EASYSOLUTIONS®

> Product Overview

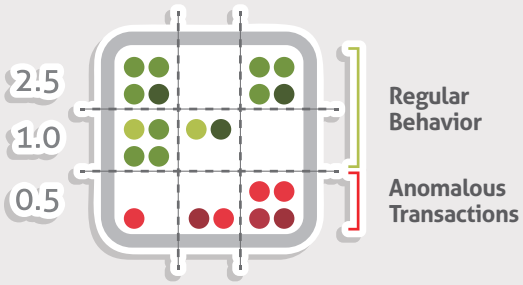
DetectTA®

Leverage the Power of Authentication and Safe Browsing for More Effective Risk Monitoring

Transaction risk and login monitoring are crucial necessities for institutions looking to stop fraud. However, banks and other organizations that are solely relying on rules-based analysis to detect anomalies are not leveraging all the tools and strategies currently available to stop fraudulent transactions. By merging the power of DetectTA's real-time threat evaluation, DetectID's strong multi-factor authentication system and Detect Safe Browsing's keen identification of compromised devices, banks can stop unsafe transactions while providing a frictionless authentication process for legitimate customers.

Combine threat-evaluation technology with an authentication system and malware detection to successfully protect against cybercriminals.

Behavior-Based Analysis: A Better Way to Detect Anomalies



Detecting anomalies by tracking user behavior

Utilizing behavioral analytics combined with rules-based analysis is a far more effective method of monitoring fraud than rules-based analysis alone. DetectTA instantly qualifies a transaction's risk based on a heuristic profile of user behavior learned over time. A baseline profile is created for each user, documenting both their IP geolocation data, as well as their normal habits such as transfer, withdrawal and purchase history. Prior data that institutions possess about their customers' past transactions can be fed into DetectTA's heuristic engine.

Instantly qualify a transaction's risk through heuristic analysis of customer behavior using machine learning techniques.

Since DetectTA creates a baseline profile and documents normal habits and history, non-financial transactions can be monitored using this state-of-the-art technology as well. DetectTA is able to find anomalies in all types of transactions, even if those transactions do not involve money. This also means that financial institutions can identify more risks by correlating monetary transactions with administration events.

While behavioral analysis is a critical component of risk-based monitoring, the DetectTA strategy does not exclude rules-based analysis. Institutions can also screen transactions through the use of a rule-creation engine. Alerts are then generated for atypical activities. This is an effective feature to assist with meeting compliance directives.

Rules can even be created to generate alerts associated with non-financial activities such as logins and personal information updates, or even block the activity entirely. This feature is vital to a proactive approach because it alerts about potentially suspicious behavior before money is actually stolen.

EASYSOLUTIONS®
TOTAL *FRAUD PROTECTION*

> Product Overview

Easy Authentication Following A Suspicious Transaction

Once DetectTA identifies a potentially fraudulent transaction, risk-based authentication then can be implemented to determine if the end user is legitimate. By utilizing this sophisticated system, financial institutions avoid challenging random customers without cause, and can choose a level of authentication which is appropriate for the risk involved.

Authenticate risky transactions instantly by leveraging the power of DetectID, which provides frictionless methods of verifying end users.

After a suspicious transaction or login occurs, a financial institution can employ a diverse array of methods through DetectID to ensure the customer is not a fraudster. For example, if DetectTA identifies a suspicious transaction, a request for more authentication can be instantly sent to the customer's mobile device. The request can come in the form of a push alert, allowing customers to verify themselves and their transactions by simply pressing a button on their mobile device after DetectID automatically sends out the push alert. Financial institutions also have the option of employing biometrics to quickly authenticate customers.

Fingerprint scanners already installed onto many mobile devices, as well as facial and voice recognition, are all frictionless technology that allows customers to quickly authenticate themselves and proceed with the transaction. Other seamless and simple risk-authentication methods include utilizing QR codes, soft tokens and one-time-passwords.

Evaluate Whether a Device Could be Compromised, Then Take Action

DetectTA can be combined with Detect Safe Browsing to further assess whether fraud is occurring on a device. Detect Safe Browsing protects customers against identity theft and account takeover, even if they are using compromised devices. The state-of-the-art technology blocks online and mobile threats and leverages threat analytics to quickly and decisively act before fraud can occur.

By including Detect Safe Browsing in the DetectTA protocol, financial institutions are aware of a much wider range of variable risks, such as whether a device is jailbroken. For example, if Detect Safe Browsing determines a user is logging in from a risky device, DetectTA can then use this information to flag the device and any transactions performed on it. Once flagged, DetectTA can block all transactions performed on that particular device or require users to verify themselves using the range of authentication options available through DetectID. This route ensures customers are still able to perform safe transactions even if the device is deemed risky.

Collect valuable insight into a whether a device is compromised and make a calculated decision on how to proceed.

By combining Detect Safe Browsing with DetectTA, financial institutions immediately gain more visibility into whether the transaction the device is performing is suspicious or not. This allows DetectTA to use information derived from the device in addition to rules and behavior when determining if a transaction is risky, thus proactively protecting against future attacks.

A Simple Combination Combats Costly Fraud

Combining transaction risk detection with other protection layers does not have to be complicated, nor should it hassle customers with various hoops to jump through. Unlike some competitors, Easy Solutions efficiently implements anomaly detection paired with risk-based authentication and secure browsing so fraud is detected and stopped in the most direct fashion.

To quickly begin reducing fraud, contact Easy Solutions at sales@easysol.net.