RSA® ADAPTIVE AUTHENTICATION
A Comprehensive Authentication Platform for Web-Based, Remote Access Entry Points

AT A GLANCE
- Measures risk of login by evaluating over 100 indicators in real-time
- Determines authentication requirements based on risk and policy
- Supports wide range of authentication options
- Provides certified integration to industry-leading enterprise applications
- On-premise installation & hosted service options available

As the usage of online portals, Sockets Layer (SSL) Virtual Private Network (VPN) applications, Web Access Management (WAM) applications, mobile applications and online portals continue to grow within the enterprise, so does the need for strong authentication to protect against unauthorized access to information contained within these. Concurrently, organizations are faced with the need to extend access to a more diverse user base 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 authentication to secure their assets and information while balancing costs and end user convenience. RSA Adaptive Authentication addresses this challenge by providing cost effective protection for an entire user base in the form of risk-based, multifactor authentication.

ADAPTIVE AUTHENTICATION OVERVIEW
Adaptive Authentication is a comprehensive authentication and fraud detection platform. Powered by RSA’s Risk-Based Authentication technology, Adaptive Authentication is designed to measure the risk associated with a user’s login by evaluating a variety of risk indicators. Using a risk and rules based approach, the system then requires additional identity assurance, such as out-of-band authentication, for scenarios that are high risk and violate a policy. This methodology provides transparent authentication for the majority of the users.

TECHNOLOGY & COMPONENTS
Adaptive Authentication leverages a series of technologies and components to provide cross-channel protection, including the RSA Risk Engine, RSA Policy Management, Device & Behavior Profiling, RSA eFraudNetwork™, "Step-up" Authentication, and RSA Case Management.

Figure 1: RSA Adaptive Authentication Technology & Components
RSA Risk Engine
The RSA Risk Engine is a self-learning statistical machine learning technology that utilizes over 100 indicators to evaluate the risk of an activity in real-time. Adaptive Authentication leverages the Risk Engine to generate a unique score for each activity that ranges from 0 to 1,000, where 1,000 indicates the greatest level of risk. The score is reflective of device profiling, behavioral profiling, and eFraudNetwork data. The Risk Engine combines rich data input, machine learning methods and authentication feedback to provide intelligent, real-time risk evaluations to mitigate fraud. Unlike most solutions, RSA takes both a risk and rules based approach. Customers can utilize the Policy Management application to set policy rules and that can be layered on top of the Risk Engine to create a hybrid approach.

RSA Policy Manager
The RSA Policy Management application translates risk policies into decisions and actions through the use of a comprehensive rules framework. For example, the Policy Management application can be used to set the risk score that will require later review in the Case Management application, prompt additional assurance or "Step-up" Authentication, and/or deny access in which the likelihood of fraud is very high. In addition, the Policy Management application can create rules independently of the risk assessment, such as blocking authentication from a specific IP address.

Device Profiling
Device profiling analyzes the device from which the user is accessing an organization’s website or mobile application. Adaptive Authentication determines whether a device used for a given activity is a device that is typically used by the user, or if the device has been connected to previous fraudulent activities. Parameters analyzed include characteristics such as operating system version, browser type and version, and cookies and/or flash objects.

Behavior Profiling
Behavior profiling is a record of the typical activity for the user. Adaptive Authentication compares the profile for the activity with the user's usual behavior to assess risk. The user profile is used to determine if the various activities are typical for that user, or if the behavior is indicative of known fraudulent patterns. Parameters examined include frequency, time of day and type of attempted activity.

RSA eFraudNetwork™
The RSA eFraudNetwork is a cross-functional repository of fraud patterns gleaned from RSA’s extensive network of customers, internal research lab, ISPs, and third party contributors across the globe. When fraudulent elements such as IP Address and Device Fingerprint are identified, they are shared with the eFraudNetwork. The eFraudNetwork provides direct feeds to the Risk Engine so when an activity is attempted from a device or IP that appears in the repository, it will be deemed high-risk.

Case Management
A highly effective fraud management tool that enables the tracking of activities that trigger Policy Engine rules and determines if flagged activities are genuine or
Adaptive Authentication can be directly embedded in mobile devices through the Software Development Kit (SDK) fraudulent. Organizations use this information to take appropriate measures in a timely manner and minimize the damage caused by fraudulent activities. Further, this tool also enables an organization to provide feedback into the risk engine upon case resolution.

**Step-up Authentication**

A Step-up Authentication is an additional factor or procedure that validates a user’s identity, usually prompted by high risk transactions or according to policy rules. The following are examples of out-of-the-box step-up authentication methods supported in Adaptive Authentication:

- **Challenge Questions**: Secret questions that have been selected & answered by end user during enrollment
- **Out-of-Band Authentication**: Onetime passcode sent to the end user via phone call, SMS text message or email. Transaction details can be included in the communication to help prevent fraudulent activities.
- **Other third party authentication methods via the RSA Multi Credential Framework.**

**CROSS CHANNEL PROTECTION: WEB & MOBILE**

**Mobile Protection**

The proliferation of mobile devices brings opportunity as well as risk; however, mobile applications that directly integrate Adaptive Authentication protect against unauthorized access with minimal impact to the end user. Adaptive Authentication offers a dedicated mobile risk model that includes capabilities such as location awareness and mobile device identification. Location awareness detects the location of the device using a series of time and geography based algorithms and can access location data gathered through Wi-Fi, cell-tower triangulation, and GPS. Device identification captures characteristics such as device model, language, and screen size. Anomalies such as locations or devices which are new to the user, are deemed high risk.

Adaptive Authentication offers integration through a web services call, or a Software Development Kit (SDK) that allows developers to build controls directly into their mobile applications. Supported platforms include Apple iOS, Android OS and Blackberry OS. Developers of mobile applications for business and data access can now help increase security and confidence by integrating strong risk-based authentication in their mobile offerings.

**ADVANCED THREAT PROTECTION**

Organizations are constantly battling new forms of threats. Adaptive Authentication is designed to address Man in the Browser (MITB) and Man in the Middle (MITM) techniques employed by the latest Trojan attacks that aim to comprise end user accounts by detecting the use of proxies, automated scripts, and HTML injections. With Adaptive Authentication, anomalies are flagged so that an organization can take action to block, monitor or require additional authentication measures to complete an activity.
FLEXIBLE DEPLOYMENT & CONFIGURATION OPTIONS

RSA recognizes that no two organizations share the exact same user authentication needs, and as a result, Adaptive Authentication offers a wide array of deployment and configuration options to meet the varied needs of organizations. For instance, organizations worldwide currently deploy Adaptive Authentication in two ways – as an on-premise installation that uses existing IT infrastructure or as a hosted Software-as-a-Service (SaaS). Further, 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 use the Policy Management application to determine action to take based on risk. This flexibility enables Adaptive Authentication be used to protect a variety of remote access points such as web portals, mobile applications, and SSL VPNs.

Certified Adapters for Enterprise Application Protection

RSA has developed several Adaptive Authentication Adapters to eliminate custom integration into web-based enterprise applications and application delivery solutions thereby shortening and simplifying deployments. The Adaptive Authentication Adapter can be deployed as is or it can be branded and further customized using the configuration wizard. For example, a company logo or different look-and-feel can be added to the authentication pages for unique branding. Adaptive Authentication Adapters include Juniper IVE, Cisco ASA, CheckPoint Connectra, Microsoft UAG, RSA Access Manager, CA SiteMinder®, IBM Trivoli, Citrix XenApp, and Citrix NetScaler.

A PROVEN SOLUTION

Adaptive Authentication is a comprehensive, risk-based authentication platform that balances security, usability, and cost. Further, Adaptive Authentication helps to increases user confidence and willingness to transact with online portals and mobile devices. Adaptive Authentication is a proven solution that is currently deployed at over 8,000 organizations worldwide and across multiple industries including financial services, healthcare, and government. It is currently being used to protect over 200 million users and has processed and protected over 20 billion transactions.

CONTACT US

To learn more about how EMC products, services, and solutions can help solve your business and IT challenges, contact your local representative or authorized reseller—or visit us at www.EMC.com/rsa.

www.EMC.com/rsa