



# Adaptive Authentication for the Enterprise

As the usage of online portals, SSL VPN applications, and web access management (WAM) products continue to grow, so does the need for strong authentication to protect against unauthorized access to the information contained within them.

Providing single-factor authentication, or password-only protection, creates a significant security threat to organizations. Single-factor authentication is easily defeated by hackers and can result in a security breach, financial loss, or loss of sensitive data such as personally identifiable information (PII). Concurrently, many IT departments are grappling with business requirements to extend access to enterprise applications to an even broader audience – including vendors, suppliers, partners and customers.

Whether driven by compliance or the need to effectively manage information risk, organizations are faced with the challenge of providing strong multi-factor authentication to secure their assets and information while balancing cost and end user convenience.

---

## The Right Choice for Authentication

---

A recent survey by RSA shows that on average, only 20-40% of the typical enterprise workforce is issued hardware or software tokens. The main reason for low deployment rates is often attributed to the acquisition cost and ongoing management of rolling out physical authenticators to every single user. As a result, organizations are considering new methods of authentication that will enable them to extend strong authentication to a broader user base and provide an additional layer of security without impacting the user experience. RSA® Adaptive Authentication is becoming a likely choice for authentication among organizations in multiple industries for protecting access to portals, VPNs and other enterprise applications.

RSA® Adaptive Authentication is a comprehensive authentication and fraud detection platform providing cost-effective protection for an entire user base. Adaptive Authentication is powered by Risk-Based Authentication (RBA), a risk assessment and authentication technology that operates transparently and classifies all users by measuring a series of risk indicators. This transparent authentication for the majority of users provides for a convenient online experience as users are only challenged when suspicious activities are identified and/or an organizational policy is violated.



The Security Division of EMC

A variety of authentication methods exist that can be used on top of the Adaptive Authentication platform including:

- Invisible authentication. Device identification and profiling
- Out-of-band authentication. Phone call, SMS, or e-mail
- Challenge questions. Challenge questions or knowledge-based authentication (KBA)
- Multi-Credential Framework. For organizations wanting more choices, Adaptive Authentication is designed to easily integrate with a large selection of other authentication methods. The Multi-Credential Framework allows organizations to develop authentication methods via RSA Professional Services, “in-house” or through third parties to customize Adaptive Authentication.
- Site-to-user authentication. Site-to-user authentication assures users they are transacting with a legitimate website by displaying a personal security image and caption that has been pre-selected by the user at login.

By having the ability to support most existing authentication technologies, organizations that use Adaptive Authentication can be flexible in:

- How strongly they authenticate end users
- How they distinguish between new and existing end users

- What areas of the business to protect with strong authentication
- How to comply with changing regulations
- What they are willing to accept in terms of risk levels
- How to comply with the various requirements of the regions and countries where they operate

---

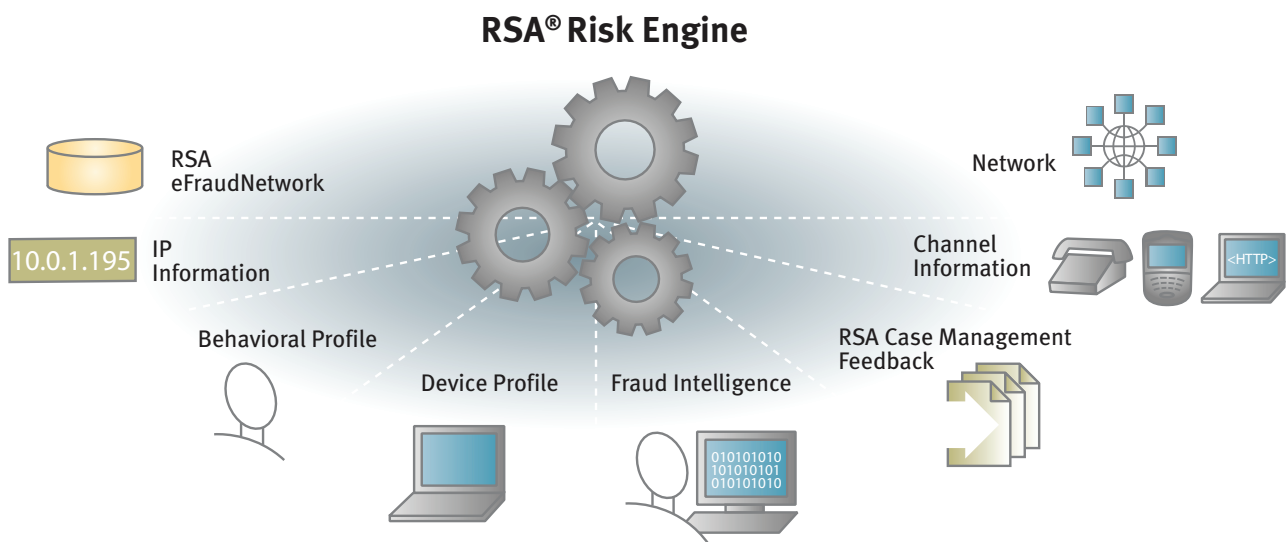
## The Dynamics of Risk-based Authentication

---

RSA’s Risk-Based Authentication is powered by a series of core technologies – device profiling, behavioral profiling, the RSA® Risk Engine, the RSA® eFraudNetwork™, the RSA® Policy Manager, and the RSA® Multi-credential Framework.

### Device Profiling

Profiling enables Adaptive Authentication to assure the identities of the vast majority of users transparently by comparing the profile of a given activity with their typical profile patterns. Device profiling analyzes the device profile (the physical laptop/PC from which the user accesses the website or application) and determines if the device is known as having been previously used by this user. The two main components of device profiling are unique device identification and statistical device identification.



The RSA Risk Engine measures a number of factors in generating a risk score.



Unique device identification distinguishes a device through the use of two main elements embedded on the user's laptop/PC – secure first party cookies and flash shared objects (sometimes referred to as “Flash cookies”). Statistical device identification is a technology that analyzes the characteristics of a device to statistically identify a user's device.

#### **Behavioral Profiling**

Risk-Based Authentication also uses behavioral analysis to identify high-risk authentication attempts. Some parameters that are measured include velocity checking, IP address information, and time of day comparisons. Behavioral profiling analysis complements device profiling with user behavior to offer a form of multi-factor authentication that includes something you have (the device) and something you do (behavior).

#### **RSA® Risk Engine**

The RSA Risk Engine is a proven, self-learning technology that evaluates each online activity in real-time, tracking over one hundred indicators in order to detect fraudulent activity. A unique risk score, between 0 – 1000, is generated for each activity. The higher the risk score, the greater the likelihood is that an activity is fraudulent.

#### **RSA® Policy Manager**

The RSA Policy Manager enables organizations to instantly react to emerging localized fraud patterns and effectively investigate activities flagged as high-risk. The Policy Manager translates organizational risk policy into decisions and actions through the use of a web-based Rules Management application, comprehensive rules framework, real-time configuration, and Performance Simulator for testing prior to being put into production.

#### **RSA® eFraudNetwork™**

The RSA eFraudNetwork is a cross-organization, cross-industry data repository of fraud patterns gleaned from RSA's worldwide network of customers, end users, ISPs, and third party contributors. The eFraudNetwork community is dedicated to sharing and disseminating information on fraudulent activity to help keep its members one step ahead of fraudsters. When a fraud pattern is identified, the fraud data, activity profile, and device fingerprints are moved to a shared data repository. The eFraudNetwork enables real-time proactive protection to hundreds of millions of online

users worldwide that are actively connected to the network and is one of the many sources that feeds the Risk Engine in determining risk.

#### **RSA® Multi-credential Framework (MCF)**

The RSA Multi-credential Framework (MCF) provides an abstraction layer that enables one software platform to support multiple authentication methods (based on end user segment and risk assessment) in a single deployment. With the Multi-credential Framework, different authentication methods are leveraged through policy settings to accommodate different end user populations, different online products, and different risk levels.

---

### **On-Premise or SaaS / Hosted Deployment Options**

---

Organizations worldwide currently deploy Adaptive Authentication in two ways – as an on-premise installation that uses existing IT infrastructure or as a hosted authentication service that helps to manage the end user lifecycle. Recognizing that no two organizations share the exact same user authentication needs, RSA offers the widest possible range of authentication, deployment, and customization options.

RSA has one of the world's largest security Software-as-a-Service (SaaS) practices, with more than 3,700 organizations relying on RSA Hosted Operations for a variety of our products that offer this delivery model. RSA Hosted Operations has been providing SaaS products for more than seven years in the areas of card authentication, web authentication, and identity verification.

---

### **Multiple Configuration Options**

---

Adaptive Authentication can be configured in a number of ways to balance security and risk without compromising the user experience. Many organizations currently provide risk-based authentication for their entire user base and allow the RSA Risk Engine to determine those individuals that require additional protection. Other organizations choose an appropriate supplemental form factor based on a user's preference or the types of activities they conduct.



---

## A Proven Solution

---

RSA Adaptive Authentication is a proven solution that is currently deployed at over 8,000 organizations worldwide and across multiple industries including healthcare, financial services, government, insurance, automotive, real estate, manufacturing, and pharmaceuticals. It is currently being used to protect over 200 million online users and has processed and protected over 20 billion transactions to date.

## About RSA

RSA, The Security Division of EMC, is the expert in information-centric security, enabling the protection of information throughout its lifecycle. RSA enables customers to cost-effectively secure critical information assets and online identities wherever they live and at every step of the way, and manage security information and events to ease the burden of compliance. RSA offers industry-leading solutions in identity assurance and access control, encryption and key management, compliance and security information management and fraud protection. These solutions bring trust to millions of user identities, the transactions that they perform and the data that is generated. For more information, please visit [www.RSA.com](http://www.RSA.com) and [www.EMC.com](http://www.EMC.com).

RSA and the RSA logo are registered trademarks or trademarks of RSA Security Inc. in the U.S. and/or other countries. EMC is a trademark of EMC Corporation. All other trademarks mentioned herein are the property of their respective owners. ©2009 RSA Security Inc. All rights reserved.

AAVPN DS 0409



The Security Division of EMC

RSA Security Inc.  
RSA Security Ireland Limited  
[www.rsa.com](http://www.rsa.com)