Reveal security

Solution Brief

# Mitigate Third-Party Risks

Detect Suspicious API and Third-Party Behavior in Applications and Cloud with the Reveal Security Platform

## Overview

As organizations become more effective at protecting their infrastructure, threat actors are increasingly shifting their focus to third-party users, integrations, or services to find alternative attack vectors. This presents a significant challenge for security teams since the interconnected nature of modern business ecosystems means that a breach of one organization will often cause collateral damage to many others.

> "31% of risk leaders view **third-party risks** as the greatest threat to their company's ability to drive growth[1]"

## Benefits

- Detect and eliminate unauthorized activity in SaaS, Cloud, and on-premises applications
- Identify and stop API abuse
- Reduce data leakage risks
- Extend compliance efforts to third parties

Reveal Security helps you mitigate third-party risks by extending advanced detection capabilities to the APIs and user accounts your ecosystem partners use to interact with your sensitive applications and data. Using its patented Identity Journey Analytics™ technology, Reveal Security builds detailed profiles of normal third-party behavior and detects potential security compromises or abuse with precision.

## The Cascading Impact of Third-Party Risks

Interconnection of IT infrastructure with trusted third parties is now a fact of life for companies striving to be competitive in the modern marketplace. But for security teams, broad third-party access to sensitive systems and data through both APIs and user accounts presents a complex challenge. After all, even as organizations go to great lengths to secure their own infrastructure, they can be blindsided without warning by the cascading effects of data breaches, malware, and insider threats at affiliated third-party organizations that they have little visibility into or control over.

This can lead to:

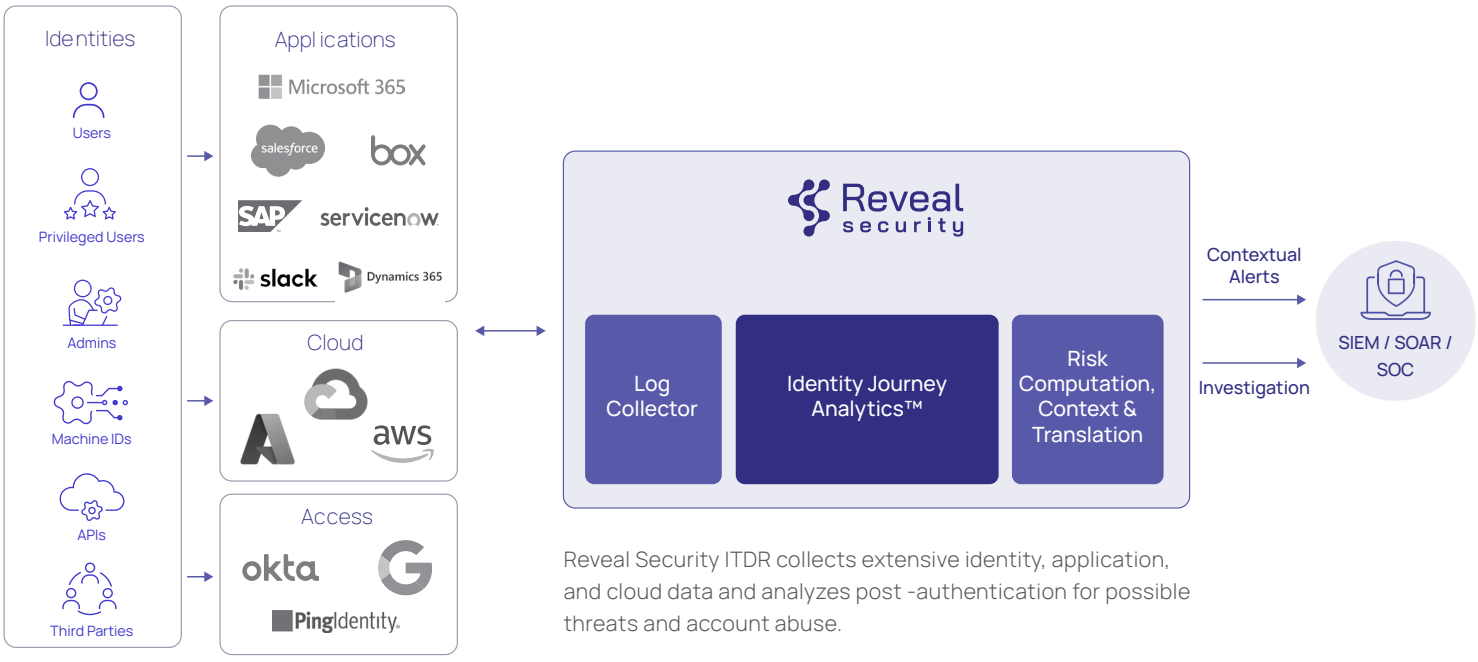
- Data breaches that exploit compromised identities of partners
- Malware or ransomware propagation through interconnected systems
- Risks to regulatory compliance posture due to third-party behavior
- Abuse and unsanctioned use of systems or data by users

Concerns about these third-party risks directly impact organizations' ability to execute against their business objectives. In fact, a survey by PwC revealed that 31 percent of risk leaders view third-party risks as the greatest threat to their company's ability to drive growth.

## Reveal Security Extends Visibility and Control to Third-Party Activity

The Reveal Security platform learns how third parties typically interact with your applications and data and detects anomalies that represent likely threats or abuse.

Reveal Security is a critical complement to both your identity and access management (IAM) approach and threat detection, investigation and response (TDIR) strategies, ensuring that unexpected third-party threats are met with rapid detection, response, and remediation.




Reveal Security ITDR collects extensive identity, application, and cloud data and analyzes post -authentication for possible threats and account abuse.

The platform's patented Identity Journey Analytics™ technology, powered by unsupervised machine learning, builds micro-personas of your internal and third-party users, including API consumers and other machine identities, and learns their normal behavior and typical "journeys," even when they span multiple applications. Ongoing user and application activity is then compared to past journeys by the same or similar human or machine identities to detect abnormal or high-risk behavior by third-party identities. This includes instances when cohorts of API consumers from different third-party relationships interact with APIs in inconsistent, and potentially abusive, ways.

# Business Impact

### Detect breaches that exploit third-party access

Reveal Security spotlights attempts to use compromised third-party identities to access sensitive assets and data or perform other suspicious actions like creating new user accounts or attempting to elevate privileges.

### Prevent account abuse by trusted third parties

Reveal Security also surfaces instances where third-party identities are using applications or accessing data in unsanctioned ways, whether it is unintentional or a case of intentional abuse.

### Spot API abuse by both partners and threat actors

Reveal Security differentiates between legitimate and suspicious API activity, enabling the detection of unintended usage by partners or API vulnerability exploit attempts by threat actors.

### Continuously improve access policies

In addition to accelerating the initial detection and response of third-party threats, Reveal Security provides valuable insights that can inform possible improvements to IAM and other preventative identity controls.

### Strengthen your compliance posture

Extending detection to your third-party relationships will help you demonstrate to regulators and other stakeholders that your security strategy is future-proofed to address a broad spectrum of possible threats.

## About Reveal Security

Reveal Security quickly and accurately detects insider threats and identity-based attacks in and across SaaS, cloud and on-premises applications. The Reveal Security platform is the only solution in the market based on patented Identity Journey Analytics™ technology that uses unsupervised machine learning to learn the usage patterns or typical "journeys" of human and machine identities in applications and uses it to detect anomalies. This approach delivers a superior level of accuracy and context, reduces alert volumes by orders of magnitude, and enables the business to respond quickly before a material breach can occur.

For more information, visit **www.reveal.security**

[1] Source: PwC Pulse Survey, January 27, 2022.