RSA® Adaptive Authentication

Advanced fraud detection for omnichannel environments

Within the realm of financial services, there are constantly new ways of doing business anytime, anywhere. Digital transformation has become compulsory for every organization to remain relevant and competitive in today's digital economy. With a growing array of digital banking channels available, customers seemingly have infinite possibilities for conducting financial business. Consumers expect the best digital experiences delivered with the least friction. In order to meet end-user demand for convenience, organizations continue to extend product and service offerings across a variety of digital channels.

At the same time, this expansion of banking channels increases the risk of fraud. The ability to manage the risk of fraud can become what frees organizations to embrace business opportunity. A critical consequence of the proliferation of digital banking channels is the problem of having multiple channels that operate independently of each other. Back when “multiple channels” at most meant a bank branch and an ATM network, this wasn't so much an issue. Channels today range from web to mobile browser/mobile app, call centers and IVRs, as well as branches, ATMs and third parties. With so many channels, both traditional and new, organizations are struggling with ways to offer a seamless customer journey while also managing digital risk. Achieving the right balance of security—while maintaining a positive and consistent user experience across channels for consumers—is challenging. Whether the activity involves logging in, performing a transaction, making a payment or editing a profile, among others, consumers expect that the experience across the myriad of channels they're being offered will be both frictionless and secure. A cross-channel experience involving multiple devices through a web and mobile app medium should feel seamless.

Organizations today need to:

• Distinguish between legitimate and fraudulent behavior for consumers across channels

• Reduce fraud losses and operations costs associated with fraud investigation

• Balance risk and consumer convenience

RSA Adaptive Authentication offers proven fraud detection rates from 90-95 percent with low intervention.
• Centralize fraud management and break down business channel silos

• Quantify the business impact with business context around a given fraud incident

What’s needed is an omnichannel architecture in which assets are centralized and shared, so that operations can be carried out as a whole rather than relying on an array of discrete parts. This eliminates the need to build and maintain a separate infrastructure (including separate point solutions for fraud detection and prevention) for every channel. Instead, all channels—both online and offline—can share knowledge and awareness of the consumer’s interaction. This will lead to more streamlined operations, a more secure banking environment and a smoother customer experience.

Within the omnichannel architecture, technologies such as deep entity profiling and machine learning specifically help improve fraud detection. Deep entity profiling involves gathering information from across multiple consumer channels and touchpoints and analyzing it to assess whether a given activity is likely to be fraudulent. When you align your anti-fraud initiatives with digital risk across channels, you start to create an environment that works together—one that takes a wider view of the risk your business faces across channels, and cuts through silos and unneeded complexity.

RSA Adaptive Authentication solves these challenges by providing an omnichannel fraud detection hub, powered by the RSA Risk Engine. Deployed at more than 3,000 organizations worldwide, RSA Adaptive Authentication protects more than 1 billion consumers spanning multiple industries including financial services, healthcare, insurance, retail and government.

RSA Adaptive Authentication overview

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.
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 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, enabling a true omnichannel experience.
The RSA Adaptive Authentication workflow

When a consumer accesses an application protected by RSA Adaptive Authentication (by entering their username and password), the consumer is profiled for this specific activity. The profiling that occurs focuses on 100+ risk indicators that are contributed to the risk engine: information about the user’s device and the user’s behavior, information from the RSA eFraudNetwork and also risk score custom facts, if the business is contributing third-party anti-fraud tool data elements or internal business intelligence.

RSA Adaptive Authentication looks at the device being used for current activity to determine whether it is a device that the user typically leverages, or if the device has been connected to previous fraudulent activities. Further, RSA Adaptive Authentication looks at the current activity and behavior, and compares it with the user’s usual behavior in conjunction with the genuine and fraud population behavior, in order to assess risk. From there, the system checks against known fraudulent data held within the RSA eFraudNetwork—a cross-industry, confirmed fraud repository. This information is provided to the RSA Risk Engine, which computes a risk score for the activity. The risk score is then fed to the RSA policy management application, where the business determines what kind of fine-grained policy should be enacted given risk tolerance. The RSA policy management application then determines if the risk score and/or activity violates an organization’s policies. For example, if the user activity is not deemed suspicious and does not violate any of the policies or rules, the user is transparently authenticated and continues on as normal without any change to their user experience. Thus, there is no impact on usability, and the consumer experience is frictionless.

Conversely, if a risk score exceeds a threshold set in the RSA policy management application, the system can prompt for additional assurance or step-up authentication, mark the activity for later review in the case management application and/or block the activity outright. If step-up authentication is required, and a user fails this attempt, a case is sent to the case management tool. Cases are evaluated by fraud analysts and the results of the analysis are fed back into the risk engine, along with any step-up results.

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, which 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. In addition to considering predefined risk indicators, organizations can leverage the RSA ecosystem approach to incorporate additional third-party risk indicators into the RSA Risk Engine assessment.
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 weighted 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 online fraud risks in real time.

To meet the challenges of fraud detection, the RSA Risk Engine:

- Quickly detects new patterns of behavior and adapts the analysis to these new patterns. This is valid to both genuine and fraudulent activity as the patterns for each change quickly.

- Extrapolates and generalizes based on small samples. Because fraud rates are low, behavior patterns and early warning signs must be extrapolated from small bits of activity. The risk engine is able to extrapolate correctly by working with a background pool of knowledge that enables small activity sets to be understood within a larger context.

- Allows the majority of users to benefit from behind-the-scenes authentication while targeting only a fraction of the population for extra security measures.

- Enables effective real-time learning: Due to the rich feedback, the risk engine can quickly adjust its identified fraud patterns and develop new patterns.

The Naive Bayesian algorithm, leveraged by the RSA Risk Engine, affords fast, highly scalable model building and scoring. Bayesian classifiers are typically faster to learn new fraud patterns on smaller data sets (e.g., when less fraud/genuine feedback is available). They are flexible to additions of new predictors, which is crucial in the ever-changing fraud reality, and their simplicity prevents them from fitting their training data too closely.

With the Bayesian approach, the parameters that contribute to the final risk assessment result can be made visible (hence not a “black box”). This means that Bayesian classifiers are free from the intrinsic disadvantages of other methods (such as Artificial Neural Networks) that cannot provide information about the relative significance of the various parameters. To that end, RSA Adaptive Authentication customers have the ability to understand the top parameters that contributed the most to the risk assessment, and these factors are visualized through a case management application.

BEHAVIORAL PROFILES

In addition to analyzing risk indicators, the risk engine attempts to determine if the various activities are typical for that user by maintaining a profile of the user’s activities and using that profile for comparison.
**RSA ecosystem approach**

The RSA Adaptive Authentication ecosystem approach is designed to enable omnichannel 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.

The RSA Fraud & Risk Intelligence Suite data science team ran a proof of concept (POC) with a large U.S.-based financial institution (FI) over the course of three weeks. The objective was to utilize cross-channel knowledge in order to enhance web and mobile protection using calculated data elements based on the organization phone channel knowledge. RSA performed a simulation and measured the benefit. By using 6 Risk Score Custom Facts shared by the FI, and considering the top 1 percent of high risk transactions, the RSA data science team was able to demonstrate:

- 2 percent improvement in fraud detection across all event types
- 0.9 percent improvement in fraud detection for payment transactions
- $40,000/month in fraud savings for payment transactions

**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 threshold 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, or rules that combine the risk score and additional attributes such as the transaction...
amount (for example, challenge trx with a score over 700 and an amount higher that $500). 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 too?

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. Nearly one in seven 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 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.

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

**Protection for mobile users**

The proliferation of mobile devices brings opportunity as well as risk. In Q2 2018, the RSA Adaptive Authentication platform observed that 56 percent of transactions originated in the mobile channel and 71 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 the entire consumer environment, including channels and user sessions. By breaking through silos, and delivering insights across all channels with multichannel analytics, organizations can gain a deeper understanding of the business impact behind each fraud incident, while reducing fraud. By instituting an omnichannel approach, the business can further link fraud strategy to business strategies and priorities.

By leveraging an omnichannel approach, organizations can:

- Increase fraud detection rates
- Better utilize existing investments in anti-fraud tools
- Unlock internal business intelligence for use during risk assessment
- Centralize fraud management

**Proven fraud detection results**

The RSA data science team publishes the fraud detection rates of RSA Adaptive Authentication to showcase the effectiveness of the solution. The different intervention rates represent the customer’s choice with respect to the percentage of transactions to challenge or decline out of the entire transaction base. As shown in the graph below, by interrupting only 3 percent of the activities, you can stop over 93 percent of the fraud attempts. Organizations set their intervention rates to reflect the balance they are seeking to strike between consumer convenience and strong fraud protection.

Looking at Figure 1 below, RSA Adaptive Authentication customers have recorded fraud detection rates, at login, of 92.3 percent for the web channel, and 91.8 percent for the mobile channel, with only a 3 percent intervention rate.

Fraud detection rates are measured by the percentage of fraud transactions in the respective risk score band/intervention rate, out of the entire fraud transactions.

![FRAUD DETECTION RATE](image)

**Figure 1**
Looking at Figure 2 below, RSA Adaptive Authentication customers have recorded fraud detection rates, at payment, of 93.6 percent for the web channel and 90.3 percent for the mobile channel, with only a 3 percent intervention rate.

**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.

**Omnichannel visibility**

- **Omnichannel protection**: Protect consumers across channels through a centralized anti-fraud hub

- **RSA eFraudNetwork**: Cross-institutional, confirmed fraudulent indicators increase your fraud detection (14 percent of fraudulent transactions in RSA Adaptive Authentication have an entry in the RSA eFraudNetwork)

**Insights & flexibility**

- **RSA ecosystem approach**: Leverage existing investments and utilize your own business insights: In addition to proven, predefined risk indicators, the RSA Risk Engine provides organizations the option to ingest their own third-party risk indicators to both further enhance fraud detection and augment their existing, current set of anti-fraud investments
• **Deployment options**: On premises or cloud

• **Case management API**: Leverage the built-in case management tool or integrate your preferred case management application

**Action—reduce fraud not customers**

• **90-95 percent fraud detection rates with low intervention** across channels

• **Consumer choice**: Balance your security and consumer needs with a breadth of step-up authentication options including biometrics and transaction signing

• **Proven reliability**: Over 3,000 organizations choose RSA Adaptive Authentication

**About RSA**

RSA® Business-Driven Security™ solutions link business context with security incidents to help organizations manage digital risk and protect what matters most. With a ward-winning cybersecurity solutions from RSA, a Dell Technologies business, organizations can detect and respond to advanced attacks; manage user identities and access; and reduce business risk, fraud and cybercrime. RSA solutions protect millions of users around the world and help more than 90 percent of Fortune 500 companies thrive in an uncertain, high-risk world.