RSA® Adaptive Authentication

Advanced fraud detection for web and mobile

In order to meet end user demand for convenience, organizations continue to extend product and service offerings and account access into online and mobile channels. At the same time, fraud continues to proliferate with cybercriminals leveraging phishing, man-in-the-middle, man-in-the-browser, and other advanced attacks to gain unauthorized access to personal and corporate accounts.

Achieving the right balance of security – while maintaining a positive user experience – is a challenge for organizations. RSA Adaptive Authentication solves this challenge by providing risk-based, multifactor authentication for organizations seeking to protect access to websites and online portals, mobile applications and browsers, Secure Sockets Layer (SSL) virtual private network (VPN) applications, web access management (WAM) applications and application delivery solutions.

Adaptive Authentication is deployed at more than 8,000 organizations worldwide, protecting more than 500 million end users spanning multiple industries including financial services, healthcare, retail, and government.

Adaptive Authentication authenticates over 95% of users transparently, ensuring a positive user experience.

Adaptive Authentication overview

Adaptive Authentication is an advanced authentication and fraud detection platform for Web and mobile channels. Powered by RSA's risk-based authentication technology, Adaptive Authentication is designed to measure the risk associated with a user's login and post-login activities 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/or violate rules established by an organization. This methodology provides transparent authentication for the majority of the users, ensuring a positive user experience.

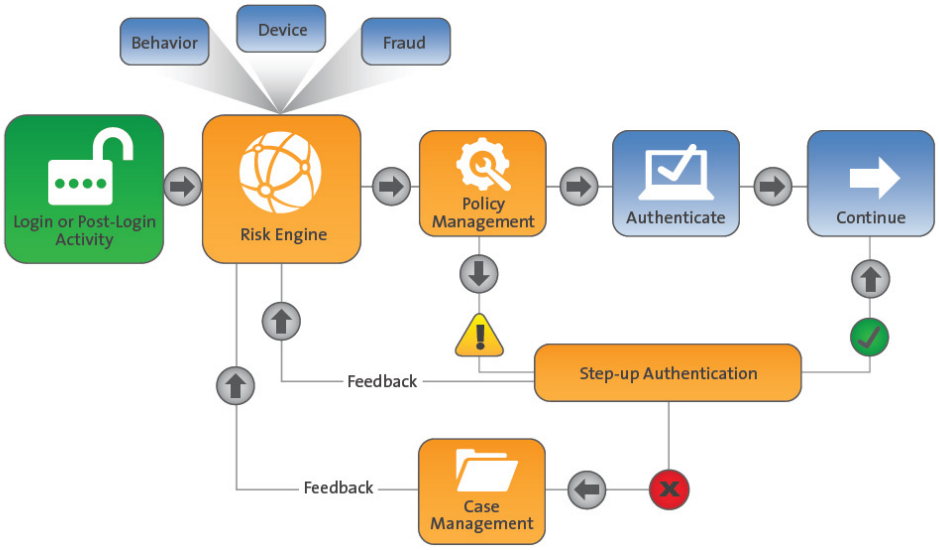
Adaptive Authentication leverages a series of technologies to provide crosschannel protection, including the RSA Risk Engine, RSA Policy Management, device and behavior profiling, RSA eFraudNetwork, RSA Case Management and step-up authentication.

RSA Risk Engine

The RSA Risk Engine is a self-learning statistical machine learning technology that utilizes over one hundred 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.

An overview of the technologies that drive Adaptive Authentication

The Risk Engine combines rich data input, machine learning methods and authentication feedback to provide intelligent 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 that can be layered on top of the Risk Engine to create a hybrid approach.



RSA Policy Management

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, initiate step-up authentication, and/or deny transactions 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 transactions 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 compares the profile of a given activity with the typical profile patterns to determine risk.

The device profile is used to determine whether the current device is one from which the user typically requests access from or if the device has been connected to previous known fraud. Parameters analyzed include IP address & geo-location, operating system version, browser type and other device settings.

Behavior profiling

Behavior profiling is a record of typical activity for the user. Adaptive Authentication compares the profile for the activity with the usual behavior to assess risk. The user profile determines 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 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 a fraud pattern is identified, the fraud data, transaction profile, device fingerprints and payee (mule) account are moved to a shared repository. 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, the risk score will be raised. Nearly 1 in 7 fraud transactions are identified by the eFraudNetwork at the time of the transaction.

Nearly 1 in 7 fraud transactions are identified by the RSA eFraudNetwork at the time of the transaction.

RSA Case Management

RSA Case Management enables organizations to track activities that trigger Policy Engine rules and determines if flagged activities are genuine or fraudulent. Organizations use this information to take appropriate measures in a timely manner and minimize the damage caused by fraudulent activities. The Case Management application is also used to research cases and analyze fraud patterns, which are essential when revising or developing new policy decision rules. Further, this tool also enables an organization to provide feedback into the Risk Engine upon case resolution.

The Case Management API is an extension of Adaptive Authentication Case Management capabilities which allows incidents to be shared with existing external case management systems for even greater flexibility.

Step-up authentication

Step-up authentication is when an additional authentication factor is used to further validate a user's identity in high-risk scenarios. Some out-of-the-box step-up authentication methods supported in Adaptive Authentication include:

- **Challenge questions:** Secret questions that have been selected and answered by an end user during enrollment.
- **Out-of-band authentication:** One-time 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.
- **Biometrics:** Fingerprint and eyeprint biometrics (available for mobile users).
- **Transaction signing:** Provides integrity assurance, cryptographic signature and authenticity for payment transactions to combat fraud from advanced financial malware attacks. Transaction signing can optionally integrate with biometrics as a stronger means of authentication layered on top of the payment transaction signature.

Protection for mobile users

The proliferation of mobile devices brings opportunity as well as risk. In 2015, 45% of fraudulent transactions identified by Adaptive Authentication originated from a mobile device. Through direct integration with Adaptive Authentication, organizations can extend fraud protection to users accessing via a mobile application or mobile browser.

Adaptive Authentication supports biometrics step-up authentication for mobile users.

Adaptive Authentication offers a dedicated mobile risk model that includes capabilities such as location awareness and 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 location 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 and Android OS.

Flexibile deployment and configuration

Adaptive Authentication offers a wide array of deployment and configuration options to meet the need of almost any organization. Adaptive Authentication can be deployed in two ways – as an on-premise installation that uses existing IT infrastructure or as a hosted Software-as-a-Service (SaaS).

Adaptive Authentication can be configured in a number of ways to balance security and risk. Many organizations currently provide risk-based authentication for their entire user base and allow the RSA Risk Engine to choose an appropriate step-up authentication method based on the risk score or access level of the user.

About RSA

RSA provides more than 30,000 customers around the world with the essential security capabilities to protect their most valuable assets from cyber threats. With RSA's award-winning products, organizations effectively detect, investigate, and respond to advanced attacks; confirm and manage identities; and ultimately, reduce IP theft, fraud, and cybercrime. For more information, visit **www.rsa.com**.