TrackerIQ

TrackerIQ Detects Malicious Activities in Enterprise Applications

The most important criteria in a detection solution is accuracy: the number of false positives and number of false negatives, and the goal is of course to minimize these alerts. However, current application detection solutions are based on rules and highly inaccurate.

TrackerIQ's unique analytic approach achieves high accuracy using the context of the activity, i.e. by analyzing a sequence of activities, instead of the activity itself. TrackerIQ does this with user journey analytics in the application.

User Journey Analytics

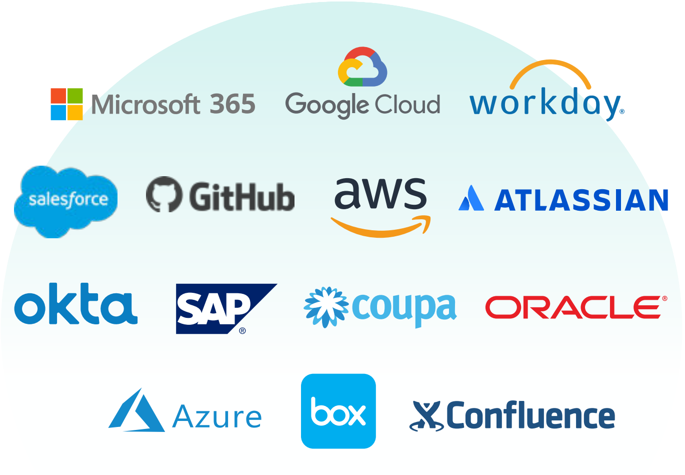
Tracking user journeys enables a new level of application activity analysis, one which is far more accurate and comprehensive than older rule-based and statistical model solutions. A User journey is a sequence of activities the user has performed in an application. Research has proven that each user has typical journeys when they use an application. Learning the typical journey per user (per application), enables us to accurately detect an abnormal journey which isn't similar to the user's typical journeys in the application.

For example when an insider performs a malicious activity, their journey will deviate from their typical journeys and/or the typical journeys of their peer groups. In addition, an accurate way to detect account takeover (i.e. impersonator) is by comparing the impersonator's journey to the real typical user journeys.

Applying Machine Learning to Learn the User Journey Profiles

The challenge is of course how to learn automatically all the typical user journeys in an application (or even cross applications) as each user has many typical journeys (or journey profiles). It is important to emphasize that there is no meaning to an average journey, and to accurately detect the abnormal journey, it is required to learn all the user's typical journeys.

To learn accurately the user journey profiles TrackerIQ reads the log events and generates the user journeys (i.e. the user sessions in the application). Then it groups similar user's journeys together to generate the user's journey profiles. To perform this grouping of journeys accurately RevealSecurity has developed a patent pending clustering engine (since the existing clustering engines in the market don't provide the required accuracy). Based on the groups generated by the clustering engine, TrackerIQ generates user's journey profiles and uses them to detect abnormal journeys. (Note: even if anomaly journeys exist in the log data used for learning they are detected as anomalies by TrackerIQ.) To enhance the detection accuracy a journey is compared both to the user's journey profiles and to the journey profiles of the user's population (both learned automatically by TrackerIQ).



+ any custom built application!

Ubiquitous Detection Solution: The Essence of Activities Makes No Difference to TrackerIQ

As explained above TrackerIQ's detection is based on the user journey characteristics, i.e. the activities performed during a user journey, the order in which they have been performed and the time difference between them. These user journey characteristics are completely indifferent to the essence of specific user activities. Thus, TrackerIQ's detection model can be applied to any application because it is ubiquitous and agnostic to the meaning of an application's activities. This is fundamental to RevealSecurity's detection, as each application has a different set of activities.

The Bottom Line

Application Agnostic

TrackerIQ's detection model is agnostic to the meaning of an application's activities, so that it can be applied to any application and even cross applications.

User Journey Analytics

TrackerIQ analyzes user journeys (i.e. application sessions), not individual activities, and the journey provides a context which is important for accurate detection.

Unmatched Accuracy

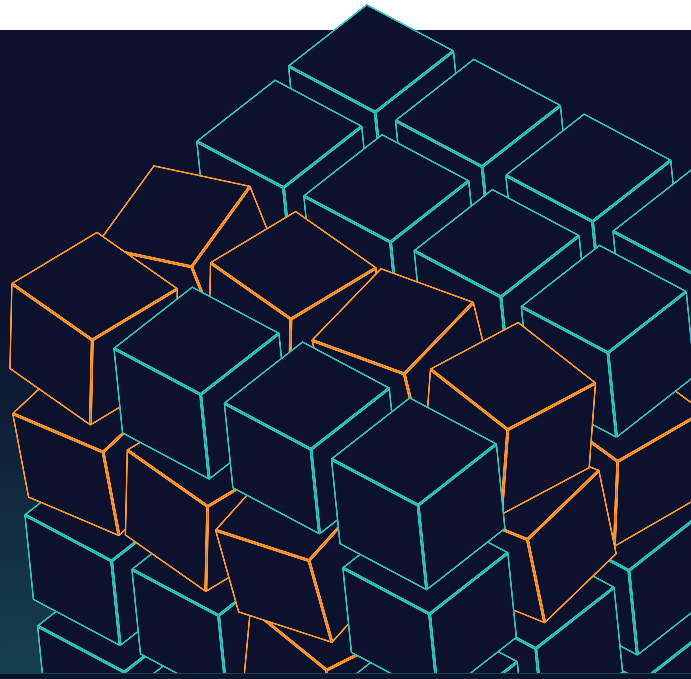
To achieve unprecedented accuracy, TrackerIQ machine learns using its patent pending clustering engine all user journey profiles and use them to detect abnormal user journeys.

No Rules Required

Rule based detection detects only known attack patterns, generates a high number of false alerts, requires constant expensive maintenance, and doesn't scale.

About Reveal Security

RevealSecurity detects malicious insiders and imposters by monitoring user journeys in enterprise applications. RevealSecurity's detection is ubiquitous - applied on any application, and across applications, including SaaS applications, cloud applications and custom-built applications. The detection protects enterprise organizations against cases in which either an authenticated user is taking advantage of their permissions to perform malicious activities, or when an impersonator successfully bypasses authentication mechanisms to pose as a legitimate user. RevealSecurity's tracking of user journeys does not rely on application-specific rules, and is instead powered by innovative user journey analytics, combined with a unique clustering engine to accurately detect abnormal journeys which reflect malicious activities.



TAG CYBER 2022 DISTINGUISHED VENDOR