RSA

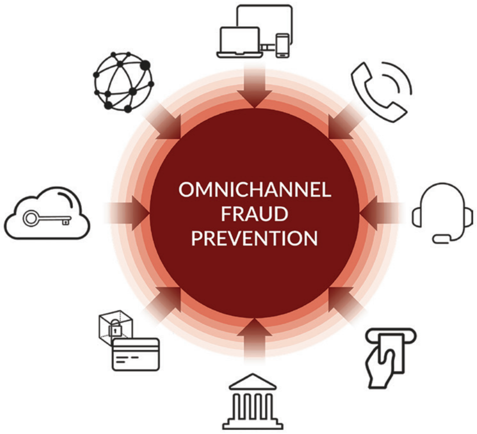
DATA SHEET

RSA Adaptive Authentication

Mitigate fraud across consumer facing digital channels

RSA Adaptive Authentication overview

The global pandemic has accelerated organizations digital transformation, especially when it comes to consumer facing digital channels. Lock down and "stay home" instructions around the globe forced organizations and consumers to interact through digital channels like never before. 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 consumer accounts. Achieving the right balance of security while maintaining a positive user experience is a challenge for organizations.

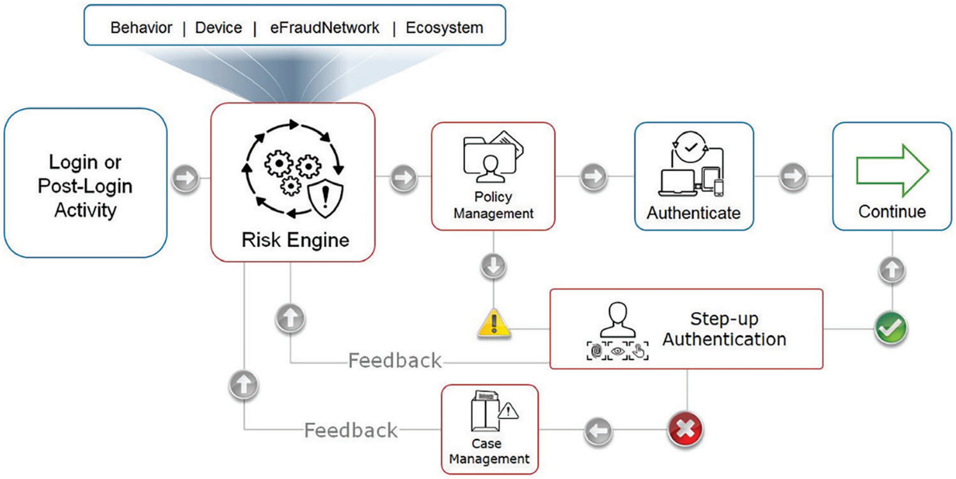


The RSA Adaptive Authentication omnichannel anti-fraud hub is developed for organizations that want to align fraud prevention efforts with risk tolerance and strategic priorities so they can reduce fraud—not their customer base. The platform provides centralized fraud detection across channels with low intervention that uniquely blends risk-based decisioning and flexible rules-based policy management. By incorporating shared global fraud intelligence with the ability to ingest insights from third-party anti-fraud tools, the platform further enriches the risk assessment, improving fraud detection.

Align fraud prevention efforts with risk tolerance and strategic priorities to reduce fraud, not customers.

Powered by the RSA Risk Engine, RSA Adaptive Authentication is designed to measure the risk associated with a user's login and post-login activities (such as: payments, add payee, edit payee and many more) by evaluating a variety of risk indicators. Using powerful machine learning, in company with options for fine-grained policy controls, the RSA Adaptive Authentication anti-fraud hub only requires additional assurance, such as out-of-band authentication, for scenarios that are high risk and/or that violate rules established by an organization. This methodology provides transparent authentication for the majority of the users, ensuring a frictionless user experience and high fraud detection rates.

The RSA Adaptive Authentication anti-fraud hub is comprised of the RSA Risk Engine, RSA eFraudNetwork™, RSA policy management, case management and reports, and a breadth of step-up authentication options. Through the RSA Adaptive Authentication ecosystem approach, organizations can add other data elements to the risk assessment from third-party tools, or their own business intelligence, centralizing fraud prevention efforts and enhancing detection rates.



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. RSA Adaptive Authentication leverages the risk engine to generate a unique score for each user activity that ranges from 0 to 1,000, where 1,000 indicates the greatest likelihood of the activity being performed by a fraudster. The score is reflective of device profiling, behavioral profiling and RSA eFraudNetwork data. The risk engine combines rich data inputs, machine learning methods, authentication feedback and case management feedback to provide accurate risk evaluations to mitigate fraud.

RSA Adaptive Authentication offers proven fraud detection rates from 90-95 percent with low intervention.

Machine learning method

The RSA Risk Engine uses a Naive Bayesian statistical approach to calculating the risk score. A Bayesian approach looks at the conditional probability of an event being fraudulent given the known facts or predictors. All available factors are taken into consideration but weighed according to relevance, so that the most predictive factors contribute more heavily to the score. The combination of an efficient statistical machine learning Bayesian model with RSA's extensive background of fraud expertise, wide range of real-world knowledge and rich feedback enables the RSA Risk Engine to meet the challenges of detecting fraud risks in real time.

RSA ecosystem approach

The RSA Adaptive Authentication ecosystem approach is designed to enable centralized fraud management and enhance fraud detection by using data elements from external sources. The RSA Risk Engine can consume data elements that are not predefined by RSA and use these third-party facts to influence the risk assessment and impact the risk score. Customers can contribute additional insights from both internal knowledge and additional anti-fraud tools.

Break down silos with the ecosystem approach, while instilling cross-channel analytics and enabling omnichannel fraud detection.

RSA Policy Management

The RSA Policy Management application translates risk policies into decisions and actions through the use of a comprehensive rules framework. With fine-grained policy capabilities, organizations can set their policies to reflect business objectives such as identifying fraud prevention targets, improving user experiences and controlling operational costs associated with case analysis.

Device profiling

Device profiling analyzes the device from which the user is accessing an organization's website or mobile application. RSA Adaptive Authentication compares the profile of a given device with previous devices used by the individual in the past. The device profile is used to determine whether the current device is one from which the user typically requests access or if the device has been connected to previous known fraud. Parameters analyzed include IP address and geolocation, operating system version, browser type and other device settings.

Behavior profiling

Behavior profiling is a record of typical activity for the user. RSA 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. For example: is this payment amount typical for the user and is the payee someone the user usually transfers money to?

RSA eFraudNetwork

The RSA eFraudNetwork is a repository of confirmed fraud data elements and fraud patterns gleaned from an extensive network of RSA Fraud & Risk Intelligence Suite customers across the globe. When a fraudulent activity is identified, the data elements included in the activity, such as IP, device fingerprints and payee (mule) account, are moved to the RSA eFraudNetwork. The RSA eFraudNetwork provides direct feeds to the RSA Risk Engine so when an activity is attempted from a device or IP that appears in the repository, the risk score will be raised.

RSA case management

RSA case management enables organizations to track activities that trigger 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 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 enables an organization to provide feedback into the RSA Risk Engine upon case resolution.

The case management API is an extension of RSA Adaptive Authentication case management capabilities, which allow incidents to be shared with existing external case management systems for even greater flexibility. Serving as a conduit, organizations can also leverage the case management API to provide the risk engine additional feedback for learning purposes.

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. Step-up authentication methods supported in RSA 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
- Biometrics: Fingerprint and Face ID 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.
- Multi-credential framework (MCF): Integration of additional third-party authentication methods via the RSA multi-credential framework, such as tokens (i.e., RSA SecurID® tokens) or additional biometric modalities

Take advantage of a variety of step-up options, including fingerprint and Face ID.

Protection for mobile users

The proliferation of mobile devices brings opportunity as well as risk. In Q2 2020, the RSA Adaptive Authentication platform observed that 56 percent of transactions originated in the mobile channel (mobile applications and mobile browsers) and 69 percent of fraud transactions used a mobile application or browser. Through direct integration with RSA Adaptive Authentication, organizations can extend fraud protection to users accessing via a mobile application or mobile browser. For customers interested in using RSA Adaptive Authentication for their mobile application, a software development kit (SDK) is available for Apple iOS and Android OS platforms.

RSA Adaptive Authentication omnichannel fraud prevention

The RSA Adaptive Authentication platform provides omnichannel fraud prevention by enabling a business to leverage risk-based authentication across the channels of their choice, whether it's web, mobile, call center, IVR, ATM, branch or a custom channel. The platform provides an omnichannel architecture in which assets are centralized and shared, so that operations can be carried out as a whole rather than through an array of discrete parts. This eliminates the need to build and maintain a separate infrastructure for every channel. Instead, all channels—both online and offline—can share knowledge and awareness of the consumer's interaction. By instituting an omnichannel fraud prevention strategy, businesses can provide a frictionless consumer experience for legitimate users while providing visibility across consumer facing digital channels.

Utilize the RSA Adaptive Authentication mobile SDK to protect your mobile app.

By leveraging an omnichannel approach, organizations can:

- Increase fraud detection rates
- Holistically mitigate fraud across consumer facing digital channels
- Better utilize existing investments in anti-fraud tools
- Unlock internal business intelligence for use during risk assessment
- Centralize fraud management

Business-driven fraud prevention

RSA Adaptive Authentication is a business-driven security solution that uniquely links business context with anti-fraud efforts, helping organizations manage consumer fraud risk with enhanced visibility, while balancing convenience. The platform allows organizations to blend previously siloed information sources to help deliver actionable insight across an organization's entire environment, so they can make decisions that align with their risk tolerance and strategic priorities—while keeping pace with an evolving fraud landscape by facilitating a continuous feedback loop built around intelligence and machine learning. With a business-driven approach to fraud prevention, anti-fraud leaders are better equipped to discuss the current business impact of fraud risks and prepare for the future by enabling them to work more collaboratively with business leaders to ensure they are protecting what matters most to their organization—stopping fraud, not their customers.

Centralize fraud management with omnichannel fraud prevention.

About RSA

RSA offers business-driven security solutions that provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change. For more information, go to rsa.com.