RSA® Adaptive Authentication

Alors que de plus en plus d'entreprises souhaitent faire évoluer leurs clients, adhérents ou partenaires vers des systèmes en ligne plus économiques, le niveau de confiance et l'implémentation de mesures renforcées de sécurité revêtent aujourd'hui une importance critique. La multiplication et l'évolution constante des menaces (phishing, intermédiation de type « man-in-the-middle » , chevaux de Troie, etc.) soulèvent en effet de nombreuses problématiques – notamment pour déployer une solution de protection pérenne et adaptable aux constants changements.

Il s'agit en synthèse de trouver un délicat équilibre entre les impératifs d'authentification, les exigences "d'expérience utilisateur" et les contraintes budgétaires. L'authentification forte dispose aujourd'hui de solides arguments pour sécuriser les données sensibles et maximiser le niveau d'utilisation des systèmes en ligne. En outre, la plupart des utilisateurs ayant eu l'occasion de juger des qualités de cet environnement (par exemple, avec leur banque en ligne), ils attendent aujourd'hui une protection similaire lorsqu'ils manipulent des données sensibles de n'importe quel autre site.

RSA®
The Security Division of EMC

Le choix ultime pour l'authentification

RSA® Adaptive Authentication est une plate-forme complète d'authentification multicanal et de gestion du risque offrant une protection financièrement rentable pour toute la base d'utilisateurs. RSA Adaptive Authentication supervise et authentifie les activités utilisateurs en fonction du niveau de risque encouru, des politiques institutionnelles et de la segmentation des clients. Cette solution peut être déployée avec la plupart des méthodes d'authentification existantes :

- Authentification invisible par identification et profilage de l'appareil utilisé
- Authentification « hors bande » par émission d'appel téléphonique, SMS ou e-mail
- Réponses à des questions personnelles ou par rapport à une base de connaissances
- Framework multi-habilitation. Pour les entreprises désirant plus de choix, Adaptive Authentication est conçu pour intégrer facilement avec une large sélection d'autres méthodes d'authentification. Le framework multi-habilitation permet de développer des méthodes spécifiques d'authentification (avec le support des services professionnels de RSA, en interne ou via des prestataires tiers) afin de librement personnaliser Adaptive Authentication.
- Authentification site vers utilisateur. Cette méthode garantit aux utilisateurs qu'ils réalisent des transactions avec un site Web légitime (ce dernier affichant par exemple une image de sécurité personnelle et une légende présélectionnées par l'utilisateur lors de sa connexion initiale).

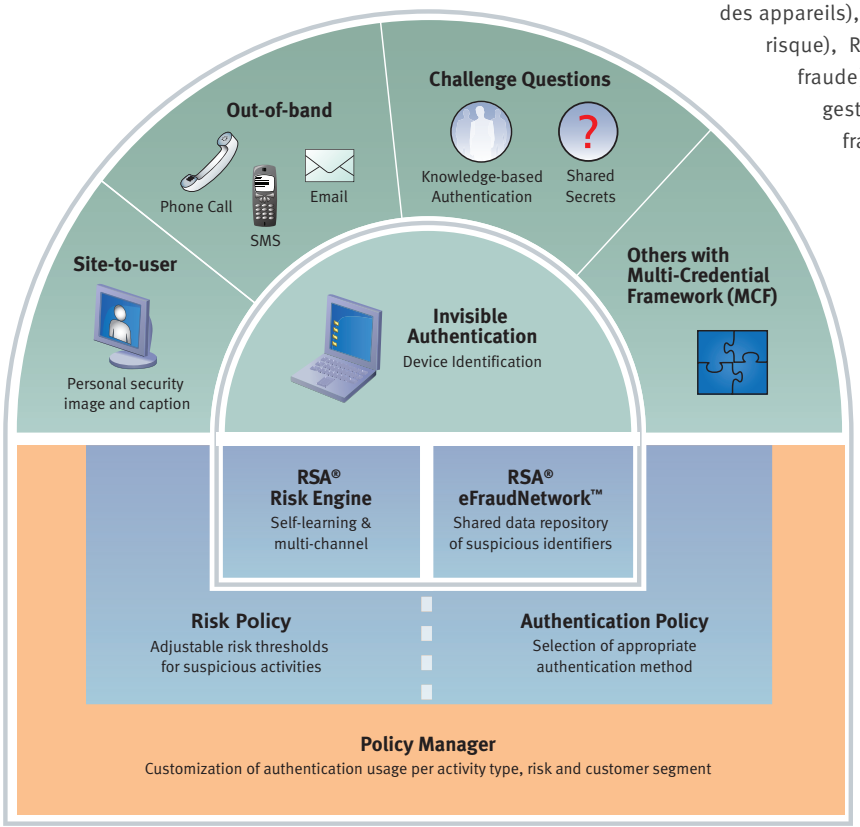
Grace à un support intelligent des différentes technologies d'authentification existantes, RSA Adaptive Authentification apporte aux entreprises une flexibilité incomparable pour:

- Choisir avec quelle force authentifier les utilisateurs finaux
- Définir comment distinguer les utilisateurs habituels des nouveaux venus
- Sélectionner les domaines de leur activité à protéger avec une authentification forte
- Adapter les moyens pour se conformer aux évolutions légales et réglementaires
- Formaliser quels niveaux de risques sont-elles prêtes à accepter
- Se conformer aux exigences spécifiques des régions et pays où elles exercent

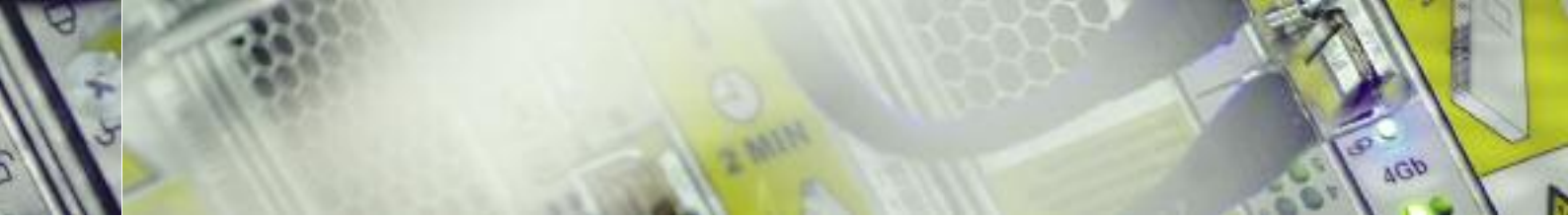
Les dynamiques de l'authentification basée sur le risque

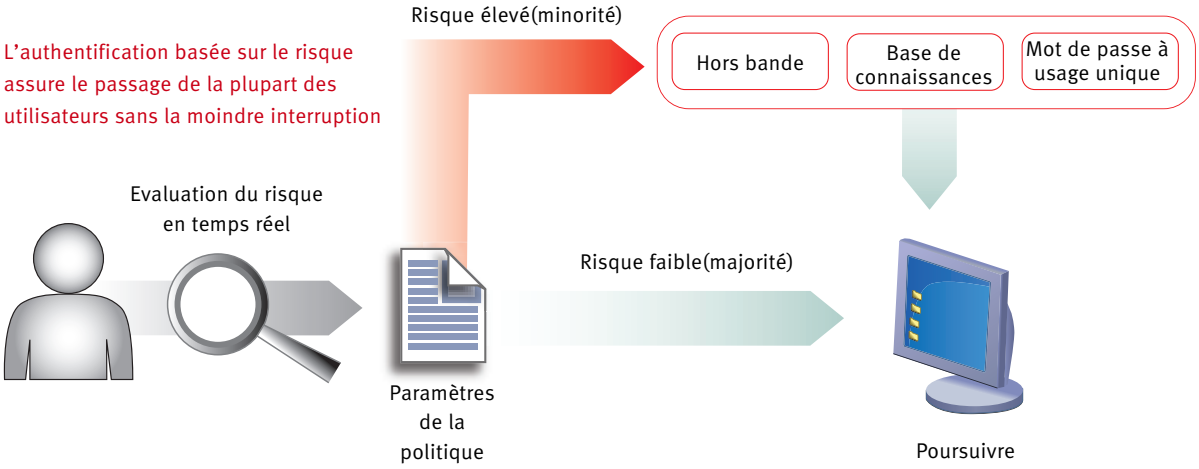
La plate-forme RSA Adaptive Authentication s'appuie sur une technologie exclusive d'authentification basée sur le risque – un système sophistiqué mesurant en tâche de fond une série d'indicateurs de risque pour certifier l'identité des utilisateurs. Cette approche transparente de l'authentification offre des gages incomparables d'expérience utilisateur dans la mesure où ces derniers ne sont réellement questionnés qu'en cas de scénario à haut risque ou de dérogation aux politiques institutionnelles. L'authentification basée sur le risque s'appuie par ailleurs sur l'auto-apprentissage pour protéger les utilisateurs contre les chevaux de Troie, les attaques d'intermédiation, et d'autres formes d'attaques de logiciels malveillants.

La solution d'authentification basée sur le risque développée par RSA exploite une serie de technologies fondamentales: RSA Device Identification(identification des appareils), RSA® Risk Engine(un moteur de risque), RSA eFraudNetwork™ (un réseau anti-fraude), RSA® Policy Manager (un gestionnaire de politiques) et le framework multi-habilitation de RSA.



RSA Adaptive Authentication offre un support transparent des diverses technologies d'authentification existantes.





RSA Device Identification Cette technologie assure l'authentification transparente de la grande majorité des utilisateurs en analysant le profile du périphérique (système employé pour accéder au serveur/réseau) et le profil comportemental (quelles sont les activités typiquement menées), puis comparant l'activité en cours avec ces profils habituels.

RSA® Risk Engine Cette technologie éprouvée, dotée de l'auto-apprentissage évalue en temps réel chaque activité en ligne à travers plus d'une centaine d'indicateurs pour détecter automatiquement toute activité frauduleuse. La probabilité pour que l'activité en cours soit effectivement frauduleuse est mesurée par un indice de risque unique compris entre 0 et 1000, généré pour cette activité.

RSA® Policy Manager Le gestionnaire de politiques réagit instantanément aux schémas de fraude émergeants et investigue plus particulièrement les activités marquées à haut risque. Il convertit la politique de risque organisationnel en décisions et actions à travers une trame de règles configurable en temps réel.

RSA eFraudNetwork Cette base de données inter-entreprises centralise les schémas de fraude recensés par le large réseau de clients RSA, de fournisseurs de services Internet et de contributeurs tiers dans le monde entier. Dès qu'un mode opératoire de fraude est identifié, ses données, profils transactionnels et empreintes système sont enregistrés dans un référentiel partagé. RSA eFraudNetwork alimente directement le moteur RSA Risk Engine de sorte que toute tentative de transaction émanant d'un appareil ou d'une adresse IP répertorié dans eFraudNetwork sera immédiatement jugée à haut risque et exigera une authentification additionnelle.

RSA Multi-credential Framework Le framework multi-habilitation constitue une couche d'abstraction permettant à une seule plate-forme logicielle de supporter plusieurs méthodes d'authentification (en fonction de la segmentation utilisateur et de l'évaluation du risque) dans le même déploiement. Les différentes méthodes d'authentification sont exploitées à travers les paramètres de la politique pour s'adapter aux différents produits en ligne, populations d'utilisateurs et niveaux de risque.

Une souplesse incomparable de déploiement et de configuration

RSA RSA reconnait qu'il n'existe pas deux business ayant exactement les mêmes besoins d'authentification utilisateurs. Ce qui explique la large gamme d'options d'authentification, de déploiement et de personnalisation, afin de répondre aux spécificités propres à chaque entreprise et à ses utilisateurs finaux.

Déploiement visible ou invisible

En fonction des besoins organisationnels ou des exigences de commodité des utilisateurs, RSA Adaptive Authentication peut être déployé de façon visible ou invisible. Certaines organisations préfèrent une authentification visible pour montrer visuellement à leurs utilisateurs qu'ils sont protégés, pour se conformer aux réglementations, ou tout simplement pour renforcer un sentiment de sécurité.

D'autres entreprises privilégient une authentification invisible pour surveiller l'activité en ligne, avec objectif de ne pas perturber l'expérience utilisateur, ne pas alerter les

fraudeurs potentiels de la mise en place d'un système anti-fraude ou bien pour déployer une couche supplémentaire de protection contre les menaces avancées.

Déploiement sur site ou hébergé (ASP)

RSA Adaptive Authentication peut être déployé sur site dans les infrastructures informatiques existantes ou être externalisé dans le cadre d'un service d'authentification hébergé par un prestataire tiers.

Multiples options de configuration

RSA Adaptive Authentication propose de multiples paramètres de configuration pour trouver un équilibre optimal entre la sécurité et les risques – sans compromis sur l'expérience utilisateur. Ainsi, de nombreux clients choisissent de déployer l'authentification basée sur le risque pour l'ensemble de leur base utilisateurs et de laisser au moteur RSA Risk Engine la responsabilité de déterminer ceux qui exigent une protection supplémentaire... D'autres choisissent de compléter l'environnement avec des clés spécifiques d'authentification (matérielles ou logicielles) fournies à tous ceux qui conduisent régulièrement des transactions à haut risque. La plupart de ces clés peuvent être siglées au nom de l'entreprise pour renforcer son image de marque de sécurité et démontrer son attachement à la protection des opérations en ligne de ses utilisateurs.

Une solution éprouvée

La plate-forme RSA Adaptive Authentication est actuellement utilisée par plus de 8 000 entreprises dans le monde et dans de multiples secteurs : services financiers, santé, administrations, etc. Elle protège plus de 200 millions d'utilisateurs en ligne et a sécurisé à ce jour le traitement de plus de 20 milliards de transactions !

À propos de RSA

RSA, la Division Sécurité d'EMC, est le premier fournisseur de solutions de sécurité pour l'accélération métier et le partenaire privilégié des plus grandes entreprises mondiales pour résoudre leurs challenges de sécurité les plus pressants, complexes et sensibles. L'approche de la sécurité centrée sur l'information prônée par RSA garantit son intégrité et sa confidentialité tout au long du cycle de vie – quels que soient ses cheminements, ses consommateurs ou ses modalités d'utilisation.

RSA propose des solutions leaders de certification des identités et de contrôle d'accès ; de prévention des pertes de données ; de cryptage et de gestion des clés ; de gestion de la conformité et des informations de sécurité et de protection contre la fraude. Cette large gamme de solutions certifie l'identité de millions d'utilisateurs dans le monde et des données qu'ils génèrent lors de leurs transactions quotidiennes. Pour plus d'informations, veuillez consulter www.RSA.com et www.EMC.com.

RSA®
The Security Division of EMC

RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

FR AA DS 0209