RSA® TRANSACTION MONITORING

A powerful layer of fraud protection for financial institutions

AT A GLANCE

- Monitor, detect and investigate fraudulent activity
- Protection against advanced threats such as man-in-the-browser and man-in-the-middle Trojans
- An additional layer of defense that can be easily implemented on top of most existing authentication solutions
- Eliminate the impact on the end user experience

Deploying strong authentication at login has become necessary to protect online financial accounts. However, fraudsters have developed technology, such as man-in-the-browser Trojans, that can bypass login authentication – and even bypass two-factor authentication systems. As a result, a transaction protection solution that monitors and challenges high-risk transactions or behavior after login has occurred is an essential part of a layered security strategy.

RSA® Transaction Monitoring is an advanced fraud detection platform for identifying fraudulent activity or transactions. RSA Transaction Monitoring offers advanced Trojan protection features including sophisticated behavioral analysis, Trojan behavior detection, and fraud monitoring to protect against attacks that can circumvent strong authentication.

RSA Transaction Monitoring allows financial institutions to:

- Monitor, detect and investigate fraudulent activity
- Add a powerful layer of security on top of existing strong authentication solutions – without disruption
- Defend against advanced threats such as man-in-the-browser Trojan attacks
- Identify fraud without impacting end users
- Increase the operational effectiveness of internal fraud analysis teams

A POWERFUL LAYER OF SECURITY WITHOUT DISRUPTION

RSA Transaction Monitoring can be layered on top of any existing authentication solution with no need to replace or alter what is already deployed including:

- One-time-password authentication
- EMV/CAP smart card authentication
- SMS mobile authentication
- TAN or iTAN lists, bingo/scratch/matrix cards
- PKI-based / client software (non-browser based) solutions
- Static login and password

In addition, RSA Transaction Monitoring can be deployed so that it is completely invisible to end users, eliminating any negative impact on the user experience. If a high-risk transaction is detected, RSA Transaction Monitoring can be set up to challenge users in real-time with an array of additional options, including out-of-band authentication. Full case and investigation management are included.

Data Sheet

The RSA® eFraudNetwork™ Service

Transaction Monitoring is also supported by the RSA® eFraudNetwork™ service, a cross-organization repository of fraud patterns gleaned from RSA's extensive network of customers, ISPs and third party contributors across the globe. When an activity is identified as being high-risk, the fraud data, transaction profile, mule account info and device fingerprints are moved to a shared data repository. The eFraudNetwork service directly contributes feeds on fraud data to RSA Transaction Monitoring and is one of the many sources used in assigning a risk score.

ADVANCED BEHAVIORAL ANALYSIS AND TROJAN DETECTION CAPABILITIES

RSA Transaction Monitoring is able to detect Trojans by conducting advanced behavioral analysis. The normal patterns of a behavior for each individual user are observed, and when any behavior that deviates from that pattern occurs, it will impact the risk score assigned to an activity. Analysis of behavior, especially behavior such as payment activities initiated by an end user, is critical at the transaction level to mitigate man-in-the-browser attacks as a Trojan generally waits until the user accesses their bank account before taking action.

During an online banking session, some patterns might be indicative of unusual behavior for the user such as adding a new payee followed by an immediate payment transaction to that payee. This type of activity cannot be detected at login. Additionally, RSA Transaction Monitoring includes even more advanced capabilities for identifying Trojans such as detecting manual session hijacking, mule accounts and HTML injection and Trojan behavior pattern analysis.

RSA Transaction Monitoring is powered by the self-learning RSA Risk Engine that conducts a risk assessment of all users behind the scenes. Each time a user initiates a transaction, it is assigned a unique risk score. When a risk score exceeds an acceptable threshold (as established by each organization) or an organizational policy is violated, a case will be opened in the RSA Case Manager tool. The Case Manager allows financial institutions to conduct full case and investigation management with a focus on only the highest risk transactions. In cases of extreme risk or when there is not sufficient time to manually review a case, the user can be challenged in real-time with an out-of-band phone call before the transaction can proceed .

MONITOR LOGIN AND POST-LOGIN ACTIVITIES

Transactions typically require more scrutiny and pose more risk than just the act of logging in to an account. For example, an unauthorized user might secure login access to an account, but the most risk is posed once a transaction is attempted, such as transferring money out of the account. A transaction protection solution will alert fraud investigation teams or challenge the users appropriately in these instances.

RSA Transaction Monitoring can be integrated at various points within online financial services applications. Typical activities monitored by the system include:

Money transfers. The system will pinpoint potentially fraudulent money transfer transactions as soon as they occur, enabling a financial institution to identify compromised accounts as well as destination accounts used by fraudsters. The system can also monitor for the addition of new beneficiaries, requests for additional credit or new checks, viewing checks and online payments.

Profile changes. The system can be set to trigger investigations of high-risk touch points such as changes to the user's password, email, address, security questions, telephone numbers, or ATM card PIN.

Multiple failed login attempts. Multiple failed login attempts alerts the Risk Engine of possible high-risk activity.

TM DS 0511 H11916