Załącznik nr 1 do Zapytania Ofertowego

Opis przedmiotu zamówienia (OPZ)

1. Przedmiot i zakres zamówienia

1. Przedmiotem zamówienia jest dostawa licencji terminowych Systemu Zarządzania Dostępami Uprzywilejowanymi klasy PAM/PIM, dalej „System PAM", na okres 12 miesięcy dla 5 użytkowników wskazanych przez Zamawiającego, wraz z dostępem do wsparcia technicznego i aktualizacji przez ten okres.
2. Zamówienie obejmuje dostawę licencji oraz udostępnienie oprogramowania i dokumentacji producenta niezbędnych do samodzielnej instalacji, konfiguracji i użytkowania Systemu PAM przez Zamawiającego.
3. Zamówienie nie obejmuje usług wdrożeniowych, instalacji, konfiguracji, integracji, migracji danych, uruchomienia produkcyjnego, szkoleń ani usług administracyjnych wykonywanych przez Wykonawcę.
4. Instalację, konfigurację, integrację, uruchomienie i bieżącą administrację Systemem PAM Zamawiający wykona we własnym zakresie.
5. Wszystkie wymagane funkcjonalności muszą być dostępne w dostarczonym zakresie licencji. Cena oferty musi obejmować wszystkie licencje i moduły niezbędne do spełnienia OPZ przez okres 12 miesięcy.
6. Licencje nie mogą ograniczać liczby chronionych systemów docelowych.
7. Dostarczone oprogramowanie i licencje muszą pochodzić z legalnego źródła oraz uprawniać Zamawiającego do użytkowania oprogramowania, korzystania ze wsparcia i pobierania aktualizacji na terytorium Polski.

2. Wymagania architektoniczne i wysoka dostępność

1. System PAM musi umożliwiać pracę w modelu lokalnym, w infrastrukturze Zamawiającego, na platformie wirtualizacyjnej VMware.
2. System PAM musi umożliwiać bezagentowe pośredniczenie w sesjach uprzywilejowanych, tj. bez konieczności instalowania agenta Systemu PAM na systemie docelowym, do którego nawiązywana jest sesja.
3. Rozwiązanie musi być kompletne. Dopuszcza się architekturę jednokomponentową lub wielokomponentową, pod warunkiem objęcia ceną oferty wszystkich elementów oprogramowania i licencji niezbędnych do spełnienia OPZ.
4. System PAM musi umożliwiać zabezpieczanie dostępu do maszyn fizycznych, maszyn wirtualnych, serwerów, urządzeń sieciowych i bezpieczeństwa, aplikacji oraz baz danych w zakresie protokołów i integracji wymaganych w OPZ.

5. System PAM musi umożliwiać uruchomienie co najmniej dwóch instancji w konfiguracji wysokiej dostępności typu active-active.
6. W razie niedostępności jednej instancji druga instancja musi umożliwiać dalszą obsługę użytkowników oraz zestawianie nowych sesji, zgodnie z mechanizmem wysokiej dostępności wspieranym przez producenta. Nie wymaga się zachowania bez przerwy sesji zestawionych przez instancję, która uległa awarii.
7. Cena oferty musi obejmować uprawnienia licencyjne niezbędne do równoczesnego uruchomienia dwóch instancji Systemu PAM w konfiguracji active-active przez cały okres 12 miesięcy. Zamawiający nie może być zobowiązany do ponoszenia dodatkowych opłat licencyjnych lub aktywacyjnych za drugą instancję ani za funkcję active-active.
8. Jeżeli architektura rozwiązania wymaga komponentu arbitrażowego, świadka klastra lub innego komponentu niezbędnego do działania konfiguracji active-active, oprogramowanie i wymagane uprawnienia do korzystania z tego komponentu muszą być objęte ceną oferty.
9. Zamawiający zapewni we własnym zakresie zasoby infrastruktury wirtualnej, sieciowej i dyskowej oraz samodzielnie wykona instalację i konfigurację Systemu PAM.

3. Wymagania licencyjne i wsparcie

1. Dostarczone licencje muszą umożliwiać korzystanie ze wszystkich funkcjonalności wymaganych w OPZ przez 5 użytkowników.
2. Uruchomienie dwóch instancji w konfiguracji active-active nie może wymagać zakupu dodatkowych uprawnień użytkowników ponad zakres objęty ceną oferty.
3. Licencje muszą obejmować co najmniej: zarządzanie kontami uprzywilejowanymi i ich poświadczeniami, zarządzanie kluczami SSH, pośredniczenie w dostępie uprzywilejowanym, monitorowanie i rejestrowanie sesji, odtwarzanie nagrań, audyt i raportowanie.
4. W ramach dostarczonych licencji System PAM musi umożliwiać korzystanie z prywatnego sejfu użytkownika do przechowywania haseł oraz plików.
5. Przez okres 12 miesięcy Zamawiający musi posiadać dostęp do aktualizacji producenta oraz wsparcia producenta lub podmiotu uprawnionego do świadczenia wsparcia dla oferowanego rozwiązania, z możliwością eskalacji zgłoszeń do producenta.
6. Wyłączenie usług wdrożeniowych z zakresu zamówienia nie wyłącza prawa Zamawiającego do korzystania ze wsparcia technicznego objętego dostarczonym pakietem.

7. Cena oferty musi obejmować wszystkie uprawnienia do korzystania z systemów operacyjnych, baz danych oraz innych komponentów oprogramowania niezbędnych do działania Systemu PAM, w tym w wymaganej konfiguracji active-active. Zamawiający nie może być zobowiązany do zakupu dodatkowych licencji na te komponenty. Wymaganie nie dotyczy zapewnianej przez Zamawiającego platformy wirtualizacyjnej VMware.

4. Wymagania funkcjonalne

4.1. Zarządzanie kontami i poświadczeniami

1. System PAM musi umożliwiać zarządzanie co najmniej: kontami lokalnymi systemów Windows i Unix/Linux, kontami domenowymi Active Directory, kontami administracyjnymi platform wirtualizacyjnych, kontami administracyjnymi urządzeń sieciowych i bezpieczeństwa, kontami baz danych oraz kluczami SSH.
2. System PAM musi umożliwiać przypisywanie użytkownikom uprawnień do określonych systemów docelowych i poświadczeń.
3. System PAM musi umożliwiać ograniczenie lub wyłączenie możliwości ujawnienia użytkownikowi hasła konta uprzywilejowanego, przy jednoczesnym umożliwieniu zestawienia sesji do systemu docelowego.
4. System PAM musi umożliwiać wykorzystanie prywatnych kont uprzywilejowanych użytkowników niezapisanych w Systemie PAM.
5. System PAM musi umożliwiać tworzenie lub aktywowanie poświadczeń typu Just-in-Time (JIT) na czas trwania sesji.

4.2. Dostęp do systemów docelowych

1. System PAM musi umożliwiać pośredniczenie w dostępie do systemów docelowych dla użytkowników wewnętrznych, w tym domenowych, oraz użytkowników zewnętrznych.
2. System PAM musi umożliwiać zestawianie i rejestrowanie sesji co najmniej przez RDP i SSH.
3. System PAM musi umożliwiać pośredniczenie w dostępie do zasobów przez VNC oraz HTTP/HTTPS.
4. System PAM musi umożliwiać dostęp do systemów docelowych przez przeglądarkę internetową oraz z wykorzystaniem natywnych klientów RDP i SSH.
5. System PAM musi umożliwiać pośredniczenie w dostępie do baz danych Microsoft SQL Server, Oracle i PostgreSQL z wykorzystaniem klienta bazodanowego.

6. System PAM musi umożliwiać zastosowanie komponentu pośredniczącego w komunikacji z systemami docelowymi znajdującymi się w wydzielonych segmentach sieci. Dopuszcza się formę komponentu wspieraną przez producenta oferowanego rozwiązania.

4.3. Uwierzytelnianie i uprawnienia

1. System PAM musi umożliwiać integrację z Active Directory lub LDAP.
2. System PAM musi zapewniać uwierzytelnianie wieloskładnikowe użytkowników.
3. System PAM musi umożliwiać wykorzystanie co najmniej jednego z mechanizmów integracji uwierzytelniania: RADIUS, SAML lub OpenID, albo uwierzytelniania za pomocą aplikacji generującej kody jednorazowe.
4. System PAM musi umożliwiać nadawanie uprawnień według ról i przynależności do grup użytkowników, w tym grup pochodzących ze zintegrowanej usługi katalogowej.
5. System PAM musi umożliwiać ograniczenie dostępu do systemów docelowych i poświadczeń według użytkownika lub grupy, roli, systemu docelowego lub grupy systemów, poświadczenia oraz dni i godzin dostępu.

4.4. Polityki dostępu i zatwierdzanie

1. System PAM musi umożliwiać rozdzielenie prawa do rozpoczęcia sesji od prawa do podglądu hasła.
2. System PAM musi umożliwiać wymaganie podania uzasadnienia rozpoczęcia sesji lub podglądu hasła.
3. System PAM musi umożliwiać uzależnienie rozpoczęcia sesji lub podglądu hasła od akceptacji przez uprawnioną osobę, w tym stosowanie wielopoziomowego zatwierdzania.
4. System PAM musi umożliwiać czasowe udostępnienie poświadczenia użytkownikowi poza standardowo przypisaną polityką dostępu.
5. System PAM musi umożliwiać zdefiniowanie dostępu awaryjnego, pozwalającego na rozpoczęcie sesji lub podgląd hasła bez standardowej akceptacji.
6. System PAM musi umożliwiać kontrolę dostępu do raportów i nagrań sesji według uprawnień użytkowników.

4.5. Zarządzanie hasłami

1. System PAM musi umożliwiać automatyczne generowanie haseł z uwzględnieniem konfigurowalnej długości oraz użycia małych i wielkich liter, cyfr i znaków specjalnych.
2. System PAM musi umożliwiać generowanie unikalnych haseł dla zarządzanych kont.

3. System PAM musi umożliwiać zmianę hasła na systemie docelowym zgodnie z polityką oraz automatyczną zmianę hasła po jego podglądzie.
4. System PAM musi umożliwiać zestawienie sesji do systemu docelowego z wykorzystaniem przechowywanych poświadczeń, bez ujawniania użytkownikowi hasła konta uprzywilejowanego.

4.6. Monitorowanie i kontrola sesji

1. System PAM musi umożliwiać podgląd aktywnej sesji w czasie rzeczywistym przez uprawnioną osobę.
2. System PAM musi umożliwiać przerwanie aktywnej sesji przez uprawnioną osobę.
3. System PAM musi umożliwiać przerwanie wszystkich aktywnych sesji pośredniczonych przez System PAM oraz zablokowanie dostępu użytkowników w sytuacji krytycznej.
4. System PAM musi umożliwiać audyt poleceń w sesjach SSH oraz definiowanie list poleceń dozwolonych i zabronionych.
5. System PAM musi umożliwiać zablokowanie zdefiniowanego polecenia oraz rozłączenie sesji po wykryciu polecenia objętego odpowiednią polityką.
6. System PAM musi umożliwiać automatyczne zablokowanie dostępu użytkownika, który próbował wykonać polecenie zabronione zgodnie z zastosowaną polityką.

4.7. Nagrywanie i odtwarzanie sesji

1. System PAM musi umożliwiać nagrywanie i odtwarzanie sesji RDP i SSH bez instalowania agenta Systemu PAM na systemie docelowym.
2. System PAM musi umożliwiać konfigurację jakości nagrań graficznych oraz okresu przechowywania nagrań.
3. System PAM musi umożliwiać pobranie zarejestrowanych nagrań sesji przez uprawnionego użytkownika.
4. System PAM musi umożliwiać rejestrowanie danych wprowadzanych z klawiatury w sesjach SSH i RDP oraz ich przeszukiwanie według wskazanych słów kluczowych.
5. System PAM musi umożliwiać wskazanie w nagraniu momentów aktywności użytkownika.
6. System PAM musi umożliwiać definiowanie ustawień rejestrowania sesji zależnie od polityki dostępu, systemu docelowego lub poświadczenia.

4.8. Audyt i raportowanie

1. System PAM musi prowadzić rejestr zdarzeń systemowych i działań administracyjnych.

2. System PAM musi umożliwiać identyfikację użytkownika korzystającego z konta uprzywilejowanego w sesji pośredniczonej przez System PAM.
3. System PAM musi umożliwiać raportowanie zmian wprowadzonych przez użytkowników oraz logowań do Systemu PAM.
4. System PAM musi umożliwiać prezentację aktywnych i historycznych sesji oraz informacji o ich statusie.
5. System PAM musi umożliwiać analizę informacji o źródle, czasie rozpoczęcia i długości sesji do systemu docelowego.
6. System PAM musi umożliwiać ograniczenie dostępu do danych audytowych i raportów zgodnie z uprawnieniami użytkowników.

5. Identyfikacja rozwiązania

1. Wykonawca wskaże w ofercie nazwę rozwiązania wraz z oferowanym pakietem licencyjnym.
2. Wymagane funkcjonalności muszą być dostępne w dostarczonym oprogramowaniu i objęte oferowanym pakietem licencyjnym w dniu dostawy. Nie dopuszcza się deklarowania zgodności na podstawie funkcjonalności planowanych w przyszłych wersjach ani wymagających dodatkowego zakupu nieobjętego ceną oferty.

6. Odbiór dostawy

1. Warunkiem odbioru jest dostarczenie licencji na okres 12 miesięcy dla 5 użytkowników, obejmujących zakres wymagany w OPZ, w tym uprawnienia do konfiguracji active-active, wsparcia i aktualizacji.
2. Wykonawca przekaże licencje w postaci elektronicznej wraz z informacjami niezbędnymi do ich aktywacji lub przypisze uprawnienia licencyjne do konta Zamawiającego, zgodnie ze sposobem dostarczania licencji przez producenta, oraz zapewni dostęp do oprogramowania i dokumentacji producenta.
3. Odbiór dostawy zostanie potwierdzony protokołem odbioru. Odbiór nie jest uzależniony od wykonania przez Zamawiającego wdrożenia produkcyjnego.

7. Termin realizacji i okres licencji

1. Wykonawca dostarczy licencje i zapewni dostęp do oprogramowania w terminie 14 dni kalendarzowych od dnia zawarcia umowy.
2. Okres obowiązywania licencji, wsparcia i dostępu do aktualizacji wynosi 12 miesięcy od dnia dostarczenia kompletu uprawnień licencyjnych umożliwiających korzystanie z Systemu PAM.