Nazwa	Minimalne wymagania co do oprogramowania
Typ	System klasy PAM – zarządzający dostępem uprzywilejowanym
Wymagania szczegółowe	Zamawiający wymaga funkcjonalności w zakresie minimum: Ogólne - architektura 1. System PAM musi być rozwiązaniem bezagentowym tj. umożliwiającym nawiązywanie sesji z wykorzystaniem serwerów proxy bez potrzeby instalacji oprogramowania (agenta) na systemie, do którego będzie nawiązywana sesja, umożliwiającym uwierzytelnianie wieloskładnikowe i obsługujące wiele platform i systemów operacyjnych. System PAM ma zabezpieczać dostęp do maszyn fizycznych, maszyn wirtualnych, sprzętu sieciowego m.in. routery, przełączniki, zapory sieciowe, aplikacje, bazy danych itp. 2. System musi być dostarczany w formie zamkniętej platformy wirtualnej przygotowanej do implementacji w infrastrukturze Hyper-V lub VMware . Przez zamkniętą platformę rozumiemy wyspecjalizowane rozwiązanie, w ramach którego zainstalowana jest całość oprogramowania (system operacyjny, baza danych, aplikacja), realizująca wszystkie funkcjonalności systemu. 3. Rozwiązanie nie może wymagać wdrożenia kolejnych komponentów jako osobne maszyny wirtualne lub fizyczne. Do prawidłowego działania wszystkich dostępnych funkcjonalności wymagane jest posiadanie tylko jednej maszyny wirtualnej. 4. Rozwiązanie musi oferować wdrożenie drugiej instancji i konfiguracji klastra typu active-active. Licencjonowanie 1. System PAM musi zostać dostarczony z kompletem licencji dla co najmniej 15 użytkowników, którzy będą korzystali z Systemu PAM, minimum dla następującej liczby funkcjonalności: a. Ochrona kont uprzywilejowanych, b. Ochrona kluczy SSH, c. Zarządzanie i monitorowanie sesji uprzywilejowanych, d. Rejestrowanie sesji uprzywilejowanych e. Raportowanie wykorzystania kont uprzywilejowanych, 2. Dostarczone licencje na System PAM do ochrony kont uprzywilejowanych nie mogą mieć ograniczeń czasowych. Dostarczone licencje będą udzielone bezterminowo. 3. Dostarczone licencje na system PAM nie mogą w żaden sposób limitować ilości chronionych systemów docelowych. 4. System powinien być dostarczony wraz z trzyletnim serwisem umożliwiającym korzystanie ze wsparcia producenta oraz dystrybutora oraz pobieranie aktualizacji przygotowanych przez producenta. 5. W ramach zakupionych licencji użytkownicy systemu muszą posiadać możliwość skorzystania z mechanizmu prywatnego sejfu. Funkcjonalności 1) System PAM musi zapewniać możliwość zarządzania (w szczególności): a) Użytkownikami na systemach operacyjnych: Windows, Unix/Linux, b) Kontami domenowymi: MS Active Directory, c) Kontami lokalnymi: VMware ESX/ESXi, d) Kontami na urządzeniach m.in.: Cisco, Aruba, Alcatel, CheckPoint, Fortigate, Huawei, IBM AIX, Brocade, e) Kontami baz danych: Microsoft SQL, Oracle, MySQL, PostgreSQL f) Kontami do zarządzania i monitorowania serwerów: m.in. iLO, iDRAC, g) Kontami aplikacji webowych: Facebook, Google, Twitter, Linkedin, Instagram, Openstack, AWS h) Kontami w innych nie wymienionych systemach/urządzeniach do których dostęp odbywa się po protokołach: SSH, RDP,VNC, TELNET, HTTP/HTTPS, i) Kluczami SSH. 2) System PAM musi umożliwiać utworzenie poświadczeń typu Just-in-Time (JIT), które będą tworzone lub aktywowane na czas trwania sesji.

	3) System PAM musi umożliwiać usługę pośredniczenia w dostępie do systemów i urządzeń dla użytkowników domenowych oraz użytkowników zewnętrznych, rejestrując obsługiwane sesje, oraz obsługując minimum następujące protokoły: SSH, RDP,VNC, TELNET, HTTP/HTTPS, X11. 4) System PAM musi wspierać również protokoły bez rejestracji sesji: Cassandra, Elasticsearch, LDAP, LDAPS, MongoDB, MySQL, Oracle, PostgreSQL, Redis, Solr, SQL Server, RDS Sybase, Windows RM, Windows RPC, Windows SMB. 5) System PAM musi umożliwiać dostęp użytkowników do systemu docelowego następującymi narzędziami: a) przeglądarka internetowa, b) klient RDP, c) klient protokołu SSH/Telnet (np. putty), d) klient serwerów bazodanowych m.in. DBeaver. 6) System PAM musi wspierać minimum następujące mechanizmy uwierzytelniania: LDAP, RADIUS, Tacacs Active Directory, OpenID, SAML. 7) System PAM musi zapewniać możliwość dwuskładnikowego uwierzytelniania. 8) System PAM musi wspierać integrację z rozwiązaniami dwuskładnikowego uwierzytelnienia takimi jak Google Authenticator i Microsoft Authenticator. 9) System PAM musi obsługiwać monitorowanie i ochronę kilkudziesięciu jednoczesnych połączeń od jednego użytkownika końcowego, do różnych systemów poprzez wiele lub jedno konto uprzywilejowane. 10) System PAM musi ograniczać administratorowi możliwość dostępu do haseł lub ograniczać podgląd do haseł uprzywilejowanych. 11) System PAM musi umożliwiać budowanie polityk kontroli dostępu w oparciu o role, np. na podstawie przynależności do grup AD/LDAP. 12) System PAM musi umożliwiać budowanie polityk kontroli dostępu wymuszającej: a) podanie powodu rozpoczęcia sesji, b) podanie powodu podglądu hasła, c) konieczność akceptacji rozpoczęcia sesji przez innego administratora/ów, d) konieczność akceptacji podglądu hasła przez innego administratora/ów, e) zakresu godzin, dni oraz dat kiedy użytkownik systemu będzie miał dostęp do poświadczeń. 13) System PAM musi umożliwiać udostępnienie poświadczenia do użytku dla użytkownika poza polityką dostępową, która jest do niego przypisana. Udostępnienie musi dawać możliwość wyboru długości trwania takiego dostępu. 14) System PAM musi posiadać log dla wszystkich zdarzeń systemowych. 15) System PAM musi umożliwiać wskazanie kont użytkowników, które realizowały logowanie do stacji/serwera. 16) System PAM musi umożliwiać raportowanie wszystkich zmian wprowadzonych przez administratorów. 17) System PAM musi umożliwiać raportowanie wszystkich logowań do systemu. 18) System PAM musi umożliwiać raportowanie oparte na nietypowym źródle, czasie i długości połączenia do systemu docelowego. 19) Rozwiązanie musi posiadać graficzną wizualizację przedstawiającą status bezpieczeństwa aktywnych oraz historycznych sesji do systemów zdalnych. 20) System PAM musi umożliwiać ograniczenie dostępu do raportów dla wskazanej grupy użytkowników lub administratorów. 21) System PAM musi mieć możliwość zmiany wartości hasła na systemie docelowym zgodnie z ustawioną polityką m.in.: a) umożliwiać zdefiniowanie wymagań na: długość hasła, znaki w haśle (małe i duże litery, cyfry, znaki specjalne), b) generować automatycznie hasła kont systemów docelowych w sposób pseudo losowy, c) generować unikalne hasła dla konta systemów docelowych, d) wymuszać automatyczną zmianę hasła po jego podglądzie. 22) System PAM musi umożliwiać transparentne połączenie do systemu docelowego, bez konieczności podawania przez użytkownika hasła konta uprzywilejowanego. 23) System PAM musi umożliwiać podgląd zestawionej sesji w czasie rzeczywistym. 24) System PAM musi umożliwiać przerwanie i/lub zawieszenie trwającej sesji. 25) System PAM musi posiadać menu pozwalające na zawieszenie lub przerwanie wszystkich sieci oraz zablokowanie dostępu do samego rozwiązania w przypadku sytuacji krytycznej.

	26) System PAM musi umożliwiać ograniczanie dostępu do systemów docelowych oraz tworzenie białych i czarnych list poleceń wykonywanych w systemie docelowym (audyt poleceń). 27) Audyt poleceń musi umożliwiać podjęcie co najmniej akcji, zablokuj polecenie i rozłącz sesję po wykryciu audytowanego polecenia a także automatyczne umieszczenie na liście blokowanych użytkowników użytkownika, który próbował wykonać blokowane polecenie. 28) Nagrywanie sesji nie może mieć żadnego wpływu na wydajność systemu docelowego. 29) System PAM musi umożliwiać konfigurację parametrów nagrań, w tym: a) ilości klatek na sekundę, b) jakości pojedynczej klatki, c) formatu pojedynczej klatki: jpg lub png, d) długości przechowywania nagrań. 30) System PAM musi rejestrować znaki wprowadzone z klawiatury przez użytkownika co najmniej dla sesji SSH i RDP oraz umożliwiać szybkie przeszukiwanie zapisanych danych pod kątem występowania wskazanych słów kluczowych. 31) System PAM musi umożliwiać utworzenie oddzielnego zestawu ustawień w oparciu o: a) politykę dostępową, b) urządzenie docelowe, c) poświadczenie, d) adresu źródłowego. 32) System PAM musi umożliwiać odtworzenie i pobranie zarejestrowanych nagrań sesji. 33) Oprogramowanie dostarczone w ramach realizacji zamówienia musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski. W przypadku zaproponowania rozwiązania z innego kanału dystrybucji Wykonawca musi przedstawić dokument potwierdzający, iż zaoferowany produkt posiada wsparcie producenta na terenie Polski. 34) System PAM musi być kompletny i pozwalać na uruchomienie minimum następujących funkcjonalności: a) zarządzać kontami uprzywilejowanymi w ramach organizacji, b) monitorować wykorzystanie kont uprzywilejowanych, c) nagrywać i archiwizować sesje zdalne, d) gwarantować skalowalność rozwiązania w przypadku dodawania nowych zasobów oraz nowych usług, 35) System PAM musi umożliwiać personalizację wyglądu aplikacji co najmniej po przez umieszczenie logo zamawiającego w głównym oknie aplikacji.
Wymagania dodatkowe	Zamawiający wymaga przeprowadzenia wdrożenia w zakresie minimum: Przygotowania maszyny wirtualnej na serwerze wskazanym przez Zamawiającego Przypisania niezbędnych licencji Asysty i pomocy (w formie zdalnej) przy konfiguracji systemu, dodawania użytkowników, tworzenia reguł i uprawnień, dodawaniu urządzeń i rozwiązań do których to będzie zapewniał dostęp PAM oraz innych prac niezbędnych do prawidłowego skonfigurowania rozwiązania. Zamawiający wymaga przeznaczenia przez Wykonawcę na prace wdrożeniowe minimum 15h
Ilość	1 sztuka