# RSA RISK ENGINE

## Introduction to the machine learning risk engine

## ESSENTIALS

### Unparalleled fraud detection

The RSA Risk Engine (RE) analyzes an activity to determine how reasonable and/or typical activities are for individual users, and if it is indicative of fraud.

### Multiple, Diverse Data Inputs

The RSA RE analyzes multiple, diverse data inputs for every user activity. The activity details analyzed by the RE are actually a set of data facts that identify the activity, data from the RSA eFraudNetwork and input from RSA FraudAction intelligence.

### Machine Learning Methods

Combining Bayesian Machine Learning methods with sophisticated analysis of device recognition and user behavior enables intelligent decisions to mitigate 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.

In today's high-tech, fast-paced, 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. Employees, contractors, and vendors demand connections to the enterprise when and where they want to be able to work remotely. The convenience afforded by the access and availability of the online world, however, is not without drawbacks. This increased access has brought with it an unparalleled growth in online fraudulent activity.

Articles about identity takeover, filled with phrases like Trojan, Man in the Middle, Man in the Browser, and Phishing, are increasingly in the news. These emerging threats have triggered a growing awareness by institutions and consumers alike. These threats are serious and must be addressed. Financial institutions, 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 Anti-Fraud and Authentication solutions to provide efficient and effective risk detection 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 and employee 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 compiles a risk assessment on the integrity of the end user's activity. This risk assessment serves as the basis for allowing transparent authentication whereby the majority of transactions pass unhindered, identifying only the most risky transactions 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 a policy manager to create a layered approach to security.

## ENABLES UNPARALLELED FRAUD DETECTION

The RE analyzes an activity to determine both how reasonable and/or typical this activity is for a user, and if it is indicative of fraud. It also looks at fraudulent patterns and uses advanced analytics to correlate among the various 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 through a variety of means and approaches work together to create the best risk based fraud detection in the marketplace.

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

## RICH DATA INPUT

The RSA RE analyzes multiple, diverse data inputs for every user activity. The activity details analyzed by the RE are actually a set of data facts that identify the activity, data from the RSA eFraudNetwork and input from RSA FraudAction intelligence.

To achieve the best results and assign the most accurate risk score, the RE takes as many factors as possible into consideration.  In addition to quantity, the quality of the data collected is also considered.

### User activity facts can include:

- The activity type such as Sign-in, Payment, or a Password Change.
- Details about the user such as the user name, user language, user country, etc.
- Details about the device that is used by the user such as IP address, browser characteristics, screen resolution characteristics, etc.
- Details that are relevant to the mobile device in use, such as mobile sim id, mobile geo location, wifi MAC address, etc.
- Details about user interactions with the browser such as mouse movements and key strokes.
- Details about payments such as the amount, currency, and the payee account.
- Details that can indicate a Trojan malware infection.

### RSA eFraudNetwork

RSA eFraudNetwork (eFN) helps organizations to proactively identify and track fraudulent profiles, patterns, and behaviors 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 many 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.

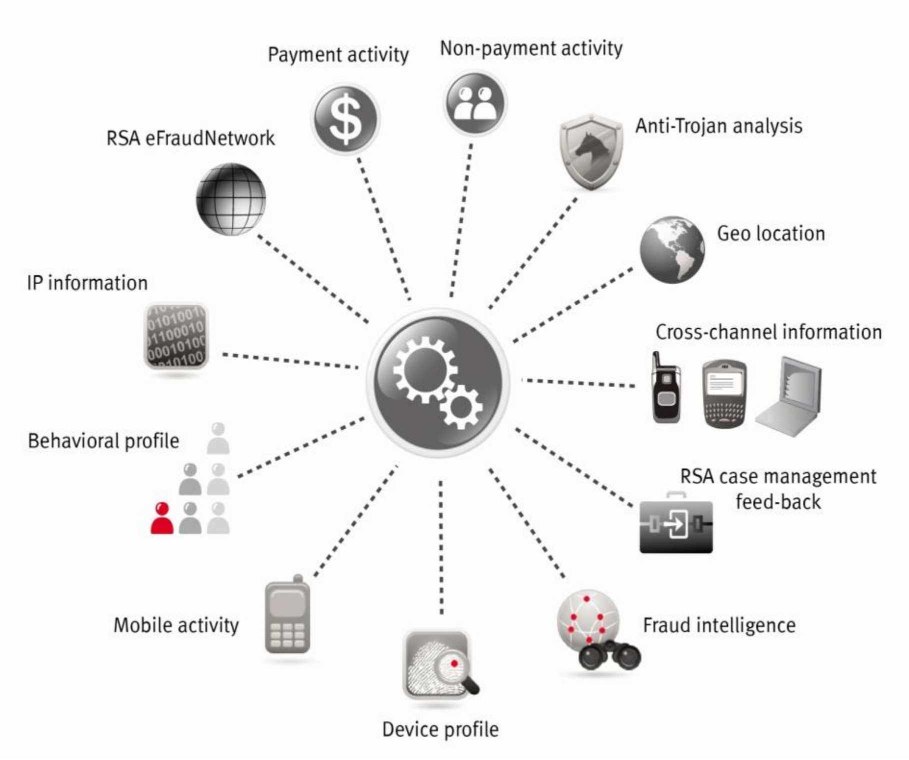
Not only does the intelligence added to the eFraudNetwork data repository come from multiple sources, it is comprised of many different types of data elements: IP addresses, device fingerprints, cookies, mule accounts, etc. When a transaction or activity is attempted by a device, IP address, or payee account that appears in the eFN as fraudulent, it will be taken into account with the RSA Risk Engine, which will deem the transaction to be high risk and either block, prompt for further authentication, or pass to an analyst for further review based on customer policies. The information sharing across thousands of RSA customers and 1/2 billion end users and devices creates a vast source of data.

### 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.  The FraudAction team will add data to the risk engine by asking questions like - Is this IP address on a blacklist or has it been otherwise flagged as suspicious based on RSA research and/or information from our Anti-Fraud Command Center?

**RSA Risk Engine Inputs**

To achieve the best results and assign the most accurate risk score to detect fraudulent activity, the RE takes as many factors as possible into consideration. In addition to quantity, quality of the data collected is also taken into consideration via a weighting and normalizing process. In other words, the more meaningful the information collected and analyzed, the more valid the conclusions can be.



## MACHINE LEARNING METHODS

The RE risk model is based on RSA's extensive fraud fighting experience. The risk model is self-learning—meaning it learns from case resolution, as well as genuine or failed authentication feedback. 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 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 banking and ecommerce 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 both 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:

- Device profiling is used for maintaining the 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 accesses (data/information). The RE also checks if a device is known from former fraudulent or genuine activities in the employee or 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 using that profile for comparison. The RE looks at items 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.

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.

In addition, the RE also checks the user profile for any historical or real-time indication of the user being infected by a Trojan malware.  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.

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

- Recent alert settings changes 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 amount deposit followed by withdrawal of the full amount shortly thereafter.

Last but not least, the RE examines the collected data in relation to the user and in relation to the general population. This is done to learn what legitimate activity is even though it may appear to be fraudulent and reduce false positives

### AUTHENTICATION FEEDBACK

The Risk Engine is a self-learning module, which can change its future predictions based on the following 3 types of feedback:

- Case management feedback – the Risk Engine/RSA® Adaptive Authentication for eCommerce solution creates cases for investigation, and modifies its future risk predictions based on the case investigation results – changing the risk model to be able to catch fraud cases that were missed, or genuine users that were wrongly flagged.
- Chargeback data feedback – similar to case management feedback, the Risk Engine learns of missed fraud from the chargeback and changes the risk model to be able to catch cases that were missed.
- 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 other parameters 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 other parameters are marked as having successful authentication. Consequently, future transactions coming from the same account with similar device parameters and similar behavior will have lower risk scores.

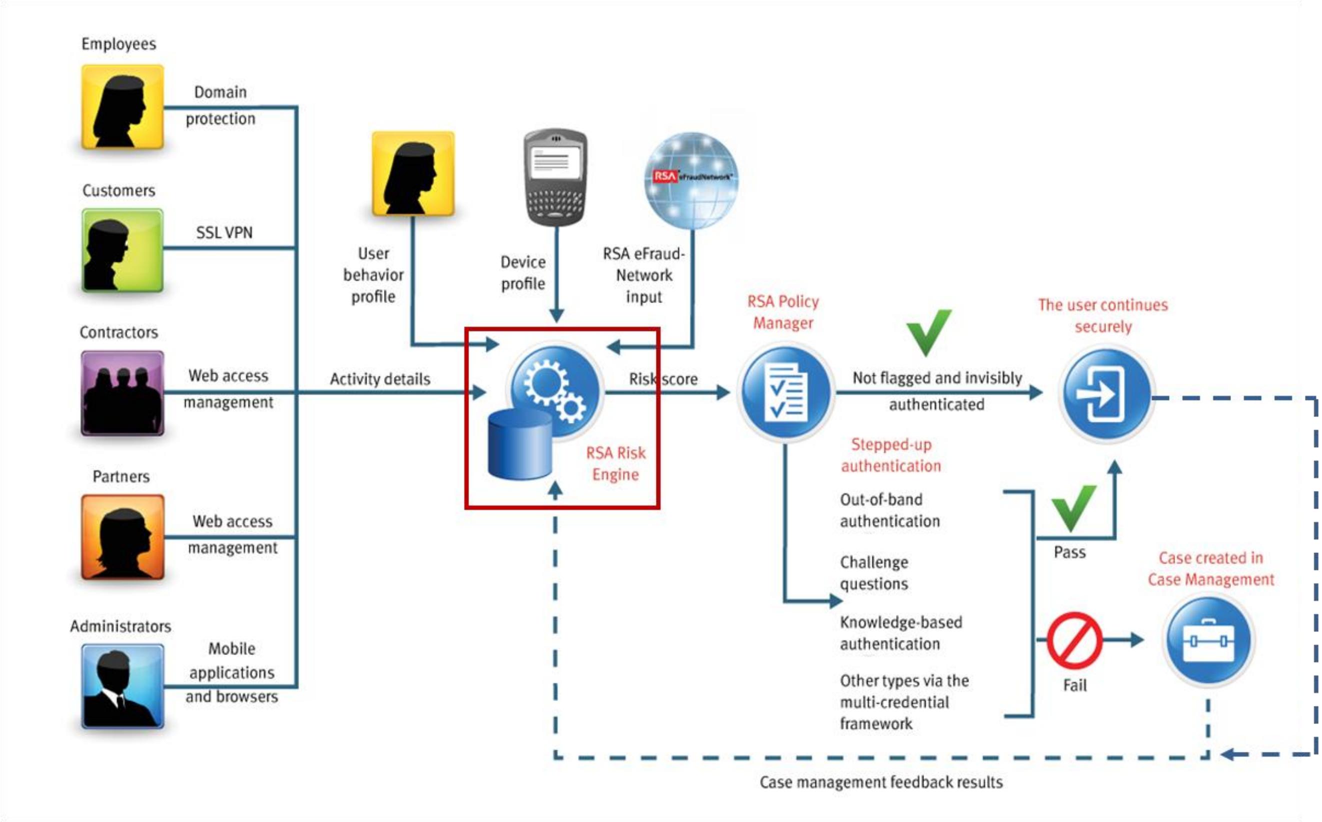
## THE RISK ENGINE IS A CORE RSA TECHNOLOGY

The RSA Risk Engine is a central component of many RSA authentication and anti-fraud products. For example, RSA's Identity Protection and Verification suite of products utilize the RSA Risk Engine technology to understand risk when dealing with the ever changing fraud landscape. Following is an example of how 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 platforms 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 to 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 user. It is only when an activity is deemed to be 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 completion rates, RSA Adaptive Authentication and Transaction Monitoring offer strong protection and superior usability, and provide an ideal solution for deployment to a large user base.

### RSA Risk Engine is central to RSA Adaptive Authentication & Transaction Monitoring


Employees
Domain protection
Customers
SSL VPN
Contractors
Web access management
Partners
Web access management
Administrators
Mobile applications and browsers
Activity details
User behavior profile
Device profile
RSA eFraud-Network input
Risk score
RSA Risk Engine
RSA Policy Manager
Not flagged and invisibly authenticated
The user continues securely
Stepped-up authentication
Out-of-band authentication
Challenge questions
Knowledge-based authentication
Other types via the multi-credential framework
Pass
Fail
Case created in Case Management
Case management feedback results

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.

## CONTACT US

To learn more about how EMC products, services, and solutions can help solve your business and IT challenges, contact your local representative or authorized reseller—or visit us at www.EMC.com/rsa.

EMC believes the information in this document is accurate as of its publication date. The information is subject to change without notice.