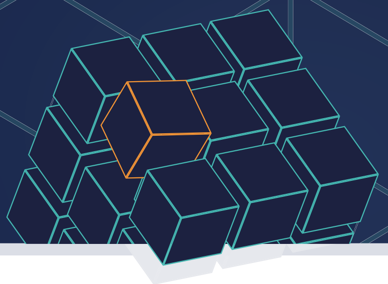
PRODUCT BRIEF

TrackerIQ

Application Detection and Response Based on User Journey Analysis



The Need

Digital transformation has changed businesses across all industries communicating with employees, partners, suppliers, and customers. The future of the enterprise will be more software-enabled - faster, boosting efficiency, and delivering digital experiences. It is evident that despite implementation of cybersecurity measures, internal threats by authenticated users are at the business application layer, and consequently, organizations from all verticals are not only susceptible to financial loss, but also to the damage resulting from loss of confidential data, customer trust, brand reputation, and significant operational disruptions.

Current Detection Solutions

Today's detection solutions are focused on infrastructure, authentication, and data access, neglecting to monitor activities on the application layer, after the user has logged-in. Detection tools are based either on rule engines to detect known attack patterns, or on thresholds set for frequency/volumetric analysis of authentication and data access activities. These detection solutions have limited effectiveness against malicious insiders as they have "legitimate" access credentials and usually work below detection thresholds. Thus, a new detection approach is required to accurately detect threats across enterprise applications (COTS, custom-built and SaaS).

[redacted]

Better Context Means Accurate Detection

It is well known that in order to achieve better detection accuracy, context is needed. The better the context the more accurate the detection is, i.e. lower rate of false positives and false negatives. RevealSecurity has developed a new and innovative detection solution based on user journey analysis. User journeys map out the sequence of activities users make through their digital journey within applications. Sequence-based analytics has been proven to deliver higher accuracy detection and is already common in network and system layers, as in NetFlow and next generation EDR solutions (see diagram below).

	Identify	Protect	Detect	Respond	Recover
Devices	Config Mgt, Vuln Scanner	IAM AV, HIPS	Endpoint Detection & Response	Endpoint Detection & Response EP Forensics	
Applications	SAST, DAST, SW Asset Mgt, Fuzzers	RASP, WAF	Reveal security		
Networks	Netflow, Network Vuln Scanner	Network Security (FW, IPS/IDS)	DDoS Mitigation	DDoS Mitigation NW Forensics	
Data	Data Audit, Discovery, Classification	Encryption, Tokenization, DLP, DRM	Deep Web, Brian Krebs, FBI	DRM	Backup
Users	Phishing Simulation	Phishing & Security Awareness	Insider Threat / Behavioral Analytics		

Degree of Dependency

Technology
Process

Source: Cyber Defense Matrix, Sounil Yu

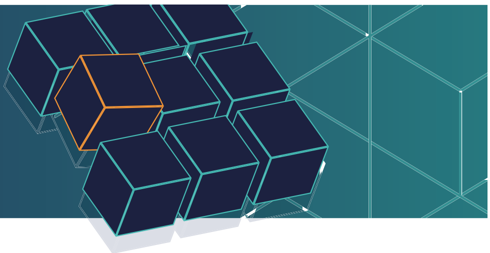
The Challenge of Detecting Malicious Activities in Applications and Platforms

Each application has a unique set of operations and application logs have no common formats or content. This challenge is augmented by the growing number of SaaS application used by enterprises.

Each user has several user journeys per application and across different applications, making the detection of anomalous user journeys (i.e. sequences) increasingly challenging.

TrackerIQ

Application Detection and Response



RevealSecurity has developed a new and innovative ubiquitous user journey model that is applied across any application. This model is based on activities performed by the user, the order in which they were performed, and the time gaps between the activities.

The user journey model is agnostic to the meaning of activities and enables a quick on-boarding process for adding new applications. Since each user has many activity flows per application, TrackerIQ learns for each user (or cohort) his/her user journey profiles.

RevealSecurity's clustering engine machine learns user journeys and build profiles, which enable the accurate detection of anomalous user journeys. TrackerIQ also assigns a risk score to each user journey anomaly based on its activities to prioritize detected anomalies.

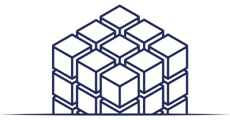
TrackerIQ generates alerts for detected anomalies with tailored recommendations. TrackerIQ also provides analysis tools that enable a swift understanding of the anomaly for security analysts who want to further investigate anomalies.

User Journey Analysis

- Provides context for each operation performed by a user to enable accurate detection
- Anomalies are prioritized based on activity risks

Generalized Activity Flow Model

- Agnostic to the activity meaning
- Applicable across all SaaS, Cloud and custom-built applications
- No need to develop a unique model per application



Application Detection and Response Based on User Journey Analysis

Multiple User Journey Profiles

- TrackerIQ detects anomalies that deviate from the user journey profiles
- Profiles are generated automatically using innovative user journey clustering engine

Operational Efficiency

- Swift on-boarding
- Integrates with log repositories (files, databases, SIEM, Splunk/ELK and Syslog)

About RevealSecurity

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.

TAGCYBER 2022 DISTINGUISHED VENDOR