



OPIS PRZEDMIOTU ZAMÓWIENIA

„Dostawa oprogramowania”

– nr postępowania FH/02/12/24

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 4 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">Licencja nie może ograniczać ilości użytkowników, których w danym momencie sesje są nadzorowane,Licencja powinna umożliwiać nadzorowanie dostęp do co najmniej 25 usług,Wsparcie producenta, które obejmuje roczne aktualizacje oraz wsparcie liczone od dnia 31.12.2024.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">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.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 połączenia 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 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, video 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 3 - 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"> 1. Pakiet licencji musi zawierać prawo do korzystania dla min. 2 oprogramowań do kontroli dostępu do sieci komputerowej, działających w klastrze niezawodnościowym; 2. 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"> 3. Wspar 4. 5. cie producenta, które obejmuje aktualizacje oraz wsparcie przez okres 12 mc. aktywności subskrypcji.
Cechy oprogramowania	<ol style="list-style-type: none"> 1. Rozwiązanie musi zapewnić mechanizmy kontroli dostępu do sieci informatycznej realizowane z wykorzystaniem protokołu IEEE 802.1x, 2. Autentykacja oraz autoryzacja muszą odbywać się na poziomie przełącznika sieciowego, 3. 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, 4. Rozwiązanie musi wspierać przełączniki wiodących producentów sprzętu sieciowego na rynku, w szczególności urządzenia Dell Powerconnect N5548 (obecnie posiadane przez Zamawiającego), 5. Rozwiązanie musi bazować (w zakresie mechanizmów autentykacji/autoryzacji) na standardach Radius, 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,

	<ol style="list-style-type: none">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 4 – 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	<ol style="list-style-type: none"> 1. Oprogramowanie powinno zostać dostarczone w formie Subskrypcji na okres 12 miesięcy 2. Oprogramowanie musi umożliwić docelowo jednoczesną pracę 200 użytkownikom, 3. Dostarczone licencje muszą umożliwić instalację i użytkowanie niezbędnej ilości hostów (hypervisor) wymaganych do uruchomienia wirtualnych maszyn stacji roboczych, 4. Dostarczone licencje mają umożliwić pracę 100, w prawie opcji do 200, użytkowników jednocześnie na systemie Windows 10, która to licencja na Windows 10 jest zapewniona przez posiadaną obecnie przez Zamawiającego licencje.
Cechy oprogramowania	<ol style="list-style-type: none"> 1. Oferowane rozwiązanie musi zapewniać możliwość instalacji wszystkich jego komponentów w infrastrukturze Zamawiającego, 2. Oprogramowanie do wirtualizacji stacji roboczych musi wspierać Microsoft Windows 10, Windows 2012 jako systemy operacyjne zainstalowane na wirtualnych stacjach roboczych, 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. 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, 5. Oprogramowanie do wirtualizacji stacji roboczych musi integrować się z usługami terminalowymi Microsoft RDSH oraz Windows Server 2012R2/2016 udostępniając użytkownikom możliwość połączenia się

	<p>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 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 wieloprocessorowych, posiadających od 1 do 4 procesorów,</p> <p>19. Oprogramowanie do wirtualizacji musi zapewnić obsługę aplikacji 3D wewnątrz wirtualnych stacji roboczych wykorzystujących API</p>
--	--

	<p>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 VDI wg wytycznych zamawiającego 4. Konfiguracji do 3 puli desktopów zgodną z wytycznymi zamawiającego 5. Konfiguracji mechanizmów dostępowych do systemów VDI dla użytkowników 6. Weryfikacja poprawności działania tworzenia desktopów użytkowników i ich konfiguracji 7. 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 rozwiązań b) Dostęp do Upgrade, Update i ServicePack c) Pomoc techniczna w języku polskim w Godzinach Pracy d) Dostęp do polskiego portalu pomocy technicznej e) Dostęp do polskiej bazy wiedzy f) Telefoniczna pomoc techniczna w języku polskim g) Mailowa pomoc techniczna w języku polskim h) Zdalna pomoc techniczna w języku polskim i) Obsługa zgłoszeń typu „How to”