Reveal security

Protecting Insurance Companies from Fraud through Applications

Not all abnormal behavior indicates malicious intent, but all fraudulent activity starts with abnormal behavior – how can you catch the early signs?

Overview

Insurance companies work with a wide range of end users, directly with their customers and through intermediaries like agents. Most of the interaction is digital, including capture of personal details, policy terms, payments, and claims settlements. As a result, the companies are exposed to a wide range of information and financial risks. Attackers (Insiders or External) are always on the lookout for ways to exploit these risks.

Insurance companies, like other businesses that provide digital interfaces for accessing information and performing activities, face a fundamental dilemma: How can they provide user-friendly access, while protecting themselves against vulnerability to data exfiltration and financial fraud?

Most insurance companies invest heavily in a wide range of cybersecurity measures to detect and respond to known cyberattacks. However, these measures are expensive, cumbersome, and fail over time. Fraudsters are always advancing and adapting their trade. They find security gaps faster than security teams can protect them. The traditional detection techniques and controls cannot keep up. Business and security experts establish long lists of complex rules, then generate reports to identify suspicious processes, often being overwhelmed with false positives and undertaking lengthy investigations, usually after the damage has been done.

- **Reduce TCO and boost effectiveness** of fraud-detection and compromised business processes
- **Respond quickly and effectively** to malicious users and rogue insiders before the damage occurs
- **Eliminate ineffective, tedious Rules,** and their false positives
- **Spot early signs of abnormal use** at the application and business processes
- **Protect the use of any or all applications** based on analysis of the application's log events

Is there really an effective way to spot and deal with fraud and misuse?

Yes, with User Journey Analytics by RevealSecurity.

User Journeys

While many of an insurance company's digital activities look the same – selecting a customer, viewing relevant details, choosing a desired action, updating information in a specific sequence, and concluding the process by submitting the form – user application journeys can be distinguished and used to identify and prevent fraud and misuse.

Customer

A customer performs actions in the portal in typical flows and subsequently logs off.

Agent

An agent may complete one activity for a client and proceed to either continue with another activity for the same client or initiate a new activity for the next client, maybe performing a different operation like inquiring about the status of claims.

Employee

Company employees interact differently. Their workload is often queued by an internal, workflow-based, task-management system. An employee completes the designated activity and moves on to a similar activity for the next client in the queue.

Three different types of users, each with a different but typical sequence of activities.

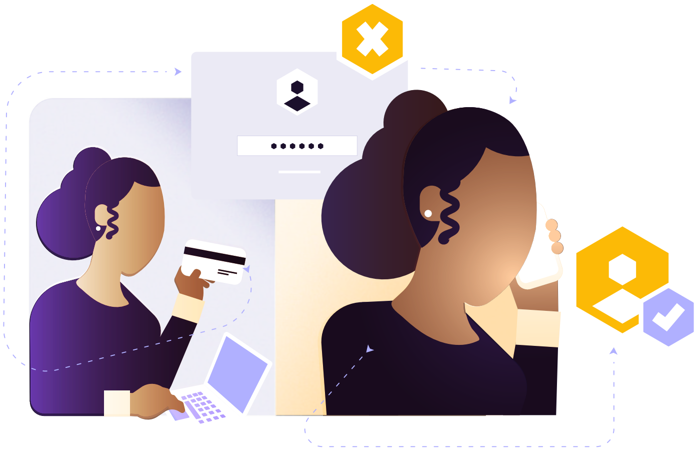
What if there was a way to rapidly learn when a user of any type performs a suspicious action based only on the **pattern** of activity? What if a cybersecurity solution could employ machine learning – no rules necessary – to automatically determine precisely what constitutes a malicious or fraudulent act?

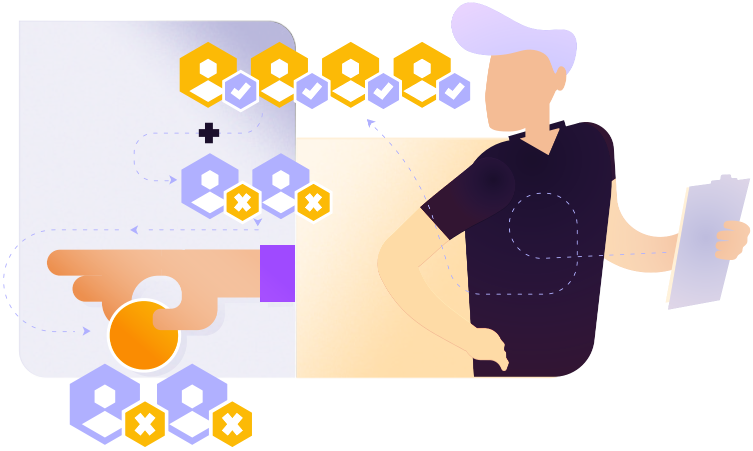
Three Cases that Require Automatic Tracking of User Journeys

Below, are three cases that exemplify the problems of detecting misuse or fraudulent activities, followed by how User Journey Analytics solves each case.

Case 1

A customer updates her payment method via the website, bypassing the insurance company's Call Center. During this simple update, the customer attempts to input her ID number repeatedly, submits a claim form, encounters an error message, then submits the form again, this time with a new payment method.



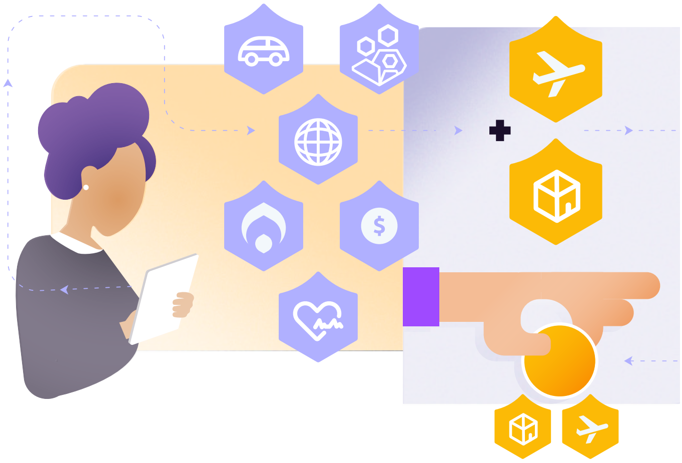


Case 2

An agent modifies a customer's contact information, including changes to the email address and phone number. The agent then updates the details of several more customers within the same session, and then proceeds to request a loan on behalf of these customers.

Case 3

An employee in the Claims Department adds new insurance coverage to a client's health insurance policy. This is an activity usually performed by the Call Center, but the Claims Department employee have the permissions. The same employee, two weeks later, files a claim on behalf of the insured against the new coverage.



Using Traditional Approaches

Companies lack accurate, cost-effective security solutions to quickly detect malicious behavior within and across business applications. Most insurance companies attempt to cover such attack vectors with rules. However, rules are static and detect known patterns only, while attackers are dynamic and constantly discovering new vulnerabilities and leveraging loopholes.

Using traditional fraud-identification approaches, insurance companies will detect such activities only by the resulting damages, which, sometimes are spotted not by the company's own security systems, but by the injured party – often a customer. The company would then rush to address the damage while alerting the security team to strengthen defenses and implement new safeguards (rules) such as:

Traditional Solution to Case 1

Changing the UX to block certain customer activities, for example, by blocking her after three unsuccessful attempts at entering her ID number.

Traditional Solution to Case 2

Updating system reports, to be reviewed manually by experienced security personnel, to include the newly identified suspicious activity.

Traditional Solution to Case 3

Implementing a stricter segregation of duties (SOD) policy and narrowing the activities a single employee can perform.

All these solutions are manual and burn valuable time and resources. Furthermore, they are undertaken in hindsight, after the deed is done.

User Journey Analytics at the Application Layer

Monitoring the application layer for fraudulent and malicious activities is a far more effective approach. It provides the best context to close the loop on fraud with high precision and no need to develop cumbersome correlation rules.

RevealSecurity's TrackerIQ detects signs for fraudulent activities and malicious cases quickly and automatically using its unique User Journey Analytics. Without having to study business processes or create new rules, TrackerIQ monitors the application layer, employing Machine Learning technology to automatically classify and identify possible threats by:

- Raising a flag when the first suspicious action occurs and assisting the company in identifying the malicious intent before actual damage is done.
- Identifying a fraudulent act after-the-fact, to assist the company in investigation and, subsequently, fixing the damage.
- Continuously identifying threats as systems evolve based solely on user activities and patterns without the need to update rules manually.

TrackerIQ monitors the application layer and detects suspicious changes in user journeys by user type. It automatically spots anomalies and abnormal behaviors.

TrackerIQ Value to insurance companies

For insurance companies, business-process compromises can have significant consequences due to the sensitive nature of the data involved and the openness and criticality of the processes. TrackerIQ's revolutionary User Journey Analytics address the deepest concerns and protect companies from:

Claims Fraud

A compromise in business processes can lead to fraudulent claims being approved, resulting in financial losses for the company. Attackers may manipulate or abuse the claims-processing workflow to submit false claims, falsify documentation, or exploit vulnerabilities to receive unauthorized payouts.

Premium Fraud

Compromises in premiums collection processes can enable premium fraud, where individuals or entities manipulate premium payment records or exploit vulnerabilities in payment systems to avoid paying the full amount. This can lead to revenue losses for the insurance company.

Policy Alteration

Business processes related to policy administration can be compromised to alter policy details or coverage terms. Attackers may gain unauthorized access to systems or exploit weaknesses in the process of modifying policy information, such as beneficiaries, coverage limits, and premiums. These alterations can result in improper coverage, unauthorized payouts, and financial losses for the insurer.

Contact us to see TrackerIQ in action: **www.reveal.security**

RevealSecurity

RevealSecurity detects attackers and malicious insiders by monitoring user journeys in SaaS applications. Time and again, reputable research has found that the longer it takes to detect a breach, the greater its damage, yet most detection of breaches within applications is still rule-based, thereby costly and ineffective due to a debilitating high rate of false alerts. Meticulous authentication is never enough, as users who have legitimate application access are still involved in misuse, abuse and malice. Tracking user journeys within SaaS applications does not rely on solution-specific rules, and is instead based on an advanced unsupervised machine learning algorithm to detect abnormal journeys.

Visit us at:
www.reveal.security