THE RSA RISK ENGINE

THE ESSENTIALS

Unparalleled fraud detection

The RSA Risk Engine (RE) analyzes a range of indicators associated with an activity to determine the probability that the activity is fraudulent.

Multiple, Diverse Data Inputs

The RSA RE analyzes a range of diverse data for user online activities including logins and financial transactions. Data inputs include a set of facts that identify the activity, historical profiles (behavioral profiles and device profiles) and data from the RSA eFraudNetwork.

Machine Learning Methods

The Risk Engine combines Bayesian machine learning methods with sophisticated device identification and recognition and user behavior analysis. This enables the intelligent decisioning that significantly reduces fraud.

Authentication Feedback

Rich feedback from a variety of methods enables the RSA RE to self learn and tune when introduced to new fraud patterns.

Advantages of the RSA Risk Engine

- Transparent real-time fraud detection with minimal impact to user experience
- Risk engine learns from past behavior and adjusts to predict and protect against future attacks
- Balances risk, cost and convenience - high fraud detection rates with low intervention rates

In today's hyper-connected world, people are spending more and more time on the internet, phone, and mobile devices to complete more of their daily activities such as online banking and shopping. The convenience afforded by the access and availability of the digital world, however, is not without drawbacks. Increased access and mobility have brought with it an unparalleled growth in online fraudulent activity.

Articles about identity takeover by Trojans, Man in the Middle, Man in the Browser, and phishing, are constantly in the news. These threats have triggered a growing awareness by institutions and consumers alike along with universal acceptance of the fact that these threats are serious and must be addressed. Organizations, trying to encourage consumer activity while at the same time minimizing losses from financial fraud, are looking for ways to identify and block fraudulent transactions while letting genuine activities proceed unimpeded.

THE RSA RISK ENGINE

The RSA Risk Engine (RE) is integrated with RSA's anti-fraud and authentication solutions to provide efficient and effective risk assessment of online activities. Used today by leading banks, credit and debit card issuers, and other organizations worldwide, the RE detects, analyzes, scores and manages online activity for the purpose of consumer protection. It reduces the risks of privacy and compliance exposure, lowers the level of fraud, detects possible impersonators, and identifies new fraud trends as they develop.

The RE collects and analyzes vast amounts of login and transactional data from multiple channels and does a risk assessment on the end user's activity. This risk assessment is the foundation of transparent authentication whereby the majority of transactions pass unhindered and only the riskiest transactions are asked for additional authentication. Taking into consideration multiple factors including user behavior and device, the RE employs a self-learning statistical model that can be used alongside the policy manager and significantly reduce fraud while supporting the organization's risk tolerance.

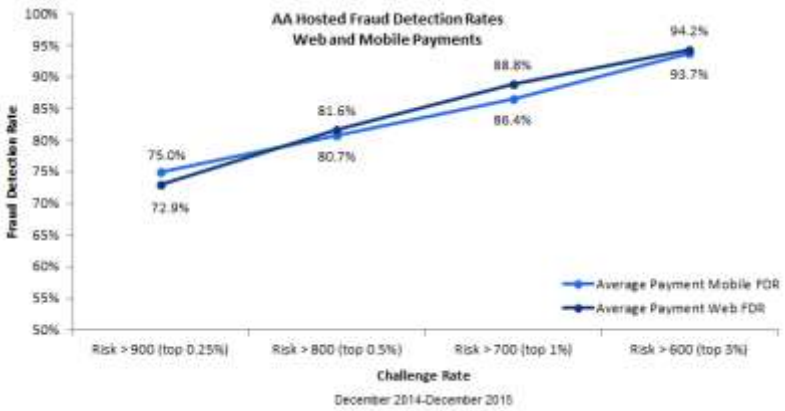
UNPARALLELED FRAUD DETECTION, LOW INTERVENTION

The RSA Risk Engine analyzes a range of indicators associated with an activity to determine the probability that the activity is fraudulent. It looks at fraud patterns and uses advanced analytics to correlate variables. The accumulated knowledge of decades of security and fraud fighting experience and fraud intelligence work combined with an intelligent analysis of the data points collected work together to create the best risk-based fraud detection solution in the marketplace.

The Risk Engine delivers unparalleled fraud detection rates even with low intervention rates. The graph below, which reflects data from the hosted customer base for our Adaptive Authentication solution, illustrates this. Think about achieving a 93% fraud detection rate while challenging only 3% of transactions - this is an incredibly powerful combination. Using the Policy Manager to apply specific business logic and step up authentication methods can drive the fraud detection rate even higher or the challenge rate even lower.

In the graph below*, fraud detection rates for both payments and logins increases as the intervention rates increases – the more users that are challenged, the more fraud will be detected. Customers can configure their challenge rates to balance customer convenience and strong fraud protection in a way that reflects their risk tolerance and unique end user attributes.

To calculate the most accurate risk score, the RE takes a wide range of indicators and attributes into consideration. In addition to quantity, the quality of the data collected is also considered, with indicators having more predictive value adding more weight to the calculated risk score.



The RE combines copious data collection, machine learning methods and rich authentication feedback to provide intelligent, real-time risk evaluations to mitigate fraud.

**Note: Data reflects average FDRs for customers who mark fraud in their application. Actual fraud detection rates can vary based on use case, implementation and other factors.*

RICH DATA INPUTS

The RE analyzes multiple, diverse data inputs for every user activity. The activity details analyzed by the RE include a set of data facts that identify the activity, historical profiles and data from the RSA eFraudNetwork. High risk transactions can be blocked, prompted for further authentication, or passed to an analyst for further review based on customer policies.

Facts that identify the activity include:

- Activity type (e.g., login, payment, password change)
- User details including name, language, country, etc.
- Device details including IP address, browser characteristics, screen resolution, etc.

- Mobile device details including mobile sim id, mobile geo location, wifi MAC address, etc.
- User interactions with the browser such as mouse movements and key strokes
- Payment details such as the amount, currency, and the payee account
- Indicators of Trojan malware activities

The Risk Engine also recognizes the channel from which the activity is generated and adjusts the risk model accordingly. Risk scoring of transactions from the mobile channel will include mobile-specific device parameters and a mobile-optimized scoring algorithm will be used. There is also cross-channel correlation for relevant patterns and data inputs.

RSA eFraudNetwork

RSA eFraudNetwork (eFN) helps organizations proactively identify and track fraudulent activities across more than 150 countries. The RSA eFN is the industry's first and largest cross-institutional, cross-platform, international, online fraud network. In existence for over 9 years, it currently has over 8,000 contributors worldwide including financial institutions, credit and debit card issuers, health care firms, Internet Service Providers, wireless providers, high-tech companies, and government and law enforcement agencies. The information sharing across thousands of RSA customers and 1/2 billion end users and devices creates a vast and valuable source of data.

Not only does the intelligence added to the eFraudNetwork data repository come from multiple sources, it is comprised of many different types of data elements: IP addresses, device fingerprints, cookies, mule account numbers, etc. When a transaction or activity is attempted by a device, IP address, or payee account that appears in the eFN as having been used in a fraudulent transaction, it will be taken into account by the RSA Risk Engine.

RSA FraudAction Intelligence

RSA fraud analysts go "undercover" and socialize with online fraudsters to gain valuable insight into their practices. This research provides RSA with a unique understanding of the fraudsters' motivation and patterns, invaluable when devising fraud fighting techniques.

MACHINE LEARNING METHODS

BEHAVIORAL PROFILES

In addition to analyzing risk indicators, the RE 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.

The RE risk model is based on RSA's extensive fraud fighting experience. The risk model is self-learning and will adapt itself based on feedback. The feedback loop includes case resolution and genuine or failed authentication results as well as chargeback files for Adaptive Authentication for eCommerce. The RE modifies its risk predictions based on case investigation results which automatically update the risk model to be able to catch fraudulent activities that were missed, or genuine activities that were wrongly flagged.

The RE uses a Naïve 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 - the most predictive factors contribute more heavily to the score.

The combination of an efficient statistical machine learning Bayesian model with RSA's rich background of fraud expertise, wide range of real world knowledge, and rich feedback enables the RE to meet the challenges of detecting and mitigating 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 RE analysis to these new patterns. This is valid to both genuine and fraudulent activity as the patterns for each change quickly.
- Extrapolate and generalize based on small samples. As fraud rates are low, behavior patterns and early warning signs must be extrapolated from small bits of

activity. The RE 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.

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

- Enable effective real-time learning. Due to the rich feedback, the RE can quickly correct errors as they occur and minimize the impact of errors.

Analyzes Activity According to Historical Profiles

The RE maintains profiles for historical data collection. For example, the device profile captures different device related data facts. For the web channel, data includes:

- HTTP headers, operating system versions, and patch levels

- Browser type and version, software versions, display parameters (size and color depth), languages, time zone, etc.

- IP address, extracted IP geo location details, and additional information on the ISP, IP owner, connection type, etc.

For mobile devices, the device profile contains additional device identifiers such as the IMEI, the ICCID, and more. In addition, the geo-location of smart mobile devices is not based solely on the IP, but also on information that can be collected directly from the mobile device itself.

The device profile is used to determine whether the current device is one from which the user usually seeks account accesses or generates transactions. The RE also checks the eFraudNetwork to determine if a device has been used in a fraudulent transaction within the consumer population as well as across activities of other RSA customers.

User profiling is used to maintain behavioral facts related to end-users. The RE attempts to determine if the various activities are typical for that user by maintaining a history or profile of the user's activities and comparing current activity against that historical profile. The RE looks at variables such as the type of payment being made, if the payee account has received payment in the past, the amount characteristic of the user, etc.

In parallel, the RE tries to determine the odds that a transaction is fraudulent by looking at fraud patterns. Examples of fraudulent activity patterns include:

- Recent alert settings change followed by a payment with high amount or to a new payee.

- Payee accounts that have been involved in previous fraud confirmed cases.

- High accumulated payment amount—instead of one high amount transaction, the fraudster completes a number of lower value transactions.

- High value deposit followed by withdrawal of the full amount shortly thereafter.

Finally, the RE compares the collected data to the general population behavior as well as the individual user's past behavior. This is done to learn what legitimate activity looks like for this particular site and reduce false positives.

If the activity appears typical, there is no indication of a Trojan acting on behalf of the user, and the activity is not typical of fraudulent behavior, then the transaction will receive a low risk score and the user will be authenticated transparently. Otherwise, the RE will assign a higher risk score to the activity and the user will be asked to authenticate himself/herself.

AUTHENTICATION FEEDBACK

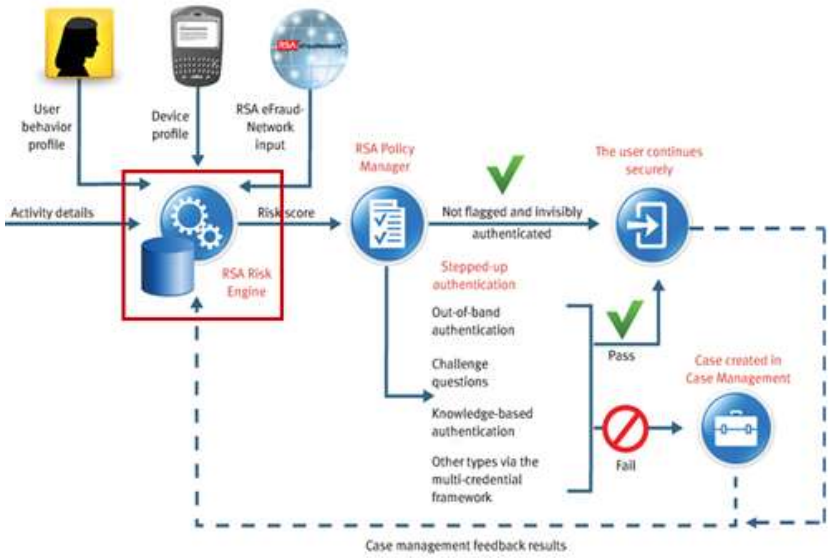
The Risk Engine is self-learning and can change its future predictions based on the following three types of feedback:

- Case management feedback –Adaptive Authentication creates cases for investigation, and the RE modifies its future risk predictions based on the case

investigation results (e.g., fraud cases that were missed, or genuine users that were wrongly flagged).

- Authentication result feedback - In the same manner as genuine and fraud feedback in case management, if a user was required to pass additional authentication and failed, the risk engine is notified and the associated account and related profiles are flagged as having failed authentication. Consequently, future transactions coming from the same account with similar device parameters and similar behavior will have higher risk scores. If the authentication was completed successfully, the risk engine is notified and the associated account and related profiles are marked as having successful authentication. Consequently, future transactions coming from the same account with similar device parameters and similar behavior will be deemed to lower risk scores.

- Chargeback feedback (Adaptive Authentication for eCommerce) – similar to case management feedback, the Risk Engine learns of missed fraud from chargeback data and adapts the risk model to identify the type of cases that were missed.



THE RISK ENGINE – A CORE RSA TECHNOLOGY

The RSA Risk Engine is a central component of many RSA authentication and anti-fraud products. For example, RSA's Fraud and Risk Intelligence suite of products utilizes the RSA Risk Engine technology to understand risk when dealing with the ever changing fraud landscape. RSA Adaptive Authentication and Transaction Monitoring rely on the RE to secure online activities.

RSA Adaptive Authentication and Transaction Monitoring are multi-channel risk-based authentication and fraud detection solutions that provide cost-effective protection for an entire user base. Powered by RSA's Risk Engine, Adaptive Authentication and Transaction Monitoring provide strong and convenient protection by monitoring and authenticating user activities based on risk levels, institutional policies, and user segmentation. The RE's ability to learn from historical activities and adapt the risk assessment allows a true risk-based approach to authentication.

Risk Based Authentication offers behind-the-scenes monitoring that is invisible to the end user. It is only when an activity is identified as high-risk that a user is then challenged to provide additional authentication, usually in the form of challenge questions or out-of-band phone authentication. With low challenge rates and high fraud detection rates, RSA Adaptive Authentication and Transaction Monitoring offer strong protection without impacting the end user experience, making it an ideal solution for deployment to a large end user base.

With the RSA Risk Engine and input from the RSA eFraudNetwork, RSA Adaptive Authentication and Transaction Monitoring are the forefront solutions for fraud detection and prevention.