. Rozpoczęcie sesji współdzielonej między kontraktorem a operatorem stacji roboczej musi podlegać procesowi akceptacji przez operatora stacji roboczej do której realizowana jest ta sesja.
7. Rozpoczęcie sesji przez zewnętrznego dostawcę musi podlegać kontroli dostępu poprzez:
 - a) Wysyłanie powiadomień o zdarzeniu rozpoczęcia i zakończenia sesji przez zewnętrznego dostawcę do zdefiniowanej listy osób,
 - b) Ograniczenie możliwości nawiązywania sesji przez zewnętrznych dostawców do określonych dni i godzin, oraz do określonych grup zasobów.
 - c) Włączenie procesu wnioskowania przez zewnętrznego dostawcę o dostęp do zasobów i mechanizmu akceptacji lub odrzucenia wniosku przez właściciela zasobu. We wniosku muszą znaleźć się przynajmniej zakres dat, kiedy zewnętrzny dostawca będzie nawiązywał sesję oraz pole pozwalające opisać zakres wykonywanych przez niego prac. Wniosek musi być wysyłany w celu akceptacji do zdefiniowanej listy osób.
8. Konsola dostępowa dla zewnętrznego dostawcy musi posiadać co najmniej poniższe funkcje:
 - a) widok grup zasobów z możliwością nawiązania sesji do tych zasobów (za pomocą menu kontekstowego lub podwójnego kliknięcia), oraz możliwością wyszukiwania zasobów po ciągach znaków
 - b) szczegółowy opis zasobu, do którego możliwe jest nawiązanie sesji, zawierający nazwę hosta / adres IP, status (aktywny/nieaktywny), typ systemu operacyjnego, edytowalną nazwę skróconą.
 - c) funkcję wieloosobowego chatu działającą między uczestnikami sesji.
9. System musi umożliwić wyłączenie synchronizacji schowka i kopiowania plików między komputerem

zewnętrznego dostawcy a zarządzanym zasobem.

10. System w trakcie sesji realizowanej przez zewnętrznego dostawcę musi umożliwiać:
 - a) Dołączenie do sesji dodatkowych użytkowników posiadających konta w systemie uprzywilejowanego dostępu zdalnego;
 - b) Dołączenie dodatkowych użytkowników do sesji nieposiadających konta w systemie uprzywilejowanego dostępu zdalnego przy jednoczesnej możliwości nałożenia dodatkowych restrykcji dla takiej osoby (minimum w zakresie odebrania kontroli myszy i klawiatury, automatyczne zakończenie sesji w przypadku braku połączenie autoryzowanego użytkownika ulegnie awarii);
 - c) Przejęcie sesji zewnętrznego dostawcy przez uprawnioną osobę (audytora) i jej zakończenie.

Funkcje raportowania

1. System musi posiadać wbudowany i centralnie zarządzany moduł raportowy.
2. System musi generować centralnie konfigurowane i składowane raporty z przeprowadzonych sesji (łącznie z nagraniami sesji).
3. System musi rejestrować sesje graficzne oraz sesje z wierszem poleceń.
4. System musi umożliwiać wybór rozdzielczości rejestrowanych sesji.
5. W systemie muszą być dostępne raporty dotyczące co najmniej przeprowadzonych sesji i wykorzystania poświadczeń z wbudowanego magazynu haseł.
6. Raporty dotyczące przeprowadzonych sesji muszą podlegać filtrowaniu co najmniej (wymagane wszystkie wymienione) w zakresie daty, nazwy użytkownika (zewnętrznego dostawcy), nazwy / adresu IP zarządzanego zasobu, grupy zarządzanych zasobów.

7. System musi posiadać możliwość uruchomienia filtrowania odbytych sesji po ciągach znaków pisanych z klawiatury w trakcie ich trwania.
8. W szczegółach raportu sesji muszą znajdować się co najmniej informacje na temat:
 - a) daty rozpoczęcia i zakończenia sesji (długość trwania sesji),
 - b) nazwy konta przechowywanego we wbudowanym magazynie haseł za pomocą którego zalogowano się do systemu,
 - c) przesyłanych plików między maszyną zewnętrznego dostawcy a zarządzanym zasobem,
 - d) nagrania z sesji (sesje graficzne oraz okna konsoli),
 - e) transkrypcji chatu,
 - f) wszystkich uczestników sesji (osoby, które dołączały do sesji w trakcie jej trwania),
 - g) listy zdarzeń (log) dotyczący pracy narzędzia uprzywilejowanego dostępu zdalnego.

Konfiguracja i instalacja agentów

1. Plik instalacyjny agenta instalowanego na zarządzanym zasobie musi być przygotowany do masowej instalacji.
2. Plik instalacyjny agenta instalowanego na zarządzanym zasobie musi posiadać datę ważności, po upływie której niemożliwe będzie jego wykorzystanie.
3. Agent instalowany na zarządzanym zasobie musi być aktualizowany w sposób centralny z poziomu systemu uprzywilejowanego dostępu zdalnego.
4. System musi zapewniać możliwość określenia polityk aktualizacji agenta (możliwość definiowania co najmniej liczby jednocześnie aktualizowanych agentów oraz pasma przeznaczonego na aktualizację przez sieć).
5. System musi zapewnić możliwość zdefiniowania akcji zbierania dodatkowych danych na temat zdalnego hosta przez agenta, bez konieczności nawiązywania sesji (przynajmniej w zakresie

zużycia CPU, nazwy zalogowanego użytkownika, zajętości dysku).

Wbudowany magazyn haseł

1. System musi posiadać wbudowaną funkcjonalność magazynu poświadczeń (przechowywanie nazw kont i haseł, ukrywanie widoczności haseł przed zewnętrznymi dostawcami).
2. System musi umożliwiać dodawanie kont wykorzystywanych do zdalnego logowania co najmniej poprzez:
 - a) wprowadzenie ręczne z poziomu interfejsu konfiguracyjnego narzędzia,
 - b) wyszukanie i import z Active Directory, z możliwością automatycznej zmiany haseł na takich kontach.
 - c) możliwość zintegrowania pobierania poświadczeń z systemu PAM (przynajmniej jednego), poświadczenia muszą być prezentowane w kontekście zasobu, do którego łączy się zewnętrzny dostawca (przy nawiązywaniu sesji musi być możliwość wyboru poświadczeń występujących wyłącznie na danym zasobie).
3. Użycie poświadczeń przez zewnętrznych dostawców musi podlegać kontroli dostępu. Uprawnienia do korzystania z danych poświadczeń (haseł) muszą być przyznawane dla pojedynczego konta dostawcy lub dla grupy kont dostawców.
4. Hasła przechowywane w magazynie haseł muszą być szyfrowane AES256 lub lepszym.

Integracje

1. System musi posiadać otwarte API w zakresie pozwalającym na wykonanie integracji z oprogramowaniem firm trzecich.
2. System musi umożliwiać wykonanie integracji z systemami typu SIEM (syslog).
3. System musi umożliwiać wykonanie integracji z systemem PAM w zakresie pobierania z niego poświadczeń.
4. System musi umożliwiać wysyłanie powiadomień z

wykorzystaniem SMTP.

Kontrola dostępu

1. System musi posiadać możliwość zdefiniowania restrykcji sieciowych pozwalających ograniczyć dostęp do interfejsu zarządzającego oprogramowaniem przynajmniej w zakresie zdefiniowania adresów IP hostów lub adresów sieci znajdujących się na białej liście (liście dostępowej) i domyślnej akcji odrzucania innego ruchu skierowanego do interfejsu zarządzającego.
2. System musi umożliwiać edycję poziomu uprawnień użytkowników lub grup użytkowników co najmniej w zakresie:
 - a) edycji grup zasobów w zakresie nadawania uprawnień dostępowych do zasobów dla zewnętrznych dostawców oraz uprawnień do edycji tych zasobów (zabronienie możliwości edycji zasobów w systemie uprzywilejowanego dostępu zdalnego),
 - b) edycji i tworzenia nowych poświadczeń w magazynie haseł oraz do przyznawania uprawnień dla zewnętrznych dostawców do możliwości wykorzystania tych poświadczeń,
 - c) generowania i podglądu raportów w tym nagrań z sesji,
 - d) możliwości zapraszania do sesji dodatkowych użytkowników,
 - e) możliwości odebrania lub nadania uprawnień do realizowania sesji z wykorzystaniem instalowanych agentów, serwerów proxy, protokołu RDP lub SSH.
 - f) możliwości definiowania białych lub czarnych list poleceń w sesjach uruchamianych w konsoli.

Zakres wdrożenia dla rozwiązania równoważnego:

1. Inicjalizacja oprogramowania w środowisku Zamawiającego
2. Konfiguracja i instalacja agentów (5 sztuk na systemach Windows i Linux) lub utworzenie elementów połączeniowych (5 sztuk RDP oraz SSH)
3. Instalacja konsol dostępowych oraz ich

	konfiguracja
	4. Skonfigurowanie integracji z domeną na potrzeby logowania do dostarczanego systemu
	5. Konfiguracja i instalacja jump point jeśli jest dostępny
	6. Konfiguracja sejfu haseł, import i tworzenie kont zarządzanych
	7. Utworzenie do 3 grup użytkowników i nadanie uprawnień (role administratorzy, wnioskujący – firma zewnętrzna, pracownicy domowi) oraz skonfigurowanie uprawnień
	8. Utworzenie polityk dla sesji
	9. Testy odbiorcze konfiguracji
	10. Opracowanie dokumentacji powdrożeniowej oraz instrukcji używania systemu dla użytkowników końcowych

Część nr 2 - Oprogramowanie do audytu środowiska ActiveDirectory dla 16 kontrolerów

Opis oprogramowania	Oprogramowanie do audytu środowiska ActiveDirectory
Warunki licencji	<ol style="list-style-type: none"> 1. Pakiet licencji musi zawierać prawo do korzystania dla min. 16 kontrolerów domeny ActiveDirectry; 2. Wsparcie producenta, które obejmuje aktualizacje oraz wsparcie przez okres 12 mc. aktywności subskrypcji. 3. Zamawiający posiada obecnie rozwiązanie ManageEngine ADAudit Plus, Zamawiający oczekuje przedłużenie licencji i wsparcia na to rozwiązanie lub w przypadku zaproponowania rozwiązania alternatywnego to również usługę wdrożenia, które zapewni ten sam poziom funkcjonalności co obecne rozwiązanie oraz szkolenie dla administratorów i analityków SOC z nowego rozwiązania
Cechy oprogramowania	Kluczowe funkcjonalności: <ol style="list-style-type: none"> 1. System działa bezagentowo. 2. System działa na systemach z rodziny Windows. 3. System pozwala na podłączenie certyfikatu, w formacie .PFX oraz Java keystore. 4. System obsługuje integracje ze Splunk'iem i ArcSight'em

5. System działa w formie aplikacji Internetowej.
6. System obsługuje bazy danych PostgreSQL oraz MSSQL, jako instancje do przechowywania danych.
7. System działa na pojedynczej bazie danych.
8. System posiada wbudowane skrypty, które pozwalają na:
 - a) backup bazy danych,
 - b) odtworzenie bazy danych,
 - c) zmianę bazy danych.
9. System używa jednego konta do połączenia z domeną.
10. System posiada wbudowany program, z interfejsem graficznym, który pozwala na aktualizację aplikacji.
11. System pozwala na zmianę portu HTTP/HTTPS z poziomu interfejsu graficznego.
12. System umożliwia audyt plików na serwerach, w określonym odstępie czasowym bezagentowo lub w czasie rzeczywistym przy użyciu agenta, w tym posiada wbudowane raporty dotyczące:
 - a) Wszystkich zmian plików i folderów
 - b) Plikach zmodyfikowanych
 - c) Plikach usuniętych
 - d) Plikach przeniesionych
 - e) Plikach utworzonych
13. System umożliwia analitykę zachowań przy użyciu uczenia maszynowego oraz analizy statystycznej, pokazując dane sumarycznie, a w szczególności:
 - a) Nietypową aktywność danego użytkownika
 - b) Nietypową aktywność użytkownika na serwerze
 - c) Nietypową ilość prób np. logowań
 - d) Nietypowe godziny logowań użytkowników
 - e) Nietypowe działania na plikach

Funkcjonalności aplikacji:

1. System działa bezagentowo.
2. System obsługuje języki: Chiński, Japoński i Angielski.
3. System działa na systemach z rodziny Windows.
4. System pozwala na podłączenie certyfikatu, w formacie .PFX oraz Java keystore.
5. System obsługuje integracje ze Splunk'iem i

	<p>ArcSight'em</p> <ol style="list-style-type: none">6. System działa w formie aplikacji Internetowej.7. System obsługuje bazy danych PostgreSQL oraz MSSQL, jako instancje do przechowywania danych.8. System działa na pojedynczej bazie danych.9. System posiada wbudowane skrypty, które pozwalają na backup bazy danych, odtworzenie bazy danych, zmianę bazy danych.10. System używa jednego konta do połączenia z domeną.11. System posiada wbudowany program, z interfejsem graficznym, który pozwala na aktualizację aplikacji.12. System posiada możliwość aktywacji podwójnej autentykacji techników oprogramowania.13. System pozwala na zmianę portu HTTP/HTTPS z poziomu interfejsu graficznego.14. System umożliwia audyt zdarzeń zarówno w czasie rzeczywistym jak i w ustawianych interwałach czasowych15. System posiada możliwość raportowania wszystkich domen z pomocą pojedynczego raportu.16. System umożliwia zbiorcze audytowanie środowiska Active Directory oraz posiada wbudowane raporty dotyczące:<ol style="list-style-type: none">a) Nieudanych próby zalogowania do środowiska domenowegob) Stacji roboczychc) Serwerówd) Kontrolerów domene) Poprawne logowanie użytkowników wraz z pełną historią logowaniaf) Nieudane próby logowania na serwery Radius oraz historię logowańg) Zmiany dokonywane na kontach użytkowników, a w szczególności:<ul style="list-style-type: none">• Tworzenie kont• Usuwanie kont• Dezaktywacja kont• Modyfikacja haseł• Spis zablokowanych użytkowników• Historie użytkownikówh) Audyt zmian w grupie obiektów, w grupie bezpieczeństwa, operacje związane z tworzeniem i usuwaniem grup.i) Raportowanie użytkowników zagnieżdżonych w innych grupach.
--	---

	<ul style="list-style-type: none">j) Raport aktywności użytkowników oraz dezaktywacji stacji roboczych przez wylogowanie lub wygaszacz ekranu. <ul style="list-style-type: none">17. Zmiany dokonane na obiektach komputerów, a w szczególności:<ul style="list-style-type: none">a) Tworzenie kontb) Usuwanie kontc) Dezaktywację kontd) Historię kont18. Audyt zmian w OU, a w szczególności<ul style="list-style-type: none">a) Tworzenie OUb) Usuwanie OUc) Listę modyfikowanych OUd) Historię OU19. Zmiany wartości OU oraz domen mogą zostać przesłane do ArcSight.20. Audyt zmian w zasadach grupowych, a w szczególności:<ul style="list-style-type: none">a) Tworzenie GPOb) Usuwanie GPOc) Listę zmodyfikowanych GPOd) Historia GPO21. Zaawansowane raporty GPO mogą zostać przesłane do systemu SIEM22. Zaawansowane zmiany w GPO23. Audyt zmian uprawnień, a w szczególności:<ul style="list-style-type: none">a) Uprawnienia dotyczące poziomu dostępu do domenyb) Uprawnienia zmian OUc) Uprawnienia zmian w kontenerachd) Uprawnienia zmian w GPOe) Uprawnienia zmian użytkownikówf) Uprawnienia zmian grupg) Uprawnienia zmian komputerówh) Uprawnienia zmian DNSi) Zmiany w DNS'achj) Śledzenie zmian nazw użytkowników/komputerów/grup24. System pozwala na zbiorcze audytowanie zmian na serwerach plików, a w szczególności<ul style="list-style-type: none">a) Windowsb) Windows file Clusterc) EMCd) Net App
--	--

	<p>e) Hitachi NAS</p> <p>25. System posiada możliwość budowania własnych raportów w oparciu o funkcjonalności systemu wraz z możliwością harmonogramowania</p> <p>26. System obsługuje regex dla wzorców wykluczania plików.</p> <p>27. System potrafi audytować wydruki, w tym:</p> <ul style="list-style-type: none">a) Kto wykonywał wydruk,b) Jaki plik drukował,c) Kiedy wykonał wydruk,d) Ile kopii wykonał,e) Jaki był rozmiar pliku,f) Ile stron pliku zostało wydrukowane,g) użytą drukarkę,h) Na którym serwerze znajduje się drukarka <p>28. System pozwala na tworzenie raportów zgodności, a w szczególności posiada wbudowane raporty dotyczące:</p> <ul style="list-style-type: none">a) Raporty zgodności dla audytów, a w szczególności:b) SOXc) HIPAAd) PCI-DSSe) GLBAf) FISMAg) RODO/GDPR <p>29. System pozwala na audyt:</p> <ul style="list-style-type: none">a) Zmian na serwerach członkowskichb) Audyt stacji roboczych <p>30. System posiada moduł powiadomień w formie alertów</p> <ul style="list-style-type: none">a) Widocznych w systemieb) Drogą mailowąc) Poprzez SMS <p>31. System umożliwia podczas tworzenia profili alertów e-mail i SMS, listy mailingowej na podstawie wielu zmiennych (np., Nazwa użytkownika, SID itp.)</p> <p>32. System umożliwia wykonanie różnego rodzaju skryptów, dzięki którym zagrożenie zostaje wyeliminowane natychmiast.</p> <p>33. System posiada alerty o przekroczonej przestrzeni dyskowej</p> <p>34. Narzędzie umożliwia zwolnienie zajętej przestrzeni dyskowej</p> <p>35. System przechowuje zarchiwizowany zbiór logów z audytowanego środowiska i ma możliwość dokładnego</p>
--	---

	<p>ustawiania czasu przeniesienia do archiwum.</p> <p>36. System pozwala na audyt Azure Active Directory, a w szczególności:</p> <ul style="list-style-type: none">a) Poprawne logowanie użytkownikab) Niepoprawne logowanie użytkownikac) Niepoprawne logowanie użytkownika bazowane na nieprawidłowym podaniu hasład) Aktywność logowania ze wskazaniem adresu IP użytkownika/stacji roboczej <p>37. System pozwala na audyt zmian na kontach użytkowników Azure Active directory, a w szczególności posiada wbudowane raporty dotyczące:</p> <ul style="list-style-type: none">a) Ostatnio utworzony użytkownikb) Ostatnio usunięty użytkownikc) Ostatnio zaktualizowany użytkownikd) Ostatnio aktywowany użytkownike) Ostatnio dezaktywowany użytkownikf) Ostatnio zmienione hasło dla użytkownikag) Ostatnio zresetowane hasło dla użytkowników. <p>38. System pozwala na Audyt nadanych ról w Azure Active Directory, a w szczególności przygotowane raporty dotyczące:</p> <ul style="list-style-type: none">a) Ostatnio przypisany członek do rolib) Ostatnio odłączony członek od roli <p>39. System pozwala na audyt zmian grup w Azure Active Directory, a w szczególności:</p> <ul style="list-style-type: none">a) Ostatnio utworzona grupab) Ostatnio usunięta grupac) Ostatnio zaktualizowana grupad) Ostatnio dodani członkowie do grupe) Ostatnio usunięci członkowie z grup <p>40. System umożliwia audyt plików na serwerach, w określonym odstępie czasowym bezagentowo lub w czasie rzeczywistym przy użyciu agenta, w tym posiada wbudowane raporty dotyczące:</p> <ul style="list-style-type: none">a) Wszystkich zmian plików i folderówb) Plikach zmodyfikowanychc) Plikach usuniętychd) Plikach przeniesionyche) Plikach utworzonych <p>41. Program posiada możliwość alertowania administratora w razie braku komunikacji z agentem.</p> <p>42. System umożliwia audyt urządzeń USB dla Serwerów Windows 2016 i systemu Windows 10, a w</p>
--	--

	<p>szczegółności posiada wbudowane raporty dotyczące:</p> <ul style="list-style-type: none">a) Zmiany na plikach lub folderachb) Odczyt danego plikuc) Zmiana danego plikud) Kopiowanie danego pliku <p>43. System umożliwia analitykę zachowań przy użyciu uczenia maszynowego oraz analizy statystycznej, pokazując dane sumarycznie, a w szczególności:</p> <ul style="list-style-type: none">a) Nietypową aktywność danego użytkownikab) Nietypową aktywność użytkownika na serwerzec) Nietypową ilość prób np. logowańd) Nietypowe godziny logowań użytkownikówe) Nietypowe działania na plikach <p>44. System posiada możliwość oceny ryzyka, opartego o uczenie maszynowe:</p> <ul style="list-style-type: none">a) Użytkownicy połączeni z dużą ilością zasobówb) Konta o dużej aktywnościc) Konta o nadmiernej aktywnościd) Konta z wysokim % niepowodzeń logowaniae) Ostatnia aktywność użytkownikaf) Uśpione konta administratorówg) Uprawnienia wykorzystane przez użytkownikówh) Pierwsze użycie przydzielonego uprawnieniai) Konta oparte na zdalnym logowaniu <p>45. System obsługuje audytowanie zmian na share'ach sieciowych, w tym posiada przygotowane raporty dotyczące:</p> <ul style="list-style-type: none">a) Zmiany nazw plików oraz folderówb) Utworzenie nowych plików oraz folderówc) Usunięcie plików oraz folderówd) Przeniesienie plików oraz folderówe) Zmiany uprawnień na plikach i folderach <p>46. System umożliwia przesyłanie logów do SYSLOG'a lub innych systemów SIEM'owych.</p> <p>47. System obsługuje połączenie LDAP'owe po SSL'u.</p> <p>48. System pozwala na eksportowanie raportów/danych do formatów:</p> <ul style="list-style-type: none">a) CSVb) PDFc) XLSd) HTML <p>49. System dostarcza informacje o bezpiecznych</p>
--	--

	<p>powiązaniach LDAP, niezabezpieczonych powiązaniach oraz powiązaniach, które zostały odrzucone z powodu błędów.</p> <p>50. System dodatkowo obsługuje raportowanie z ADLDS oraz LAPS'a.</p> <p>51. System potrafi przetworzyć dane do systemu SIEM'owego, w formacie RFC 3164 lub RFC 5424,</p> <p>a) W tym obsługuje wysyłanie danych po UDP jak i TCP.</p> <p>52. System potrafi archiwizować dane do plików .zip oraz dołączać je do bazy danych, na żądanie administratora.</p> <p>a) W tym, system pozwala na archiwizację wybranej kategorii zdarzeń.</p> <p>53. System potrafi zaimportować pliki .evt oraz .evtx, przetworzyć je wg. własnych filtrów oraz prezentować, jak resztę danych.</p> <p>54. System pozwala na określenie godzin biznesowych, w celu filtrowania prezentowania raportów, na podstawie godzin pracy, jak i godzin poza pracą.</p> <p>55. System pozwala na uruchomienie dowolnego programu, w momencie wystąpienia alertu.</p> <p>56. System obsługuje wiele domen na pojedynczej instancji.</p> <p>57. System pozwala na pobieranie danych z AzureAD, w tym przetworzenia ich wg. własnych wbudowanych reguł.</p> <p>58. System posiada możliwość wyszukiwania własnych, wbudowanych raportów, na podstawie słów kluczowych.</p> <p>59. System posiada możliwość śledzenia wiersza poleceń użytych przez proces.</p> <p>60. System umożliwia konfigurację wysokiej wydajności.</p> <p>61. System posiada raport zmian uprawnień NetApp i EMC w celu dostarczenia informacji o wartościach uprawnień przed i po.</p> <p>62. System posiada możliwość konfiguracji ustawień agenta.</p> <p>63. System umożliwia pojedyncze logowanie (SSO) za pośrednictwem NTLM lub SAML.</p> <p>64. System pozwala na prezentację wszystkich działań użytkowników w jednym raporcie w obszarze Account Management.</p> <p>65. System umożliwia przeprowadzenie audytu i raportu na</p>
--	---

	<p>temat wykorzystania podatnego na Netlogon połączenie Schannel przez urządzenia z systemem Windows.</p> <p>66. System pozwala kontrolować dostęp do plików i zmiany uprawnień w systemach pamięci masowej Huawei OceanStor.</p>
--	---

Część nr 3 - Narzędzie do śledzenia błędów oraz zarządzania projektem dla 200 użytkowników

Opis oprogramowania	Narzędzie do śledzenia błędów oraz zarządzania projektem
Warunki licencji	<ol style="list-style-type: none"> 1. Pakiet licencji musi zawierać prawo do korzystania dla min. 200 użytkowników; 2. Wsparcie producenta, które obejmuje aktualizacje oraz wsparcie przez okres 12 mc. aktywności subskrypcji. 3. Zamawiający posiada obecnie rozwiązanie Jira Software Cloud Standard, w przypadku zaproponowania innego rozwiązania, Wykonawca zobowiązany jest do migracji danych z obecnego rozwiązania Jira Software Cloud Standard do rozwiązania przedstawionego w ofercie
Cechy oprogramowania	<ol style="list-style-type: none"> 1. Oprogramowanie musi udostępniać podstawowy interfejs użytkownika dostępny przez przeglądarkę internetową; 2. Oprogramowanie musi realizować funkcjonalność narzędzia do śledzenia zadań (issue tracking) 3. Oprogramowanie musi realizować funkcjonalność narzędzia do zarządzania błędami (Bug tracking); 4. Oprogramowanie musi zapewniać możliwość zarządzania wieloma różnymi projektami; 5. Oprogramowanie musi zapewniać wsparcie dla kompleksowego zarządzania projektem i metod typu Agile (Agile Project Management); 6. Oprogramowanie musi zapewniać możliwość dowolnej konfiguracji przepływu pracy (workflow); 7. Oprogramowanie musi pozwalać integracja z popularnymi platformami programistycznymi jak Eclipse, IntelliJ IDEA, Microsoft Visual Studio, Microsoft Visual Studio Code, JDeveloper, NetBeans, Zend Studio, inne; 8. Oprogramowanie musi zapewniać możliwość zarządzania błędami, właściwościami projektu, zadaniami, osiągnięciami lub innymi zagadnieniami; 9. Oprogramowanie musi zapewniać możliwość połączenia tworzonych zadań i zgłoszeń z kodem źródłowym, dostęp do kodu źródłowego; 10. Oprogramowanie musi zapewniać możliwość dodawania załączników; 11. Oprogramowanie musi zapewniać możliwość tworzenia nowych zadań za pośrednictwem przeglądarki, poczty elektronicznej oraz zintegrowanego środowiska programistycznego (IDE); 12. Oprogramowanie musi zapewniać możliwość szeregowania zadań, nadawania priorytetów; 13. Oprogramowanie musi zapewniać możliwość śledzenia zmian w

	<p>komponentach i wersjach oprogramowania;</p> <p>14.Oprogramowanie musi zapewniać możliwość generowania powiadomień członków zespołu projektowego z możliwością ich konfiguracji;</p> <p>15.Oprogramowanie musi zapewniać możliwość tworzenia ról, poziomów uprawnień, grup użytkowników;</p> <p>16.Oprogramowanie musi zapewniać możliwość tworzenia użytkowników, przydzielanie ról, poziomów uprawnień dla grup użytkowników;</p> <p>17.Oprogramowanie musi zapewniać możliwość definiowania uprawnień dostępu z poziomu panelu;</p> <p>18.Oprogramowanie musi zapewniać możliwość synchronizacji katalogu użytkowników z systemem uwierzytelniania opisanym w poniższym dokumencie oraz LDAP;</p> <p>19.Oprogramowanie musi zapewniać możliwość rejestracji historii aktywności użytkowników – dostęp do ostatnio otwartych zadań, projektów;</p> <p>20.Oprogramowanie musi zapewniać możliwość wyszukiwania pełnotekstowego, filtrowania i raportowania;</p> <p>21.Oprogramowanie musi zapewniać możliwość generowania zestawień i statystyk podsumowujących realizację projektu;</p> <p>22.Oprogramowanie musi zapewniać możliwość generowania dokumentów w formacie xls, xlsx, xlsx, doc,docx;</p> <p>23.Oprogramowanie musi zapewniać możliwość wyświetlania podsumowań i raportów dla rozpoczętych projektów – ostanía aktywność, kamienie milowe, logi zmian, mapy projektu, wykresy;</p>
Inne wymagania	<p>1. Oprogramowanie musi być dostarczone w najnowszej dostępnej wersji;</p> <p>2. Oprogramowanie musi zapewniać możliwość instalacji wtyczek (ang. plug-in), rozszerzających funkcjonalność oprogramowania;</p> <p>3. Oprogramowanie musi zapewniać możliwość integracji z narzędziem do repozytorium kodu źródłowego dostarczonym w niniejszym postępowaniu</p> <p>4. Możliwość integracji z systemami kontroli wersji (minimum z: Subversion, Mercurial, Git);</p> <p>5. Dostępność aplikacji mobilnej na system Android i IOS.</p>

Część nr 4 - Narzędzie do repozytorium kodu źródłowego dla 100 użytkowników

Opis oprogramowania	Narzędzie do repozytorium kodu źródłowego
Warunki licencji	<p>1. Pakiet licencji musi zawierać prawo do korzystania dla min. 100 użytkowników;</p> <p>2. Licencja musi zawierać prawo do instalacji na własnym serwerze.</p> <p>3. Wsparcie producenta, które obejmuje aktualizacje oraz wsparcie przez okres 12 mc. aktywności subskrypcji.</p> <p>4. Zamawiający posiada obecnie rozwiązanie Bitbucket Datacenter, w przypadku zaproponowania innego rozwiązania, Wykonawca zobowiązany jest do migracji danych z obecnego rozwiązania Bitbucket Datacenter do rozwiązania przedstawionego w ofercie</p>

Cechy oprogramowania	<ol style="list-style-type: none">1. Oprogramowanie musi posiadać interfejs użytkownika dostępny przez przeglądarkę internetową;2. Oprogramowanie musi posiadać funkcjonalność narzędzia kontroli wersji kodu źródłowego,3. Oprogramowanie musi posiadać funkcjonalność narzędzia repozytorium kodu źródłowego, dokumentów, witryn i innych plików;4. Oprogramowanie musi posiadać możliwość przeglądania kodu źródłowego, dokumentów, witryn i katalogu innych dokumentów;5. Oprogramowanie musi posiadać możliwość zarządzania prawami dostępu do publikowanych materiałów;6. Oprogramowanie musi posiadać możliwość zakładania nieograniczonej liczby prywatnych repozytoriów dla każdego z użytkowników;7. Oprogramowanie musi posiadać możliwość automatycznego generowania plików README na podstawie plików podobnych do plików Markdown;8. Oprogramowanie musi posiadać funkcjonalność narzędzia do śledzenia problemów (Issue tracking);9. Oprogramowanie musi posiadać możliwość budowania oprogramowania;10. Oprogramowanie musi posiadać możliwość śledzenia zmian w komponentach i wersjach oprogramowania;11. Musi istnieć możliwość logowania do serwera SYSLOG.
Inne wymagania	<ol style="list-style-type: none">1. Oprogramowanie w najnowszej dostępnej wersji;2. Oprogramowanie musi posiadać możliwość instalacji wtyczek (ang. plug-in), rozszerzających funkcjonalność oprogramowania;3. Oprogramowanie musi posiadać dostępność interfejsu REST API;4. Oprogramowanie musi posiadać oprogramowanie oparte na Git;5. Oprogramowanie musi posiadać możliwość integracji z oprogramowaniem do śledzenia błędów i zarządzania projektem opisanym w niniejszym projekcie, w zakresie pozwalającym na śledzenie i edytowanie błędów i problemów, powiązań pomiędzy problemami a kodem źródłowym;6. Oprogramowanie musi posiadać możliwość instalacji oprogramowania na serwerze pracującym pod kontrolą systemu operacyjnego Linux;7. Oprogramowanie musi posiadać możliwość integracji z systemami kontroli wersji (minimum z: Subversion, Mercurial, Git);8. Oprogramowanie musi zapewniać możliwość integracji z Narzędzia do śledzenia błędów oraz zarządzania projektem

Część nr 5 - Oprogramowanie do obróbki plików multimedialnych i graficznych

Przedmiotem zamówienia jest zakup 2 szt. licencji oprogramowania Adobe Creative Cloud lub równoważnego spełniającego poniżej wskazane parametry równoważności.

Opis równoważności:

1. Oprogramowanie do tworzenia grafiki, animacji, video oraz treści internetowych.
Oprogramowanie powinno umożliwiać:
 - a. tworzenie i obróbkę grafiki wektorowej
 - b. tworzenie i obróbkę grafiki rastrowej
 - c. obróbkę zdjęć
 - d. tworzenie kompozycji wektorowych
 - e. opracowywanie, tworzenie i udostępnianie prototypów interfejsu użytkownika
 - f. obróbkę materiałów w natywnych formatach, a także tworzenie produkcji filmowych, telewizyjnych i internetowych
 - g. tworzenie animacji i efektów wizualnych na potrzeby filmów, telewizji, wideo i stron internetowych
 - h. tworzenie fotorealistycznych obrazów 3D do oznaczeń marki, ujęć produktów i projektów opakowań
 - i. projektowanie i programowanie, aktywnych witryn www
 - j. kompleksową obsługę plików PDF z dowolnego miejsca
2. Licencje czasowe (1 rok), wersja przypisana do stacji roboczej

Część nr 6 - Oprogramowanie do zgłaszania i zarządzania problemami informatycznymi dla 15 techników

Opis oprogramowania	Oprogramowanie do zgłaszania i zarządzania problemami informatycznymi użytkowników końcowych (helpdesk)
Warunki licencji	1. Pakiet licencji musi zawierać prawo do korzystania dla min. 15 pracowników helpdesk, którzy mają mieć możliwość rozwiązywania zgłaszanych problemów; 2. Pakiet licencji musi zawierać prawo do korzystania przez nieograniczoną ilość użytkowników, chcących zgłaszać problemy ze swoim stanowiskiem komputerowym i oprogramowaniem na nim; 3. Wsparcie producenta, które obejmuje aktualizacje oraz wsparcie przez okres 12 mc. aktywności subskrypcji. 4. Zamawiający posiada obecnie rozwiązanie Jira Service Management Cloud Standard, w przypadku zaproponowania innego rozwiązania, Wykonawca zobowiązany jest do migracji danych z obecnego rozwiązania Jira Service Management Cloud Standard do rozwiązania przedstawionego w ofercie
Cechy oprogramowania	1. Oprogramowanie musi udostępniać podstawowy interfejs użytkownika dostępny przez przeglądarkę internetową; 2. Oprogramowanie musi posiadać portal samoobsługowy, tj. bazę wiedzy w której użytkownicy mogą samodzielnie znaleźć rozwiązanie swojego problemu 3. Oprogramowanie musi umożliwiać rejestrację zgłoszeń poprzez wysłanie do niego maila od użytkownika 4. Oprogramowanie musi umożliwiać tworzenie formularzy i powiązane z nimi przepływy pracy do zgłaszania i obsługi zgłoszeń

	<p>5. Oprogramowaniem musi posiadać kolejki zgłoszeń, które można wykorzystać do priorytezywania zadań</p> <p>6. Oprogramowanie musi umożliwiać zarządzanie i nadzorowanie SLA realizowanych zgłoszeń</p> <p>7. Oprogramowanie musi posiadać gotowe raporty oraz możliwość tworzenia własnych, poprzez które będzie można uzyskać informacje nt. czasów rozwiązania zadań czy wskaźnika SLA</p> <p>8. Oprogramowanie musi posiadać mechanizmy automatyzujące część prac pracowników helpdesk, aby przyspieszyć realizację zadań</p> <p>9. Oprogramowanie musi posiadać gotowe szablony do zarządzania usługami</p> <p>10. Oprogramowanie ma posiadać przestrzeń na pliki o wielkości min 200GB</p> <p>11. Oprogramowanie ma umożliwiać lub mieć oficjalnie ogłoszoną funkcjonalność prowadzenia rozmów między pracownikiem helpdesk, a pracownikiem zgłaszającym błąd poprzez stosowane u zamawiającego oprogramowanie Microsoft Teams</p> <p>12. Oprogramowanie ma umożliwiać wysyłanie nieograniczonej ilości alertów i powiadomień drogą e-mail oraz SMS</p> <p>13. Oprogramowanie ma umożliwiać eskalację zgłoszeń</p> <p>14. Oprogramowanie musi umożliwiać zarządzanie dyżurami domowymi</p> <p>15. Oprogramowanie ma posiadać rejestr usług, aby móc mierzyć jakość ich realizacji</p> <p>16. Oprogramowanie ma umożliwiać zarządzanie zmianami</p> <p>17. Oprogramowanie ma posiadać dziennik w którym są rejestrowane wszystkie istotne zmiany administracyjne w oprogramowaniu jak np. zmiana uprawnień</p>
Inne wymagania	<p>1. Oprogramowanie musi być dostarczone w najnowszej dostępnej wersji;</p> <p>2. Oprogramowanie musi zapewniać możliwość instalacji wtyczek (ang. plug-in), rozszerzających funkcjonalność oprogramowania;</p> <p>3. Oprogramowanie musi zapewniać możliwość integracji z posiadanym narzędziem Jira Software;</p> <p>4. Jeśli oferowane oprogramowanie jest dostarczane jako produkt chmurowy, musi istnieć możliwość zdefiniowania, aby dane przechowywane były na terenie Unii Europejskiej;</p> <p>5. Dostępność aplikacji mobilnej na system Android i IOS.</p>

Część nr 7 - Licencje na system operacyjny Windows Server 2022 Standard

System operacyjny charakteryzujący się następującymi cechami:

- Licencja na zaoferowany system operacyjny musi być w pełni zgodna z warunkami licencjonowania producenta oprogramowania,
- najnowsza dostępna wersja oprogramowania
- wersja systemu 64-bit,

- Interfejsy użytkownika dostępne w kilku językach do wyboru – minimum w Polskim i Angielskim,
- Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika.
- Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet
- Ze względu na posiadany system ERP, musi być kompatybilna z systemem SIMPLE.ERP (producent oprogramowania: SIMPLE SA - SIMPLE Spółka Akcyjna z siedzibą w Warszawie przy ul. Bronisława Czecha 49/51)
- Ze względu na posiadaną przez zamawiającego domenę opartą na rozwiązaniu Windows i polityce kont synchronizowanych z MS Active Directory, system musi umożliwiać bezproblemową współpracę z tymi rozwiązaniami
- Z mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne – wymagane podanie nazwy strony serwera www.
- Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego,
- Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego,
- Wbudowana zaporą internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;
- Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami,
- Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimedialny, pomoc, komunikaty systemowe,
- Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,
- Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi),
- Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer,
- Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę Zamawiający rozumie zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji,
- Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji,
- Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe,
- Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
- Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
- Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.
- Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);
- Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
- Mechanizmy logowania w oparciu o:
 - a. Login i hasło,
 - b. Karty z certyfikatami (smartcard),
 - c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
- Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu,

- Wsparcie dla algorytmów Suite B (RFC 4869),
- Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec,
- Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;
- Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach,
- Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń,
- Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązywania problemu z komputerem,
- Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową,
- Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe,
- Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe
- Udostępnianie modemu,
- Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej,
- Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci,
- Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.),
- Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu),
- Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych,
- Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika,
- Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych
- Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.
- Możliwość nieodpłatnego instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.
- Poprawna współpraca z systemem MS Windows 2003/2008/2016 Serwer
- Interfejs kafelkowy
- Możliwość pracy wielowątkowej
- Okienkowy system operacyjny
- Funkcja wielu ekranów

Część nr 8 - Licencje na system operacyjny

Zakup 3 sztuk

Zakup systemu operacyjnego w wersji dla serwera 16 Core, zasada licencjonowania w oparciu o rdzenie. Proponowana wersja ma być najnowszą wersją systemu operacyjnego, spełniającą co najmniej następujące cechy:

- Ze względu na posiadany system ERP, musi być kompatybilna z systemem SIMPLE.ERP (producent oprogramowania: SIMPLE SA - SIMPLE Spółka Akcyjna z siedzibą w Warszawie przy ul. Bronisława Czecha 49/51)
- Ze względu na posiadaną przez zamawiającego domenę opartą na rozwiązaniu Windows 2016 i polityce kont synchronizowanych z MS Active Directory, system musi umożliwiać bezproblemową współpracę z tymi rozwiązaniami;
- Ze względu na politykę bezpieczeństwa stosowaną u Zamawiającego system musi bezproblemowo pracować w domenie opartej na Windows 2016 oraz w pełni wykorzystywać funkcjonalność domeny Windows;
- Uprawnienia do wirtualizacji : 2 wirtualne maszyny lub 2 kontenery Hyper-V
- Limit pamięci RAM: 48 TB RAM i 2048 rdzeni logicznych działających na 64 fizycznych gniazdach dla wymagających aplikacji warstwy 1
- Współpraca z procesorami o architekturze x64;
- Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym;
- Możliwość budowania klastrów składających się z 64 węzłów;
- Możliwość federowania klastrów typu failover w zespół klastrów z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu;
 - Możliwość uruchomienia roli klienta i serwera czasu (NTP);
 - W ramach dostarczonej licencji zawarte prawo do instalacji i użytkowania systemu operacyjnego na co najmniej dwóch maszynach wirtualnych;
 - W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego.
- Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego
- Wbudowane wsparcie instalacji i pracy na wolumenach, które:
 - a. pozwalają na zmianę rozmiaru w czasie pracy systemu,
 - b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
 - c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
 - d. umożliwiają zdefiniowanie list kontroli dostępu
- Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość;
- Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji;
- Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET;
- Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów;
- Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych;

- Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe;
 - Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków
- poprzez wybór z listy dostępnych lokalizacji;
- Mechanizmy logowania w oparciu o:
 - a. login i hasło,
 - b. karty z certyfikatami (smartcard),
 - c. wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).
 - Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla:
 - a. kreślonych grup użytkowników,
 - b. zastosowanej klasyfikacji danych,
 - c. centralnych polityk dostępu w sieci,
 - d. centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
 - Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play);
 - Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach;
 - Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach;
 - Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
 - a. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.
 - b. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
 - podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
 - ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
 - odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
 - bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
 - c. zdalna dystrybucja oprogramowania na stacje robocze.
 - d. praca zdalna na serwerze z wykorzystaniem terminala lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników.
 - e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
 - Dystrybucję certyfikatów poprzez http,
 - Konsolidację CA dla wielu lasów domeny,
 - Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, iv. Automatyczne występowanie i używanie (wystawianie)

certykatów PKI X.509.

- f. szyfrowanie plików i folderów.
 - g. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec)
 - h. szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi
 - i. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
 - j. serwis udostępniania stron WWW
 - k. wsparcie dla protokołu IP w wersji 6 (IPv6).
 - l. wsparcie dla algorytmów Suite B (RFC 4869).
 - m. wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na posiadanych komputerach z systemem Windows.
 - n. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych.
 - o. możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (Hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
 - p. możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu fail-over z jednoczesnym zachowaniem pozostałej funkcjonalności.
 - q. mechanizmy wirtualizacji mające wsparcie dla:
 - dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
 - obsługi ramek typu jumbo frames dla maszyn wirtualnych.
 - obsługi 4-KB sektorów dysków,
 - nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,
 - możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
 - możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej
 - możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.
 - r. możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.
 - s. możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
 - t. wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek.
 - u. możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
 - v. mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
- Graficzny interfejs użytkownika;
 - Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu;
 - Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa;
 - Oparta na przeglądarce aplikacja do zarządzania serwerami, klastrami, hiperkonwergentną infrastrukturą i posiadanyimi komputerami z systemem Windows 10
 - W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do

<p>oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera.</p> <ul style="list-style-type: none"> Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
--

Część nr 9 - Oprogramowanie do kontroli dostępu do sieci komputerowej (NAC)

Opis oprogramowania	Oprogramowanie do kontroli dostępu do sieci komputerowej (NAC). Obecnie posiadamy oprogramowanie : Cisco Identity Service Engine Essentials Subscription na 3 lat. W przypadku zaoferowania przez Wykonawcę produktów równoważnych w stosunku do oprogramowania i licencji opisanych przez Zamawiającego wymagane jest, aby oprogramowanie i licencje spełniały niżej wymienione wymagania oraz w ramach przekazania licencji zostały one wdrożone na sieci komputerowej.
Warunki licencji	<ol style="list-style-type: none"> Pakiet licencji musi zawierać prawo do korzystania dla min. 2 oprogramowań do kontroli dostępu do sieci komputerowej, działających w klastrze niezawodnościowym; Pakiet licencji musi umożliwić kontrolę dostępu dla min. 200 urządzeń jednocześnie; <p>W przypadku oferowania rozwiązania bazującego na dedykowanym sprzęcie wymaga się zapewnienia usług serwisowych gwarantujących wymianę uszkodzonych elementów na następny dzień roboczy licząc od chwili zgłoszenia;</p> <ol style="list-style-type: none"> Wsparcie producenta, które obejmuje aktualizacje oraz wsparcie przez okres 12 mc. aktywności subskrypcji.
Cechy oprogramowania	<ol style="list-style-type: none"> Rozwiązanie musi zapewnić mechanizmy kontroli dostępu do sieci informatycznej realizowane z wykorzystaniem protokołu IEEE 802.1x, Autentykacja oraz autoryzacja muszą odbywać się na poziomie przełącznika sieciowego, Dla urządzeń (komputer, drukarka) które nie wspierają protokołu 802.1x muszą być dostępne mechanizmy umożliwiające autentykację za pomocą MAC adresu oraz tzw. tryb pasywny pozwalający na identyfikację komputera po adresie IP, na którym użytkownik dokonał poprawnej autentykacji poprzez kontroler domeny, Rozwiązanie musi wspierać przełączniki wiodących producentów sprzętu sieciowego na rynku, w szczególności urządzenia Dell Powerconnect N5548 (obecnie posiadane przez Zamawiającego), Rozwiązanie musi bazować (w zakresie mechanizmów autentykacji/autoryzacji) na standardach Radius,

	<ol style="list-style-type: none"> 6. System musi oferować możliwość modyfikacji, tworzenie oraz importu słowników Radius dla różnych platform sieciowych, tak aby w przyszłości można było dalej korzystać z rozwiązania również na innych przełącznikach sieciowych, 7. Rozwiązanie musi zapewniać autentykację oraz autoryzację dostępu do sieci przewodowej jak i bezprzewodowej dla następujących scenariuszy: <ol style="list-style-type: none"> 1. Dostęp dla pracowników do sieci firmowej poprzez 802.1x z użyciem autentykacji poprzez certyfikat, dane logowania oraz jedno i drugie, 2. Dostęp dla pracowników do sieci firmowej z wykorzystaniem tzw. pasywnej autentykacji poprzez mapowanie IP komputera z danymi logowania użytkownika na poziomie kontrolera domeny, 3. Dostęp dla gości z wykorzystaniem z wykorzystaniem tzw. Captive Portal, z możliwością zdefiniowania trybu hotspot, self-registered oraz sponsored, 4. Autentykacja urządzeń peryferyjnych za pomocą adresy MAC, 8. System musi zapewniać widoczność podłączonych użytkowników/urządzeń do sieci, umożliwiając ich identyfikację na poziomie danych logowania, adresu MAC/IP komputera, przełącznika do którego jest podłączony dany komputer, 9. Poza bieżącym podglądem danych nt. widoczności wymagana jest możliwość raportowania w zakresie jak powyżej na okres co najmniej 3 m-cy wstecz, 10. System musi posiadać graficzny interfejs użytkownika o intuicyjnej architekturze, 11. Rozwiązanie musi wspierać integrację z MS Active Directory jako bazą użytkowników, 12. Rozwiązanie musi zapewniać wykonanie kopii ustawień/konfiguracji oraz logów za pomocą wbudowanych mechanizmów umożliwiających odtworzenie systemu na „świeżej” platformie w razie awarii, 13. Oferowane rozwiązanie musi zapewniać możliwość obsługi na poziomie 1000 jednoczesnych sesji autentykacji/autoryzacji bez konieczności rozbudowy systemu (ponoszenia dodatkowych kosztów) za wyjątkiem zwiększenia zasobów na poziomie platformy wirtualizacyjnej.
--	--

Część nr 10 – Monitory

Parametry nie mniejsze niż:

- Zastosowanie: Monitor będzie wykorzystywany dla potrzeb aplikacji biurowych, edukacyjnych, obliczeniowych, dostępu do Internetu, poczty elektronicznej oraz systemu SIMPLE.ERP
- Przekątna ekranu: 23.8"
- Rodzaj matrycy: LED, TFT, VA
- Rozdzielczość ekranu: 1920 x 1080
- Format obrazu: 16:9
- Częstotliwość odświeżania ekranu: 75Hz
- Liczba wyświetlanych kolorów: 16,7 ml
- Czas reakcji plamki: 5 ms – 12 ms
- Kontrast: 3000:1
- Jasność: 250 cd/m²
- Kąt widzenia pion: 178 °
- Kąt widzenia poziom: 178 °
- Porty wejścia/wyjścia: HDMI x 1, VGA x 1
- Wielkość plamki: 0,2745mm
- Możliwość montażu na ścianie: tak / Standard VESA 100x100 mm
- Informacje dodatkowe: regulacja pochylania w pionie
- Standardowe zużycie energii: 15,7W
- Maksymalne zużycie energii: 24W
- Wyposażenie: instrukcja obsługi, kabel HDMI
- Gwarancja: Producenta nie mniejsza niż 12 miesięcy

Część nr 11 – Oprogramowanie do wirtualizacji stacji roboczych wraz z oprogramowaniem do zarządzania i monitorowania środowiska VDI oraz wsparciem technicznym

Zamawiający posiada wdrożone rozwiązanie VDI VMware Horizon Standard dla 100 użytkowników na klastrze składającym się z trzech serwerów fizycznych. Zamawiający chce zakupić 100 licencji z prawem opcji zakupu kolejnych 100 licencji. Obecnie zainstalowane są:

1. Horizon 8 Standard
2. vCenter Server 7 Standard for Horizon
3. vSphere 7 Enterprise Plus for Desktop Stand Alone
4. Dynamic Environment Manager Standard

Poniższą specyfikację należy rozumieć jako przedłużenie / rozszerzenie tych licencji lub zaoferowanie rozwiązania alternatywnego wraz z wdrożeniem i szkoleniem dla 3 administratorów. W specyfikacji ilości użytkowników są podane jako ich maksymalne wartość.

Opis oprogramowania	Oprogramowanie do wirtualizacji stacji roboczych wraz z oprogramowaniem do zarządzania i monitorowania środowiska VDI oraz wsparciem technicznym
Warunki licencji	1. Oprogramowanie powinno zostać dostarczone w formie Subskrypcji na okres 12 miesięcy

	<p>2. Oprogramowanie musi umożliwić docelowo jednoczesną pracę 200 użytkownikom,</p> <p>3. Dostarczone licencje muszą umożliwić instalację i użytkowanie niezbędnej ilości hostów (hypervisor) wymaganych do uruchomienia wirtualnych maszyn stacji roboczych,</p> <p>4. Dostarczone licencje mają umożliwić pracę 100, w prawie opcji 200, użytkownikom jednocześnie na systemie Windows 10, która to licencja na Windows 10 jest zapewniona przez posiadaną obecnie przez Zamawiającego licencje.</p>
Cechy oprogramowania	<p>1. Oferowane rozwiązanie musi zapewniać możliwość instalacji wszystkich jego komponentów w infrastrukturze Zamawiającego,</p> <p>2. Oprogramowanie do wirtualizacji stacji roboczych musi wspierać Microsoft Windows 10, Windows 2012 jako systemy operacyjne zainstalowane na wirtualnych stacjach roboczych,</p> <p>3. Oprogramowanie do wirtualizacji stacji roboczych musi wspierać dostęp do wirtualnych stacji roboczych przez aplikację kliencką, która można zainstalować na: Windows 8.1 (32 lub 64 bit), MacOS X, iOS i Android, oraz dostęp do stacji roboczych przez terminal typu Thin Client. Dla pozostałych systemów operacyjnych musi być możliwy dostęp bezpośrednio przez przeglądarkę internetową obsługującą HTML5.</p> <p>4. Serwer/serwery zarządzające infrastrukturą wirtualnych stacji roboczych muszą być instalowane na maszynach fizycznych lub wirtualnych z systemami operacyjnymi Windows Server 2012 R2/2016/2019. Wspomniane systemy mogą być w wersji Standard lub Enterprise,</p> <p>5. Oprogramowanie do wirtualizacji stacji roboczych musi integrować się z usługami terminalowymi Microsoft RDSH oraz Windows Server 2012R2/2016 udostępniając użytkownikom możliwość połączenia się z pełną sesją terminalową lub pojedynczą aplikacją za pomocą dostępnych klientów opisanych w punkcie 2.</p> <p>6. Konfiguracja i zarządzanie dostępem do sesji i aplikacji terminalowych musi być realizowana z poziomu tej samej pojedynczej konsoli zarządzającej.</p> <p>7. Oprogramowanie do wirtualizacji stacji roboczych musi posiadać możliwość instalacji więcej niż jednej instancji serwera zarządzającego połączeniami, tak aby w przypadku awarii takiego serwera zapewnić możliwość nawiązania nowej sesji przez inny serwer zarządzający,</p> <p>8. Dostęp do centralnej konsoli zarządzającej musi być możliwy przy wykorzystaniu przeglądarki Internet Explorer lub Firefox, lub Chrome</p> <p>9. Centralna konsola do zarządzania musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory,</p> <p>10. Centralna konsola do zarządzania musi posiadać możliwość przydzielania i konfiguracji uprawnień do poszczególnych wirtualnych stacji roboczych lub grup wirtualnych stacji roboczych,</p> <p>11. Centralna konsola do zarządzania musi posiadać możliwość integracji z tokenami RSA celem zapewnienia uwierzytelniania dwuskładnikowego do wirtualnych stacji roboczych,</p> <p>12. Oprogramowanie do wirtualizacji stacji roboczych musi zapewniać możliwość szybkiego dynamicznego tworzenia grup wielu nowych wirtualnych stacji roboczych oraz tworzenia grup wirtualnych stacji w</p>

	<p>skład których wchodzi stacje już istniejące,</p> <p>13.Oprogramowanie do wirtualizacji stacji roboczych musi zapewniać możliwość tworzenia grup wirtualnych stacji roboczych, w których:</p> <ul style="list-style-type: none"> a) przypisanie użytkownika do wirtualnej stacji roboczej następuje na stałe po pierwszym zalogowaniu i wówczas wszystkie dane użytkownika pozostają zapisane pomimo jego wylogowania b) przypisanie użytkownika do wirtualnej stacji roboczej następuje przy każdym kolejnym logowaniu <p>14.Oprogramowanie musi zawierać mechanizmy obsługi przekierowania profili i ustawień użytkownika niezależnie od mechanizmów oferowanych przez system operacyjny w wirtualnym desktopie (natywna wirtualizacja profili użytkownika).</p> <p>15.Oprogramowanie do wirtualizacji stacji roboczych musi zapewniać mechanizm pozwalający na podłączenie do wirtualnej stacji roboczej urządzeń typu dysk usb, pendrive poprzez włączenie do portu USB urządzenia fizycznego na którym zainstalowana jest aplikacja klienta,</p> <p>16.Oprogramowanie do wirtualizacji stacji roboczych musi zapewniać wbudowane mechanizmy do dostarczania zwirtualizowanych aplikacji poprzez dostarczenie całej aplikacji do wirtualnej stacji roboczej lub jej streaming,</p> <p>17.Warstwa wirtualizacji musi posiadać możliwość alokacji dla wirtualnych stacji roboczych większej ilości pamięci RAM niż fizycznie zainstalowanej w serwerze w celu osiągnięcia maksymalnego możliwego stopnia konsolidacji,</p> <p>18.Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania wirtualnych stacji roboczych jedno lub wieloprocesorowych, posiadających od 1 do 4 procesorów,</p> <p>19.Oprogramowanie do wirtualizacji musi zapewnić obsługę aplikacji 3D wewnątrz wirtualnych stacji roboczych wykorzystujących API OpenGL lub DirectX bez obciążania procesorów fizycznych w serwerach.</p> <p>20.Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania wirtualnych stacji roboczych posiadających do 255 GB pamięci RAM,</p> <p>21.Oprogramowania musi umożliwiać monitorowanie pamięci masowych, obciążenia procesorów oraz urządzeń sieciowych.</p> <p>22.Oprogramowanie musi umożliwiać sprawdzanie stanu serwerów pośredniczących w procesie dostarczania maszyn wirtualnych.</p> <p>23.Oprogramowanie musi umożliwiać szybkie diagnozowanie ewentualnych nieprawidłowości w działaniu środowiska i wyświetlanie odpowiedniej sesji użytkownika, która powoduje nieprawidłowości.</p>
Wdrożenie:	<p>Wykonawca dla dostarczenia rozwiązania alternatywnego do VMware Horizon, zrealizuje wdrożenie, które będzie polegać na:</p> <ol style="list-style-type: none"> 1. Instalacji niezbędnych elementów infrastruktury, w tym elementy warstwy wirtualizacyjnej oraz serwerów zarządzających wchodzących w skład rozwiązania 2. Konfiguracji dostarczonego rozwiązania wraz z integracją z systemami wewnętrznymi 3. Przygotowaniu wzorcowego obrazu systemu operacyjnego dla

	<p>VDI wg wytycznych zamawiającego</p> <ol style="list-style-type: none">4. Konfiguracji do 3 puli desktopów zgodną z wytycznymi zamawiającego5. Konfiguracji mechanizmów dostępowych do systemów VDI dla użytkowników6. Weryfikacja poprawności działania tworzenia desktopów użytkowników i ich konfiguracji7. Przygotowanie dokumentacji powdrożeniowej <p>Wykonawca dla przypadku rozszerzenia licencji VMware Horizon przeprowadzi rozszerzenie licencji i skonfiguruje rozwiązanie do korzystania z sumarycznie trzech serwerów</p>
Wsparcie techniczne:	<p>Rozwiązanie musi posiadać wsparcie techniczne w języku polskim na okres do dnia 06.11.2025 r.</p> <ol style="list-style-type: none">a) Pomoc techniczna wraz z producentem rozwiązańb) Dostęp do Upgrade, Update i ServicePackc) Pomoc techniczna w języku polskim w Godzinach Pracyd) Dostęp do polskiego portalu pomocy techniczneje) Dostęp do polskiej bazy wiedzyf) Telefoniczna pomoc techniczna w języku polskimg) Mailowa pomoc techniczna w języku polskimh) Zdalna pomoc techniczna w języku polskimi) Obsługa zgłoszeń typu „How to”