REVEAL

CASE STUDY

Global Investment Firm Bolsters Cloud and SaaS Defense with Identity Behavior-Driven Detection

Gains identity visibility and response across the applications that run the business

> With Reveal Security, my team gained immediate visibility into how our identities interact with our critical applications & sensitive data – without months of engineering effort.

CISO
Global Investment Firm

Key Outcomes

- Protects sensitive data by detecting threats hidden in everyday user activity
- Faster investigation and response to suspicious activity in critical applications
- No manual detection engineering required
- Moved from "static logs to living insight"

Challenge

As a global investment management firm operating in a highly regulated sector, the company manages an extensive portfolio of sensitive data and intellectual property across cloud, SaaS, and custom applications. Nearly all of the company's employees require 'unfettered' access to the sensitive data in order to conduct business and the CISO knew he needed an unobtrusive way to monitor user activity in their mission-critical applications.

Despite a mature security posture – including SSO with MFA, endpoint detection, and a SIEM-based detect-and-respond process – the CISO recognized a critical blind spot:

"We could pull application logs into our SIEM and even write some rules, but that's static visibility. We weren't seeing how identities were actually behaving inside our most important applications."

The firm's small, agile security team needed a solution that would surface meaningful identity anomalies across complex application ecosystems, without requiring constant tuning or custom rule writing. Prior solutions – including UEBA – were too noisy, too static, and too resource-intensive to maintain.

Solution

The firm selected Reveal Security to provide continuous visibility into identity activity across its core SaaS and custom business applications including Google Workspace, Okta, Microsoft 365, and Island Enterprise Browser. The Reveal Platform's ML- and AI-driven identity behavior analytics enabled the security team to automatically learn normal user and service account behavior – detecting anomalies that indicate insider threats, compromised sessions, or negligent actions.

"We were blown away by how quickly Reveal delivered value," said the CISO. "I expected we'd need weeks of detection engineering, but the platform started surfacing meaningful insights right away."

Reveal's approach seamlessly integrated with the firm's existing infrastructure, where the security team manages incidents in a SIEM and via Slack.

RESULTS

Reveal's Impact

Since adopting Reveal Security, the firm has significantly improved its ability to detect and respond to identity-driven threats across critical application systems. Reveal gives them a unified view of identity activity, reducing the burden on an already lean security team.

Accelerated threat detection: Reveal identified anomalous activity from a legitimate executive account that had been compromised after a device theft — allowing the security team to revoke access and contain the incident before data exposure occurred.

Compensating control for data sharing and data access: Reveal detected instances of employees unknowingly "oversharing" highly sensitive data, as well as data access policy violations.

Reduced workload and noise: Analysts no longer spend time writing or maintaining static rules. Reveal continuously learns from user behavior, surfacing only high-fidelity anomalies that warrant investigation.

Enhanced analyst effectiveness: "Even our newest analyst can easily understand what she's looking at and know exactly what actions to take," noted the CISO.

Trusted partnership: The security leader highlighted Reveal's transparency and collaboration throughout the deployment: **"The Reveal team has been incredibly open with us – explaining how models are built and showing us exactly where the insights come from. That level of trust is rare."**

About The Customer

This global investment management firm oversees billions in assets across technology and financial markets. The firm maintains a mature yet lean cybersecurity program designed to protect sensitive financial and operational data across cloud, SaaS, and custom applications.

About Reveal Security

Reveal Security is the preemptive identity security company helping enterprises stop identity-based threats before they cause harm. By applying ML- and AI-powered identity behavior analytics across enterprise applications, Reveal brings visibility, precision, and automation to identity security.
Learn more: www.reveal.security

Discover how Reveal Security protects SaaS and cloud applications from identity-based attacks – including insider threats, stolen credential attacks, and API abuse.

Learn more at www.reveal.security