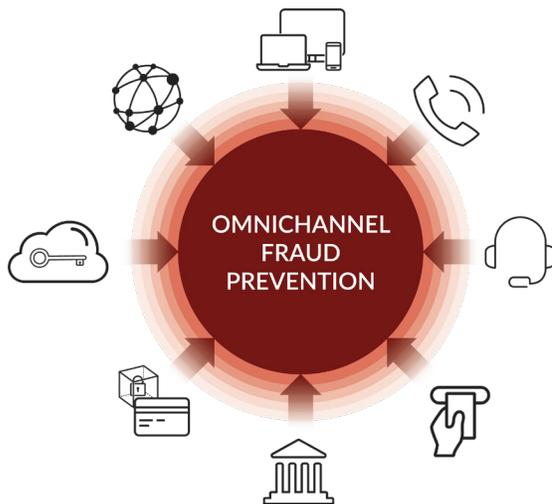


RSA® Adaptive Authentication

Transaction signing

RSA adaptive authentication overview

In order to meet end-user demand for convenience, organizations continue to extend product and service offerings across channels. At the same time, fraud continues to proliferate with cybercriminals leveraging 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.

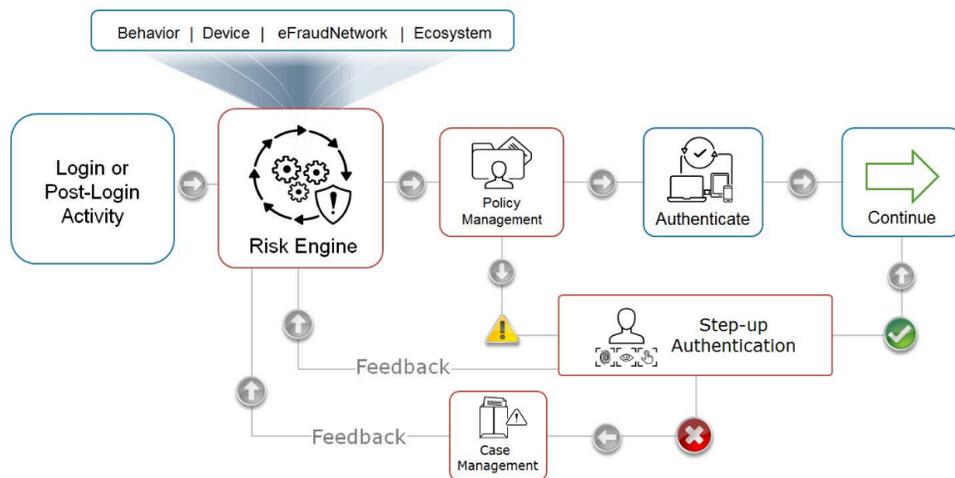


The RSA Adaptive Authentication omnichannel anti-fraud hub is developed for organizations that want to align fraud prevention efforts with risk tolerance and strategic priorities so they can reduce fraud—not their customer base. The platform provides centralized fraud detection across channels with low 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.

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.

Despite the convenience offered to end users, these channels are vulnerable to hackers who continue to proliferate and evolve, leveraging phishing, Man in the Middle (MitM), Man in the Browser (MitB), and other advanced techniques to gain unauthorized access to funds, accounts and transactions. Deploying risk-based authentication at both login and post-login has become necessary to protect online financial accounts and transactions. However, fraudsters continue to develop more sophisticated MitB Trojans, which infect a user's browser and are capable of manipulating webpages and transaction details in real time.

Figure 1: The RSA Adaptive Authentication workflow:



“Assure the integrity of a payment transaction, the device being used, and the authenticity of the user to combat fraud”

Protecting payment transactions with transaction signing

Protecting payment transactions and the loss of money due to fraudulent transactions is top of mind for both your organization and your customers alike. A secure solution that both instills confidence and is easily adopted by your end users is needed. A transaction protection solution that monitors and challenges high-risk transactions after login has become an essential part of a layered security strategy.



By using the RSA Adaptive Authentication anti-fraud hub to understand the risk of each payment transaction, you can apply the correct control based upon the risk level. As a step-up validation method for payment transactions within RSA Adaptive Authentication, RSA Transaction Signing assures the integrity of a payment

transaction, the device being used and the authenticity of the user to combat fraud from advanced Trojan attacks. RSA Transaction Signing allows genuine end users to cryptographically sign their payment transactions by using specific details such as destination account and payment amount to ensure transaction integrity. Given granular policy controls, should any payment transaction details be changed or tampered with by a fraudulent entity, the transaction will be blocked.

Figure 2: The RSA Adaptive Authentication Transaction Signing workflow:



“By leveraging the Mobile SDK, Transaction Signing has the optional ability to take advantage of fingerprint and Face ID”

RSA Transaction Signing takes advantage of the RSA Adaptive Authentication Mobile Software Development Kit (SDK), which allows your developers to build controls directly into mobile applications. When a transaction-signing validation policy is invoked based on the risk score, a push notification via the Azure Mobile Service sends a notification to the end user's mobile phone to complete the transaction. By leveraging the Mobile SDK, Transaction Signing has the optional ability to take advantage of fingerprint and Face ID technologies that are available as a means of layered step-up authentication. By combining a cryptographically signed payment transaction with a follow-up biometric authentication into one simple mobile device workflow, organizations can improve the user experience for their customers by eliminating the need for additional hardware.

Using a fully software-based layered security approach, RSA Transaction Signing allows you to offer the highest level of transaction protection to your end users. RSA Adaptive Authentication provides the granular controls to invoke transaction signing through policies when the risk level is most appropriate. Enriched through the Mobile SDK, Transaction Signing is highly customizable and configurable to balance end-user convenience and mitigate payment transaction fraud.

Benefits of transactions signing:

- Mitigate fraudulent payment transactions stemming from banking Trojans
- Instill end-user confidence through transaction integrity and biometric authentication
- Secure high-value and risky transactions through step-up validation

- Mitigate MitB and MitM attacks by cryptographically signing payment transactions
- Help meet regulatory compliance recommendations for transaction signing

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..

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 award-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.

