



The Security Division of EMC

RSA® Authentication Manager Express

Często zadawane pytania

Niniejszy dokument jest podzielony na następujące sekcje:

Spis treści

Sprzedaż a pozycja na rynku.....	1
Produkt AMX	2
Licencje, ceny, pakiety	4
Mechanizm uwzględniania ryzyka	4
Migracja i plany na przyszłość.....	5

Sprzedaż a pozycja na rynku

Pytanie: Czym jest rozwiązanie RSA Authentication Manager Express (AMX)?

Odpowiedź: Rozwiązanie AMX to mechanizm uwierzytelniania przeznaczony dla firm z mniej niż 2500 użytkownikami, które jeszcze nie mają własnego rozwiązania do bezpiecznego uwierzytelniania. Widząc ogromne możliwości rozwoju tego segmentu rynku, firma RSA postanowiła wprowadzić atrakcyjne cenowo i wyróżniające się na tle konkurencji rozwiązanie AMX.

Pytanie: Czym się różni rozwiązanie AMX od innych rozwiązań przeznaczonych dla firm tej wielkości?

Odpowiedź: Zauważyliśmy, że w wielu firmach poszukuje się mechanizmów uwierzytelniania za pośrednictwem wiadomości SMS. Rozwiązanie AMX udostępnia funkcję uwierzytelniania na żądanie (SMS) w postaci samodzielnej metody, a dodatkowo w ramach połączonej licencji można korzystać także z uwierzytelniania z uwzględnieniem poziomu ryzyka. Tylko w ofercie RSA można znaleźć produkty tego typu przeznaczone dla firm mających do 2500 użytkowników.

Pytanie: Dlaczego klienci poszukują produktów udostępniających funkcje i możliwości rozwiązania AMX?

Odpowiedź: Nasi docelowi klienci dostrzegają potrzebę pogłębienia współpracy z podmiotami zewnętrznymi (wykonawcy, dostawcy, partnerzy itp.) lub pracownikami przy pomocy dostępu zdalnego. Jednocześnie firmy te stanowią łatwy cel dla przestępców, ponieważ często nie mają infrastruktury zabezpieczeń (czego dowodem są udane ataki na podobne firmy w przeszłości), ani nie korzystają z procedur stosowanych w większych firmach. Jeśli dodamy do tego rosnące wymagania w zakresie zgodności z przepisami i sprawozdawczości, mamy klienta będącego idealnym celem cyberprzestępców. Należy także pamiętać, że wdrażanie sprzętowych lub programowych mechanizmów uwierzytelniania w firmach tej wielkości jest trudniejsze — często z powodu kosztów oraz specyficznego podejścia do zarządzania personelem.



The Security Division of EMC

RSA® Authentication Manager Express Często zadawane pytania

Pytanie: Do kogo jest skierowany produkt?

Odpowiedź: Idealny klient to firma mająca 50–1500 użytkowników, która obecnie nie ma wdrożonego mechanizmu uwierzytelniającego („świeży klient”), może być w trakcie wdrażania systemu SSL VPN, aplikacji WWW lub klienta Citrix, a także stoi przed koniecznością spełnienia określonych wymogów ustawowych.

Pytanie: W jakiej branży działa firma docelowego klienta (lub jakiego typu jest to firma)?

Odpowiedź: Opieka zdrowotna (kliniki), sprzedaż detaliczna, technologie, firmy usługowe.

Pytanie: Czym się różni rozwiązanie RSA Authentication Manager Express od tradycyjnego produktu firmy RSA — rozwiązania SecurID/RSA Authentication Manager?

Odpowiedź: Istnieje wiele różnic. Rozwiązanie AMX obsługuje funkcje uwierzytelniania z uwzględnieniem poziomu ryzyka oraz na żądanie (SMS), ale nie obsługuje tokenów sprzętowych ani programowych. Produkt RSA Authentication Manager obsługuje tokeny sprzętowe i programowe oraz uwierzytelnianie na żądanie (SMS). Z rozwiązania AMX może korzystać do 2500 użytkowników, a z oprogramowania RSA Authentication Manager nawet milion użytkowników. Główną różnicą jest jednak docelowy segment rynku: rozwiązanie AMX jest przeznaczone dla firm mających nie więcej niż 2500 użytkowników, a produkt RSA Authentication Manager — także dla dużych korporacji.

Pytanie: Czym najbardziej wyróżnia się rozwiązanie AMX?

Odpowiedź: Głównym czynnikiem wyróżniającym jest mechanizm uwierzytelniania z uwzględnieniem poziomu ryzyka (ang. Risk Based Authentication — RBA), który rozróżnia i uwierzytelnia użytkowników na podstawie urzędzeń, z których korzystają, oraz profilów behawioralnych. Firma RSA stosuje tę technologię od wielu lat w rozwiązaniach dla bankowości internetowej. Dotychczas skorzystało z niej ponad 250 milionów użytkowników, a teraz dołączają do nich kolejni.

Pytanie: Czy klient może używać rozwiązania AMX jako samodzielnej metody uwierzytelniania za pośrednictwem wiadomości SMS?

Odpowiedź: Tak. Warto jednak zaznaczyć, że w ramach licencji na rozwiązanie AMX klient uzyskuje także funkcję uwierzytelniania z uwzględnieniem poziomu ryzyka.

Produkt AMX

Pytanie: Czy wraz z rozwiązaniem RSA Authentication Manager Express można sprzedawać tokeny?

Odpowiedź: Nie w przypadku produktu RSA Authentication Manager 1.0. Tokeny sprzętowe i programowe firmy RSA (aplety instalowane na urządzeniach przenośnych i komputerach) nie są obsługiwane w tej wersji. Jeśli tokeny sprzętowe lub programowe są wymagane, klienci powinni nabyć produkt RSA Authentication Manager, który obsługuje oba rodzaje tokenów oraz uwierzytelnianie na żądanie (SMS).

Pytanie: Jakie platformy i systemy operacyjne obsługuje ten produkt?

Odpowiedź: Rozwiązanie RSA Authentication Manager Express jest sprzedawane jako samodzielne urządzenie o wzmocnionych zabezpieczeniach z systemem rPath Linux (appliance).



The Security Division of EMC

RSA® Authentication Manager Express Często zadawane pytania

Pytanie: Jakie aplikacje będzie obsługiwać rozwiązanie AMX?

Odpowiedź: Rozwiązanie AMX obsługuje systemy SSL VPN, aplikacje WWW i klienta Citrix. W przypadku wybrania samodzielnej metody uwierzytelniania za pośrednictwem wiadomości SMS można korzystać z dowolnego oprogramowania agenta RSA (oprócz klienta EAP).

Pytanie: Czy musi to być SSL VPN? Czy jest obsługiwany protokół IPSec?

Odpowiedź: Do korzystania z mechanizmu uwierzytelniania z uwzględnieniem poziomu ryzyka wymagany jest system SSL VPN, ponieważ rozwiązanie AMX bazuje na informacjach zbieranych podczas wymiany standardowych protokołów SSL przeglądarki między klientem a hostem w celu uwierzytelnienia użytkownika. Rozwiązanie AMX będzie obsługiwać sieć VPN z protokołem IP Sec, ale tylko w przypadku korzystania z funkcji uwierzytelniania na żądanie (SMS) jako samodzielnej metody uwierzytelniania oraz agentów uwierzytelniania RSA.

Pytanie: Czy ten produkt działa z dowolnym systemem SSL VPN, aplikacją WWW lub klientem Citrix?

Odpowiedź: Lista rozwiązań zatwierdzonych do integracji znajduje się na stronie RSA Secured Partner. Obecnie znajdują się na niej między innymi rozwiązania SSL VPN firm Juniper, Citrix, Cisco oraz CheckPoint.

Pytanie: Jaki jest maksymalny rozmiar wdrożenia rozwiązania AMX?

Odpowiedź: Rozwiązanie RSA Authentication Manager Express obsługuje maksymalnie 2500 użytkowników (jest to nieprzekraczalna liczba, wynikająca z licencji). Po osiągnięciu tej liczby klient nie będzie mógł przydzielić metody uwierzytelniania (uwzględniającego poziom ryzyka lub za pośrednictwem wiadomości SMS) kolejnym użytkownikom.

Pytanie: Czy rozwiązanie AMX można połączyć ze źródłem danych LDAP, takim jak usługa Microsoft Active Directory? Jeśli tak, to czy w przypadku katalogu LDAP obowiązuje limit 2500 użytkowników?

Odpowiedź: Tak, produkt obsługuje łączność z usługą Microsoft Active Directory w wersji 2003 i 2008 za pomocą macierzystego protokołu LDAP. Wynikający z licencji limit 2500 użytkowników dotyczy tylko liczby użytkowników z przydzieloną metodą uwierzytelniania, a nie łącznej populacji użytkowników usługi Microsoft Active Directory. Katalog LDAP klienta może mieć o wiele więcej niż 2500 użytkowników.

Pytanie: Czy instalacja i konfiguracja rozwiązania AMX są trudne?

Odpowiedź: Rozwiązanie AMX powinno być znacznie łatwiejsze do zainstalowania niż typowe wdrożenie produktu RSA Authentication Manager. Procedura składa się zwykle z następujących etapów: (1) skonfigurowanie urządzenia RSA SecurID Appliance za pomocą narzędzia Quick Setup, (2) wskazanie w rozwiązaniu AMX katalogu użytkowników LDAP, (3) przydzielenie użytkownikom metody uwierzytelniania z uwzględnieniem poziomu ryzyka lub na żądanie (SMS), (4) wskazanie w rozwiązaniu AMX zasobu (systemu SSL VPN, aplikacji WWW lub klienta uproszczonego Citrix), który ma być chroniony. Wszystkie te etapy można wykonać w ciągu kilku godzin.

Pytanie: Czy rozwiązanie AMX obsługuje replikację?

Odpowiedź: Tak, za pomocą dodatkowego urządzenia RSA SecurID Appliance można wdrożyć jedną replikę.



The Security Division of EMC

RSA® Authentication Manager Express Często zadawane pytania

Licencje, ceny, pakiety

Pytanie: Jak jest licencjonowane rozwiązanie RSA Authentication Manager Express?

Odpowiedź: Klient kupuje następujące trzy składniki: (1) urządzenie RSA Authentication Appliance, (2) określona liczba licencji na użytkowników rozwiązania AMX (ceny według przedziałów liczbowych, każda licencja na użytkownika obejmuje połączoną licencję na uwierzytelnianie z uwzględnieniem poziomu ryzyka lub na żądanie przez SMS), (3) całodobowa pomoc techniczna.

Pytanie: Czy cena urządzenia RSA Authentication Appliance obejmuje usługę szybkiej wymiany sprzętu?

Odpowiedź: Tak. Zakupione urządzenie jest objęte 3-letnią usługą szybkiej wymiany sprzętu (ang. advanced hardware replacement — AHR) z opcją zakupu dodatkowych lat (1 lub 2).

Pytanie: Jakie opcje pomocy technicznej są dostępne?

Odpowiedź: Firma RSA oferuje pakiet SecurCare Enhanced, w ramach którego jest dostępna całodobowa pomoc techniczna oraz portal SecurCare zawierający bogate zasoby informacyjne, pliki do pobrania oraz aktualizacje produktów. Zakup tego pakietu nie jest wymagany, jest jednak zdecydowanie zalecany, ponieważ w ramach subskrypcji klienci otrzymują aktualizacje zabezpieczeń i funkcji produktów.

Pytanie: Czy licencję należy przedłużać?

Odpowiedź: Licencja na rozwiązanie AMX jest licencją wieczystą obejmującą połączone funkcje uwierzytelniania z uwzględnieniem poziomu ryzyka i na żądanie (SMS), więc nie ma okresu ważności i klienci nie muszą jej przedłużać.

Mechanizm uwzględniania ryzyka

Pytanie: Dlaczego mechanizm uwzględniania ryzyka jest czynnikiem wyróżniającym?

Odpowiedź: Wiele firm poszukuje nieskomplikowanych rozwiązań do uwierzytelniania. W chwili obecnej jedynym tego typu rozwiązaniem, które jest atrakcyjne z punktu widzenia komercyjnego, jest uwierzytelnianie za pomocą wiadomości SMS. Ta metoda ma jednak swoje ograniczenia: wymaga technologii bramki SMS (usługodawca lub modem), są naliczane opłaty transakcyjne za jej używanie, a dodatkowo poszczególne oferty nie różnią się między sobą, ponieważ wielu klientów decyduje się po prostu na wdrożenie własnego rozwiązania. Natomiast uwierzytelnianie z uwzględnieniem poziomu ryzyka pozwala wyróżnić się na tle konkurencji — klient firmy widzi, że ma do czynienia ze sprawdzonym mechanizmem uwierzytelniania wieloskładnikowego.

Pytanie: Jakie zalety ma ten mechanizm z perspektywy klienta?

Odpowiedź: Z perspektywy klienta uwierzytelnianie z uwzględnieniem poziomu ryzyka jest rozwiązaniem, którego wdrożenie przebiega szybko i łatwo, bez zakłócania pracy firmy. Nie ma potrzeby zmieniania istniejących zasad dotyczących haseł, ponieważ nasz mechanizm uwierzytelnia użytkownika w sposób niewidoczny, wyłącznie na podstawie urządzenia i cech behawioralnych. Nie są także wymagane żadne dodatkowe działania administracyjne względem użytkownika końcowego.



The Security Division of EMC

RSA® Authentication Manager Express Często zadawane pytania

Pytanie: Czy istnieją konkurencyjne mechanizmy uwierzytelniania z uwzględnieniem poziomu ryzyka? Czym się różnią?

Odpowiedź: Istnieje kilka konkurencyjnych rozwiązań tego typu, jednak ustępują one naszemu mechanizmowi w wielu obszarach. Po pierwsze najczęściej umożliwiają uwierzytelnianie wyłącznie na podstawie urządzenia, czyli po prostu umieszczają standardowy plik cookie na komputerze użytkownika. Ten plik jest używany podczas kolejnych operacji uwierzytelniania. Mechanizm firmy RSA także obejmuje uwierzytelnianie na podstawie urządzenia, ale używa do tego celu obiektu flash, który jest znacznie trudniejszy do wykrycia. Trudniejsze jest także jego przypadkowe usunięcie. Oprócz tego dodaliśmy zaawansowaną funkcję rozpoznawania cech behawioralnych, która pozwala zidentyfikować użytkownika na podstawie wzorców zachowań. Analiza behawioralna polega na ocenianiu wzorców zachowań użytkowników, przypadków uwierzytelniania i uzyskiwania dostępu do konta oraz innych czynników składających się na ocenę poziomu ryzyka podczas każdej próby uwierzytelnienia.

Ryzyko behawioralne oblicza się przez porównanie bieżącego żądania uwierzytelnienia z historią uwierzytelniania danego użytkownika, znanymi zachowaniami innych użytkowników populacji oraz sygnaturami behawioralnymi typowymi dla prób uzyskania nieuprawnionego dostępu. Kiedy ryzyko jest niskie, zachowania użytkownika stanowią kolejny czynnik uwierzytelniający, który potwierdza tożsamość posiadacza konta w sposób niezauważalny dla tej osoby.

Pytanie: Co się stanie, gdy uwierzytelnianie z uwzględnieniem poziomu ryzyka nie zakończy się wynikiem pozytywnym?

Odpowiedź: Nastąpi kolejna próba weryfikacji tożsamości użytkownika polegająca na uzyskaniu odpowiedzi na pewne pytania i porównaniu ich z odpowiedziami uzyskanymi podczas rejestracji. Może to być też prośba o wprowadzenie w polu logowania kodu tokenu przesłanego za pomocą wiadomości SMS lub e-mail.

Migracja i plany na przyszłość

Pytanie: Jakie plany ma firma RSA względem tej platformy?

Odpowiedź: Z perspektywy firmy RSA rozwiązanie AMX jest inicjatywą strategiczną, której zadaniem jest zdobycie udziału w szybko rozwijającym się segmencie firm mających do 2500 użytkowników. Warto wspomnieć, że od dawna brakowało rozwiązań zabezpieczających w tym segmencie. W planach firmy RSA jest już wersja AMX 1.1 dodająca wiele ulepszeń do istniejącej platformy.

Pytanie: Czy klientom kupującym rozwiązanie AMX można obiecać przyszłą możliwość migracji do produktu RSA Authentication Manager?

Odpowiedź: Nie, rozwiązanie AMX powinno być sprzedawane klientom wymagającym właśnie takich funkcji. Dodanie tokenów sprzętowych i programowych lub zwiększenie limitu użytkowników ponad 2500 są brane pod uwagę w planach rozwoju produktu, ale nie należy się spodziewać tych funkcji przed rokiem 2013.