SOLUTION BRIEF

# TrackerIQ for **Salesforce**

Detecting Malicious Activities in Salesforce Applications

Sept 2022

# Table of **Contents**

## Monitoring **Salesforce**

Insider threats and compromised accounts are a serious and growing risk as organizations modernize IT applications and move from on-prem to SaaS applications. Salesforce has become a critical service for many organizations that rely on it to manage all sales, marketing, services, and other front-office applications via various API integrations. Exposure of these organizations' sensitive data within Salesforce (e.g. PII and customer info) poses significant business risk. In addition, there is the regulatory risk from stricter customer data policies, such as GDPR, CCPA and PCI.  Overall risk is even further amplified by the vast array of services Salesforce offers, which make it one of the largest and most complex attack surfaces of any SaaS application. It is therefore no surprise that Salesforce is a common target for external attackers and insider threats.

Salesforce provides customers with tools to secure information. Nonetheless, even when all security measures have been implemented and verified by an SSPM service, there are still three main threats to be monitored by a detection solution: (a) malicious insiders and especially malicious administrators; (b) malicious API usage by third party applications; and (c) imposters.

## The Three Threats

### Malicious insiders

The first threat is **malicious insiders** who use their rights to access and/or steal data they should not be exposed to, for example:

1. **Departing employees** taking data with them to their next job.
2. **Malicious insiders** leaking data, or compromising data to harm a company's reputation.
3. **Negligent insiders** who don't have bad intentions, but accidentally make a mistake that subjects an organization to security risks.

### Third party applications

The second threat is from **third party applications** that have been granted access to APIs provided by Salesforce. These applications can then use this access either to extract data, or to damage data by performing operations that they should not perform (either intentionally or accidentally).

### Imposter / external attacker

The third threat is an **imposter**, or external attacker, who succeeds to bypass the authentication mechanism (e.g. by receiving valid credentials) and impersonate a legitimate user.

## Current **Inadequate** Solutions

Today there are existing CASB, XDR and MDR solutions that mainly monitor Access to the Salesforce application. These detection solutions are mostly based on rules that detect such activities as access from an atypical geographical location, access at odd hours, or an exfiltration of extremely large volumes of data. These rule-based detection solutions suffer from known deficiencies, mainly a high level of false positives and false negatives.

In addition to the above, because these solutions focus on Access to Salesforce, they have very limited effectiveness against malicious insiders with legitimate access to the application, or against imposters with valid credentials.

To truly detect these malicious activities, we monitor the actual sequence of activities performed by the authenticated users (i.e. the User Journey) within Salesforce and its generated event log data. Salesforce provides several types of log data, such as the Login History, the Audit Trail, the Field History and the most comprehensive of them all, Event-Monitoring (part of Salesforce Shield). In most cases, Salesforce customers don't proactively analyze log data to detect suspicious/malicious activities. Salesforce offers no effective way to sift through all that data and make sense of sequences.

**TrackerIQ** is the only solution in the market which analyzes this log data to effectively monitor user journeys in the Salesforce application, thereby quickly and accurately detecting abnormal journeys indicating malicious behavior.

# TrackerIQ

## TrackerIQ Detects **Anomalous Behavior in Salesforce**

RevealSecurity's **TrackerIQ** is an innovative detection and investigation solution based on user journey analytics. **TrackerIQ** autonomously learns for each user their journeys in Salesforce, creating multiple journey profiles per user that characterize all the user's typical journeys. Based on these learned journeys, **TrackerIQ** then identifies and alerts of any anomalous user journey.

To learn these user journeys, **TrackerIQ** uses unique clustering technology which accurately groups together similar data points, i.e. user sessions. **TrackerIQ** applies clustering to group similar sessions together and then builds a typical user journey from each group of similar sessions. This is a process that runs continuously as new log data becomes available.

Once typical journey profiles are learned for a user, **TrackerIQ** starts checking every new session to see if it is similar to one of the typical user journeys learned for this user. An anomaly is detected when a current user journey is not similar to any of the learned user journey profiles.

To detect scenarios in which users behave differently than their peer group, **TrackerIQ** also compares a user journey against typical user journeys learned for the cohort of users to which the user belongs.

User journey analytics, combined with multiple common user journey profiles learned automatically for each user, provides significantly more accurate results than any other detection technology available in the market today.

## Monitoring Data Usage

Data can be extracted from the Salesforce in various ways, for example:

- Exporting reports
- Downloading documents managed by Salesforce
- Using Salesforce APIs

Most of the time these activities are legitimate, so if we would define rules for such cases, they would generate an alert each time any of these legitimate operations is performed by a user, leading to distracting false positives. Even activities of this sort with unusual parameters, like reports with many lines, may still be normal for certain users. **TrackerIQ** on the other hand, accurately detects only malicious activities with minimal false alerts, by learning typical user journeys in Salesforce and detecting the abnormal user journey. For example, an abnormal user journey related to a data exfiltration operation would trigger an alert.

## Detecting External Attackers

Most detection solutions for Salesforce are focused on access attacks, like brute-force, credential stuffing or concurrent access from multiple geo locations, which can be detected from the basic login / logout logs Salesforce provides. These detection solutions have limited effectiveness when an attacker has somehow acquired legitimate user credentials, and then uses them to log into Salesforce from a legitimate IP. However, **TrackerIQ** monitors both the access as well as the user's Salesforce application usage. Thus, even when an imposter has succeeded to bypass the authentication mechanism, they will be detected because their journey in Salesforce is different than the user's typical journeys.

## Monitoring **Management Activities**

In addition to the detection of abnormal data exfiltration, **TrackerIQ** also detects abnormal management activities, such as:

- ✓ The modification of authentication settings
- ✓ Anomalous sign-in activity and user account status
- ✓ User password changes and resets
- ✓ SSO provider changed or deactivated
- ✓ Resources accessed or altered
- ✓ Mobile devices added, deleted, or wiped

Creating rules for such activities, as certain XDR and MDR vendors have done, generates too many **false alerts**, as most of them are performed legitimately by users and administrators.

# To conclude

**TrackerIQ** provides a comprehensive and accurate detection of insider threats in Salesforce by malicious insiders and administrators, malicious API usage, and imposters.

Consider these unique benefits:

## Out of the Box Detection Solution

- Built-in interface to Salesforce's Event Monitoring
- No installation required
- No need to pre-define rules or statistical models

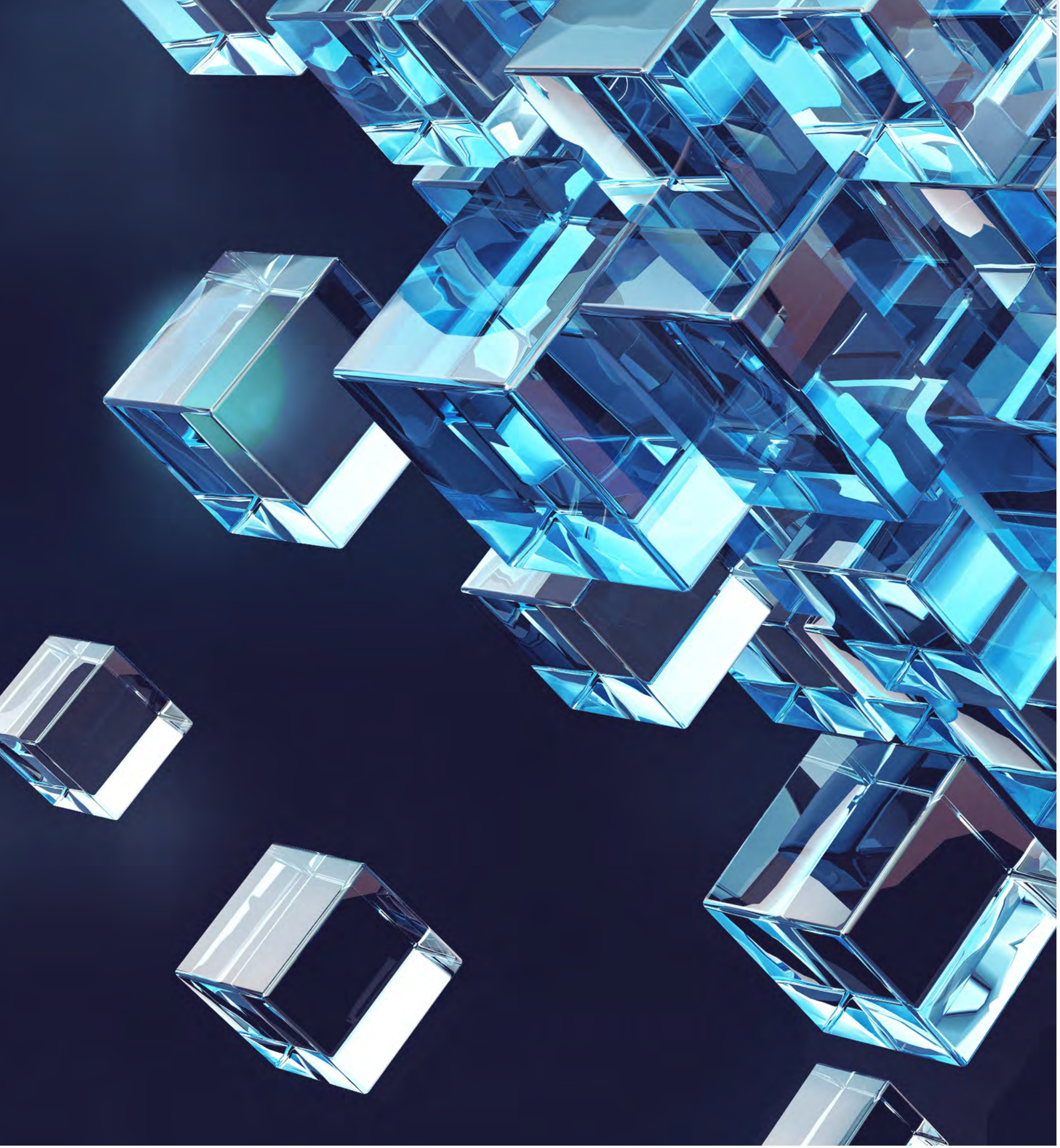
## Highly Accurate Detection

- High accuracy due to the analysis of User Journeys
- High accuracy due to automatic learning of all the common/typical journey profiles per user, or cohort
- A risk score assigned to every identified suspicious journey to allow for prioritized investigation and response

## Investigation Tools

- Swift and comprehensive investigation of alerts with **TrackerIQ**'s visualization tools

**For more information reach out to us at** www.reveal.security



Reveal security

TAG CYBER 2022 DISTINGUISHED VENDOR

## About Reveal Security

RevealSecurity monitors privileged users, malicious insiders and impostors 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