User Journey Analytics
Technology Overview

Detecting Malicious Insiders and Imposters by Monitoring User Journeys in Enterprise Applications

RevealSecurity
www.reveal.security
info@reveal.security

Table of Contents

The Need

Why Monitor Application Usage?

Rogue insiders and external attackers pose an increasing threat to enterprise business applications.

Rogue insiders, such as employees and administrators, can abuse their access privileges in enterprise business applications to engage in malicious activities. These insiders capitalize on the fact that their access permissions often are not managed according to the principle of least privilege (PoLP). The principle of least privilege is a practice where users are given only the minimum levels of access necessary for their job functions. In addition, enterprises usually do not apply proactive application layer detection. Enterprises typically only discover misuse, abuse, and/or malicious activities after victims complain, if ever. Subsequently, the investigation requires manually sifting through extensive log data from numerous sources.

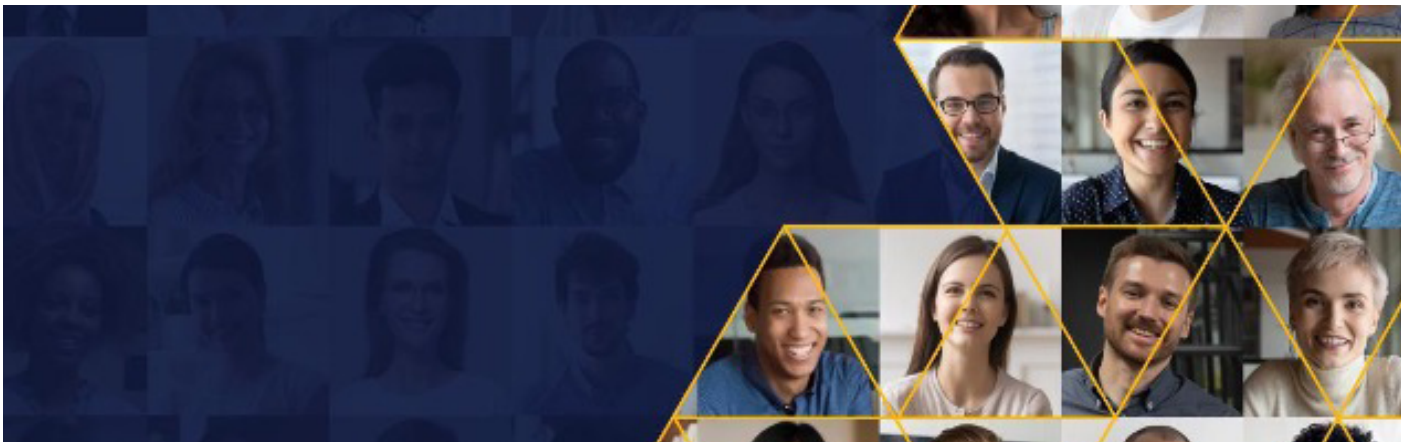
External attackers leverage stolen credentials to impersonate insiders. The continual growth of enterprises' attack surface is due to the rise of internet-accessible applications and remote work.
This expansion provides attackers ample opportunities to steal credentials, impersonate insiders, and abuse enterprise business applications to perform malicious activities.

The combination of rogue insiders and external attackers makes **application layer attacks** a significant pain point for enterprises, especially in core business applications. Consequently, organizations are vulnerable to financial loss and damage from the loss of confidential data, customer trust, reputation, and significant operational disruptions.

Despite the implementation of**preventative measures**, it is evident that threats by authenticated users persist at the business application layer.

Cybersecurity **detection solutions** nowadays focus on malicious activities at the network, device and access layers. Once a user logs in, these solutions cannot monitor the activities of authenticated users who have "legitimate" access.

Therefore, there is a significant need for an application detection solution that closely monitors the actions taken by authenticated users within business applications.



Rule-based Detection Solutions are Inadequate!

Current application-specific detection solutions primarily rely on per-application rules. Rules do not adequately detect malicious application layer activity –

Rules are inaccurate - Resulting in numerous false negatives and false positives.

Creating rules requires understanding the application's business logic - Creating effective rules necessitates in-depth, expert familiarity with each application's unique business logic.

Rules require constant maintenance - Application functionality and business logic are continuously modified and enhanced. Rules are a static solution that cannot address a dynamic problem.

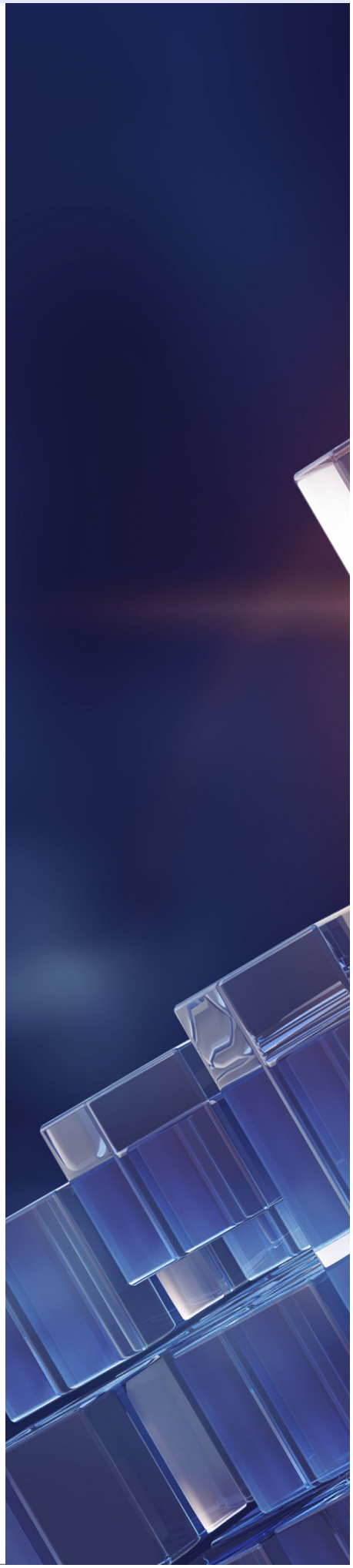
Rules do not scale - Even when perfect rule-based detection is achieved for one application, the process must be repeated from scratch for each business application.

The New Approach – Application Layer User Journey Analytics

Analyzing sequences of events rather than individual ones has proven essential for gaining highly accurate insights into user activity. Cisco's NetFlow, a network detection tool, is an example of this approach. In the context of application threat and fraud detection, this approach calls for examining the **sequences of user actions**, meaning the **user journeys**, within the application.

By contextualizing each user's actions, user journeys facilitate the accurate detection of malicious activities.

User Journey Analytics learns the typical journeys per user and uses these typical journeys to identify abnormal journeys. Abnormal journeys are highly correlated with the activity of imposters, as it is challenging to imitate users' typical journeys in an application. It also accurately detects insiders looking to misuse or abuse an application as they would deviate from the typical user journeys.



What is TrackerIQ?

TrackerIQ is a **novel application layer detection solution** that utilizes machine learning techniques based on the User journey Analytics Approach. Analysis can be conducted per application or across multiple applications to provide greater context and a holistic view.

At the heart of TrackerIQ lies RevealSecurity's **patented clustering engine**, which learns and builds user journeys, enabling the accurate detection of anomalous user journeys. Since each user has multiple activity sequences per application and across applications, TrackerIQ learns the typical user journeys of each user or group of users (cohorts).

TrackerIQ's User Journey Analytics performs the following:

#1 TrackerIQ ingests **application events** using application log records.

#2 TrackerIQ builds user journeys and categorizes the user journeys into groups of similar user journeys, resulting in a set of **typical user journeys** for each user and groups of users (cohorts).

#3 TrackerIQ performs **anomaly detection** using these sets of typical user journeys. An abnormal user journey is a journey that is not similar to other users' typical journeys. Abnormal user journeys are highly correlated with malicious activities.

#4 TrackerIQ computes a risk score for each user journey. This **risk score** combines each user journey's anomaly score (indicating how anomalous it is) and sensitivity score (representing the extent of its business impact) to prioritize detected anomalies.

#5 TrackerIQ generates **alerts** for detected anomalies with tailored recommendations. Additionally, TrackerIQ provides **analysis tools** that enable the understanding of the anomaly for security analysts who want to investigate anomalies further.

#6 TrackerIQ continuously ingests new events, builds journeys, updates the model, detects anomalies, and generates alerts as required.

How Does TrackerIQ Work?

TrackerIQ's components work behind the scenes to identify sensitive user journey anomalies in application audit logs with the utmost accuracy. TrackerIQ's workflow was detailed in the previous section. The following focuses on its components, describing their functionality and how they operate together.

Log Collector

The Log Collector can retrieve application audit log records from almost any log repository, including databases, SIEM, Splunk, files, or APIs (primarily for SaaS applications).

The module analyzes each audit log record to map it to TrackerIQ's normalized internal model, which is focused on the user action (what), the user identifier (who) and the timing (when). In addition, TrackerIQ optionally extracts supplementary data from the log record for analysts to review while assessing an anomaly.

User Journey Builder

TrackerIQ's detection mechanisms rely on user journeys. A user journey represents a user's activities in an application or across multiple applications within a relevant timeframe. The User Journey Builder can create journeys on a per-session basis, daily, and beyond.

TrackerIQ extracts features from the generated user journeys, which enables TrackerIQ to remain agnostic to the meaning of each user action, such as login, search, transfer money, report generation or any other type of activity.

The fact that feature extraction is agnostic enables TrackerIQ to detect abnormal journeys in the audit log of any application or even across applications.

TrackerIQ extracts three key features from each user journey:

#1

The set of actions performed by the user during the user journey.

#2

The order in which these actions were performed during the user journey.

#3

The time difference of these actions during the user journey.

Anomaly Detection Engine

TrackerIQ learns the set of typical user journeys while training the model.

RevealSecurity's patented Clustering Engine groups the user journeys (generated by the User Journey Builder) into groups of similar user journeys. It then creates a single typical user journey from each group of similar user journeys, thus resulting in a set of typical user journeys for each user or group of users (cohorts). These sets of typical user journeys are used for TrackerIQ's anomaly detection.

Note
Anomalous user journeys detected by the Clustering Engine are not included in the set of typical user journeys created by the Clustering Engine.

The detection analysis can:

#1 Compare each individual's user journeys to their own typical journeys.

#2 Compare each individual's user journeys to the typical journeys of their peers in the same organization, department, or role.

If a user journey is similar to a typical one, it is considered typical. If it is not similar to a typical user journey, TrackerIQ can still detect whether it is a new typical user journey by analyzing all the dissimilar user journeys. If it is not a typical user journey, it is classified as anomalous.

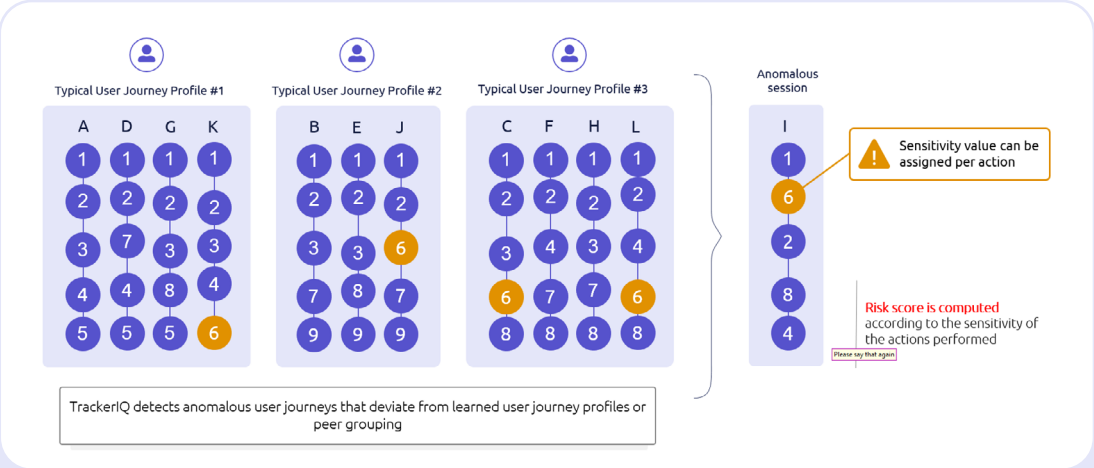
Moreover, TrackerIQ will reclassify an anomalous user journey as a typical one if repeated later. This process creates a new typical user journey to classify subsequent similar user journeys as typical.

Risk Analysis

For each detected anomaly, TrackerIQ computes a risk score which is a combination of its anomaly score (meaning how anomalous it is) and sensitivity score (meaning the extent of its business impact). TrackerIQ assigns a sensitivity score to each user journey that reflects its business impact. The sensitivity score is based on the sensitivity of the actions in this user journey.

Examples of sensitive actions are:

- Using Salesforce to export PII (Personally Identifiable Information).
- Awarding administrator permissions to a financial application.
- Transferring funds to a foreign account.
- Sharing a document link with external recipients.

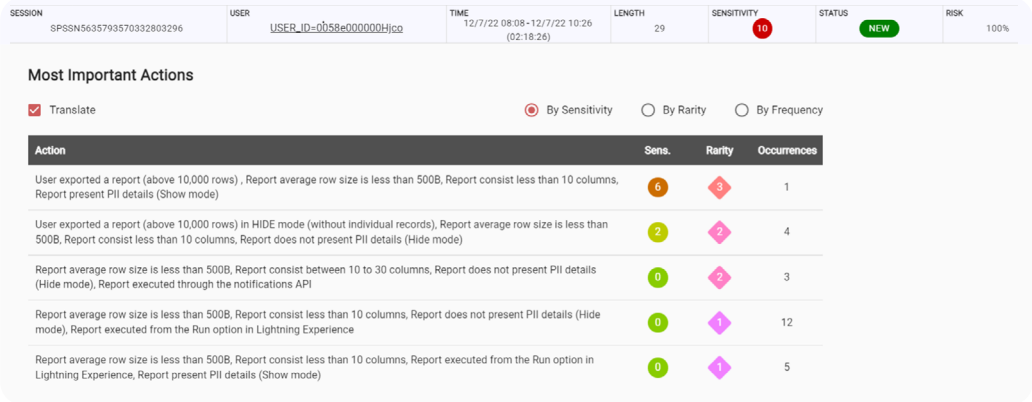


In the example above, action 6 was defined as a sensitive action. Therefore, the system automatically recognizes user journeys K, J, C, L and I as sensitive because they include action 6.
Since user journeys K, J, C and L are similar to typical user journeys, their risk score is zero.
User journey I is classified as an anomaly because it consists of transitions between activities not part of any typical user journey and includes a sensitive action (so it is high risk).

Out-of-the-box TrackerIQ identifies typical sensitive user activities in SaaS applications, which can be customized. For unique business applications, our professional services team will guide you through defining their sensitive user activities.

Investigating Alerts

TrackerIQ delivers realtime alerts to notify your SIEM, Email, Syslog, SMTP or API of abnormal user behavior that includes sensitive actions. A single click on an alert link opens each alert in the TrackerIQ investigation GUI, providing a rich variety of tools and accompanying data to ease anomaly analysis and streamline SOC incident investigation.



TrackerIQ Onboarding

Step #1 Application Audit Log Integration

Audit Log Retrieval Methods

The first step is to provide TrackerIQ access credentials to the application audit log repository. The method for retrieving these audit logs depends on the type of application:

SaaS API
TrackerIQ can retrieve SaaS application audit logs using the SaaS vendor's standard API when the enterprise's license enables such access.

Enterprise Log Repository
If an enterprise is already collecting application audit logs and storing them in its repository (such as Splunk™, Snowflake™, a database, or so on), then TrackerIQ can connect to this repository.

Audit Log Structure

TrackerIQ is intricately familiar with the log structures commonly found in SaaS applications. TrackerIQ provides out-of-the-box integration for these SaaS applications using their APIs, automatically parsing and mapping these audit logs into TrackerIQ's internal structure.

For custom-built enterprise applications, the mapping of audit log structures into TrackerIQ's internal format is defined in TrackerIQ's graphical user interface or with the assistance of our professional services team.

Step #2 Training TrackerIQ Models

TrackerIQ comes with trained User Journey Analytics models for well-known SaaS applications and some COTS applications. SaaS application audit log data is required to tune the model. Each SaaS application has a distinct policy regarding how long historical audit log data is retained and the extent to which logs can be retrieved via API, both of which may depend on your licenses. For example, Microsoft offers multiple licensing options with data retention limits and retrieval interval constraints.

If historical audit logs exist, training the user journey model for SaaS applications (meaning learning all the typical journeys of the applications' users) is quick so you can transition to production within a few days. TrackerIQ can digest this log data over time while training the model if historical audit logs do not exist.

For custom-built applications, TrackerIQ's professional services team will build, train and tune a model for you. Training this type of model requires at least three to twelve months of applications' audit logs to learn all the typical user journeys of the enterprise's application users. Enterprise applications with enough historical audit log data may only take two to four weeks.

Our professional services team will be delighted to respond quickly regarding the timeframe for TrackerIQ deployment allowed by your enterprise application's existing audit logs.

Step #3 Alerting Integration

TrackerIQ provides out-of-the-box integration with leading SIEM and other log repositories to send alerts via email, Syslog or APIs. Configure the credentials of the destination where TrackerIQ will send the alerts.

On-premises deployment is possible for selected customers with special requirements.

About Reveal Security

RevealSecurity monitors privileged users, malicious insiders and imposters to detect anomalies in applications and platforms. 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. RevealSecurity champions ubiquity and accuracy in the application detection market.

Visit us at
www.reveal.security

General inquiries
info@reveal.security

Media
media@reveal.security