REVEAL

How to Protect Your Identities and Applications from Becoming the Next Attack Vector

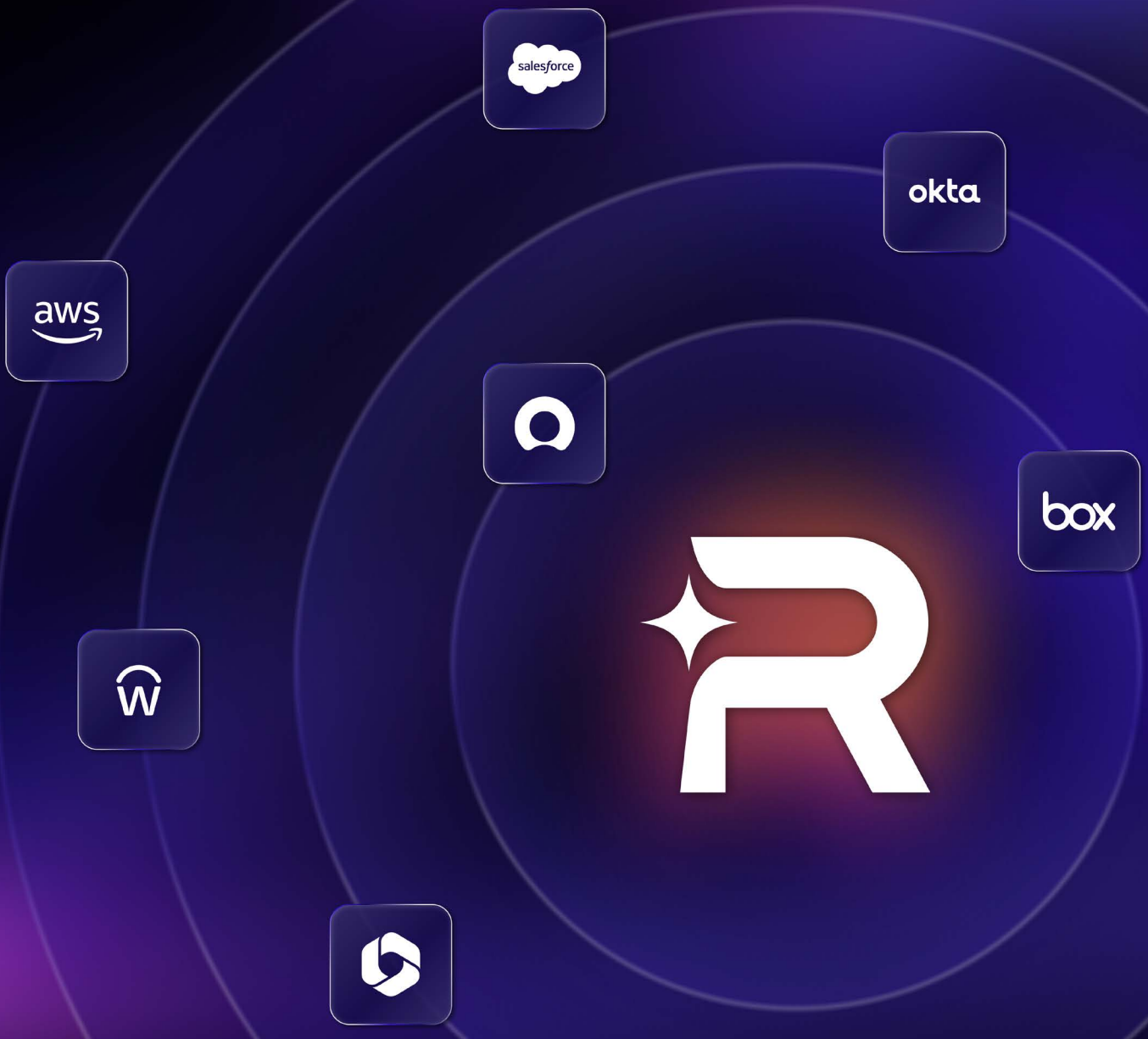
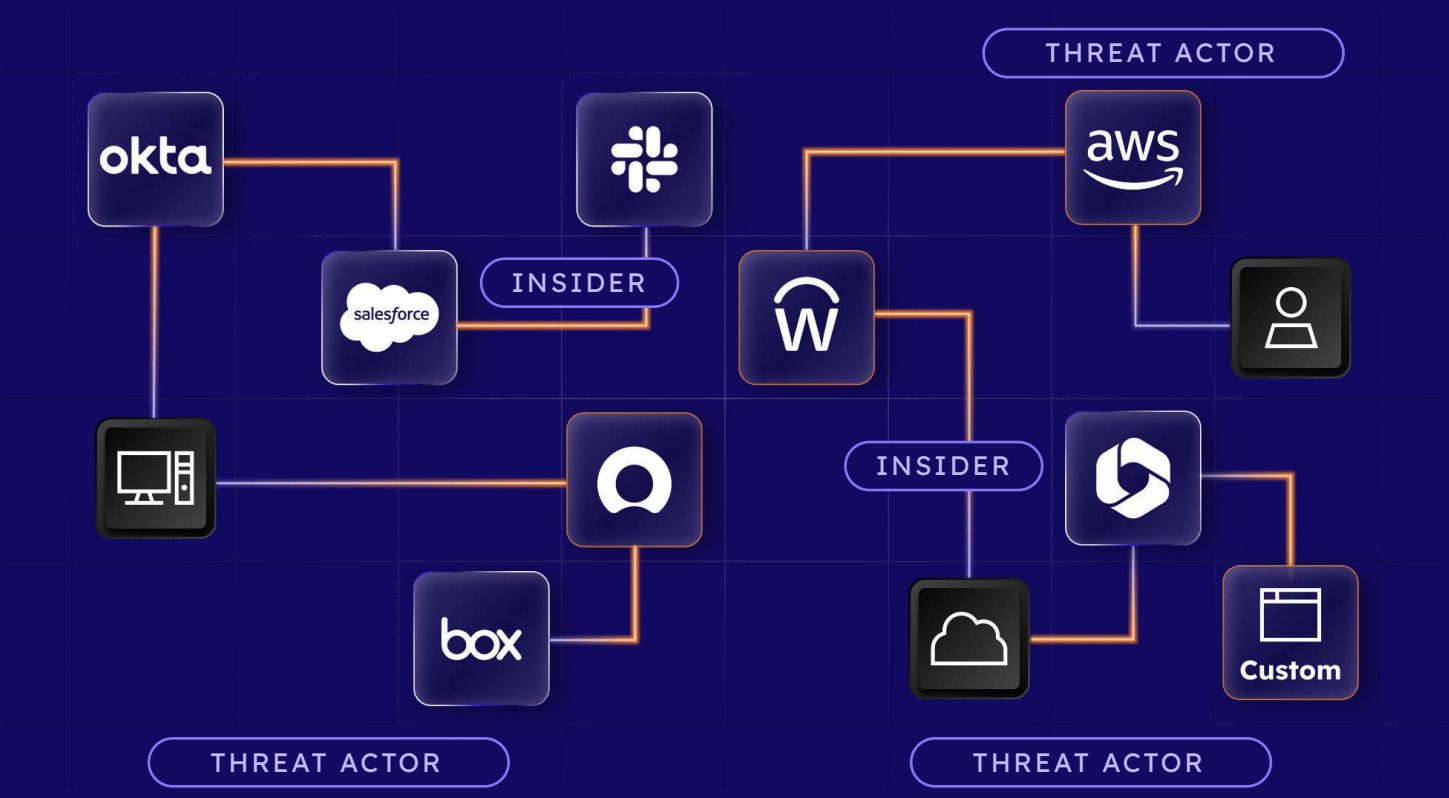


Table of Contents

Protect Your Identities and SaaS Ecosystem from Becoming the Next Attack Vector

Attackers are using trusted identities, authenticated at the edge, to infiltrate enterprise applications and clouds. They conduct reconnaissance, access critical business systems, manipulate administrative operations, and exfiltrate data – all without detection by conventional cybersecurity tools. Protecting your SaaS ecosystem from exploited identities requires visibility into the behavior, activity, and intent of every identity — both at authentication and beyond the login.



Enterprise Applications are under attack and Identity is the #1 Attack Vector

02 The Challenge

A Threat Landscape Defined by Identity Exploits in Critical Applications

Stolen Credentials Are the New Skeleton Key

Malicious intent moves faster than the speed of traditional security solutions – especially when attackers weaponize AI, steal valid credentials, and gain unrestricted access into your enterprise. In recent attacks, SaaS applications, integrated software platforms, and cloud services have been successfully compromised using valid, exploited credentials.

88%

of the breaches involve the use of stolen credentials, which sometimes serve as both the first and only action, while other times, it is just one piece of a larger attack chain.

Verizon DBIR 2025

Threat groups play the long game with APTs (Advanced Persistent Threats) and impersonate employees to trick help desks into giving them valid credentials to log into applications. This is one of the many ways attackers can bypass MFA (Multi Factor Authentication) and perimeter defenses for unfettered access into your environment.

Using compromised credentials against SaaS ecosystems has become the prevalent new attack vector. The attacks are silent, scalable, and difficult to detect. AI is serving as an accelerant for adversaries, speeding up and broadening the reach of threat actors through successful phishing schemes, Ransomware-as-a-Service, vulnerability exploitation, and account takeovers.

Identity Breaches in SaaS

Salesforce
March 2025
A cascading breach that began when attackers accessed GitHub and harvested sensitive credentials to compromise Drift data and infrastructure. With stolen OAuth tokens from Drift, attackers connected through Salesforce to customer instances to export high-value data. According to reports, other high value access paths – AWS keys, VPN credentials, Snowflake credentials – have surfaced from this breach.

Workday
August 2025
An authenticated threat actor incident where attackers used stolen credentials to access and export sensitive customer data from the HR giant.

Snowflake
June 2024
UNC5537, a financially motivated threat group, used stolen credentials to break into 169 Snowflake customer instances to exfiltrate data and demand ransom. Stolen data was advertised for sale on cybercrime forums.

Scattered Spider

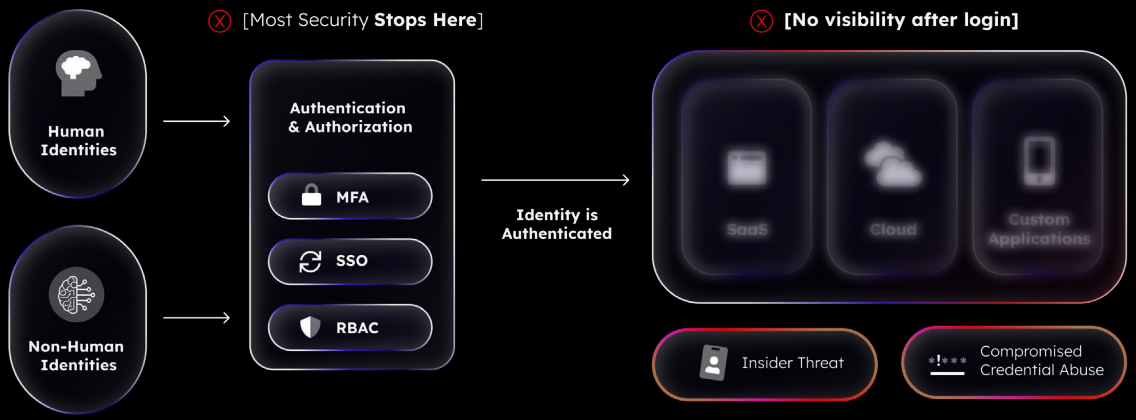
Is one such crime group, infamous (and highly efficient) for propagating large-scale identity breaches into corporations for data extortion. Their MO is to gain full access to networks and systems through social engineering tactics - impersonating employees and triggering MFA fatigue to gain authorization and installing remote tools. Scattered Spider is a serious threat to enterprise security and is responsible for identity-based attacks, data exfiltration, and ransomware deployment across many industries worldwide. Once an attacker (like Scattered Spider) is authenticated using legitimate credentials, they essentially become invisible to your security stack. The outside adversary, using insider permissions, can move freely throughout your hybrid enterprise and attack your SaaS, custom apps, and cloud services.

03 Why Existing Tools Fall Short

Your Security Tools Weren't Built for This

Most IAM tools are built for prevention at the point of access and in the case of ITDR: detection on the identity infrastructure itself. These tools are usually overseen by the IT team or the Identity team. Standard identity tools like MFA (Multi-Factor Authentication) and SSO (Single Sign-On) tools are important, but these controls are isolated identity components and lack post-authentication visibility into an identity's activity across SaaS, clouds, and custom applications. Detection tooling, which is under the purview of the security team and the SOC, is typically rules based, noisy, and focused on the network and perimeter. For example, while endpoint security is a critical first line of defense against targeted attacks and known bads, these tools focus outward. They are of little to no help once an attacker using legitimate credentials logs into the critical SaaS platforms and cloud services that hold your sensitive data and underpin your business. Recent breaches exposing sensitive data and credentials highlights the need for organizations to add visibility and security beyond authenticated logins. Enterprises need a solution that can contextualize behavior analytics within their ecosystem - at scale - and respond to threats in near real time.

The SOC needs a stronger identity signal, and the identity team needs more visibility and intelligence beyond the login.



Attackers log in and defenders lose visibility and ability to detect and contain

Beyond the Login: Monitoring Identity Behaviors

Considering growing identity-based attacks, enterprises need a security solution that runs in the background, ingesting audit logs (without slowing your operations or business processes) to understand the behavior and intent of every identity. EVERY user – human, machine, or bot - post authentication.

> "CISOs are re-architecting their security programs for a post-perimeter, cloud-first world. The shift is massive and it's happening fast."
>
> **Kevin Hanes, CEO,** Reveal Security

The gap between identity authentication and identity behavior must be filled with a simple-to-use, post-authentication identity behavior monitoring solution. With the growing threat of stolen credentials, identity behavior monitoring and analytics are key to getting ahead of malicious activity and stopping threats left of boom.

Anomalous behavior detection is just as important as threat prevention. While your SIEM (Security Information and Event Management) is responsible for gathering and synthesizing telemetry data from security tools to detect, respond to, and manage threats, it is not a standalone solution to the problem of identity attacks. The SIEM triggers alerts – many, many alerts - so many that teams waste a significant amount of time chasing false positives. Or worse: **ignoring the alerts altogether.**

SOC teams need an additional layer of defense that works alongside existing security infrastructure to trigger high-fidelity insights with SaaS-specific identity context and identity attribution. SOC teams need to know the who, why, where, what, and when of all identity activity within your ecosystem.

The new security imperative must be identity-aware, behavior-driven visibility across SaaS and custom applications and cloud infrastructure. **Behavior doesn't lie, making behavior and identity analytics a core security strategy.**

Who Needs to Protect Their Applications?

Any organization in a regulated industry that uses a multi-stack cloud environment, SaaS applications for critical business operations, and understands that highly sensitive financial, technology, or healthcare data needs top-tier protection.

Any organization that needs visibility into identity behavior post-authentication.

Any organization using strong identity foundations but lack post-authentication behavior analytics.

Any organization using AI and ML to facilitate business processes.

Any organization with lean Security teams that are burning cycles responding to false positive alerts.

Any organization with unexamined audit logs.

Enterprise organizations feeling vulnerable after recent high-severity, identity-based attacks need to layer post-authentication identity monitoring into their security stack.

05 Introducing Reveal Security

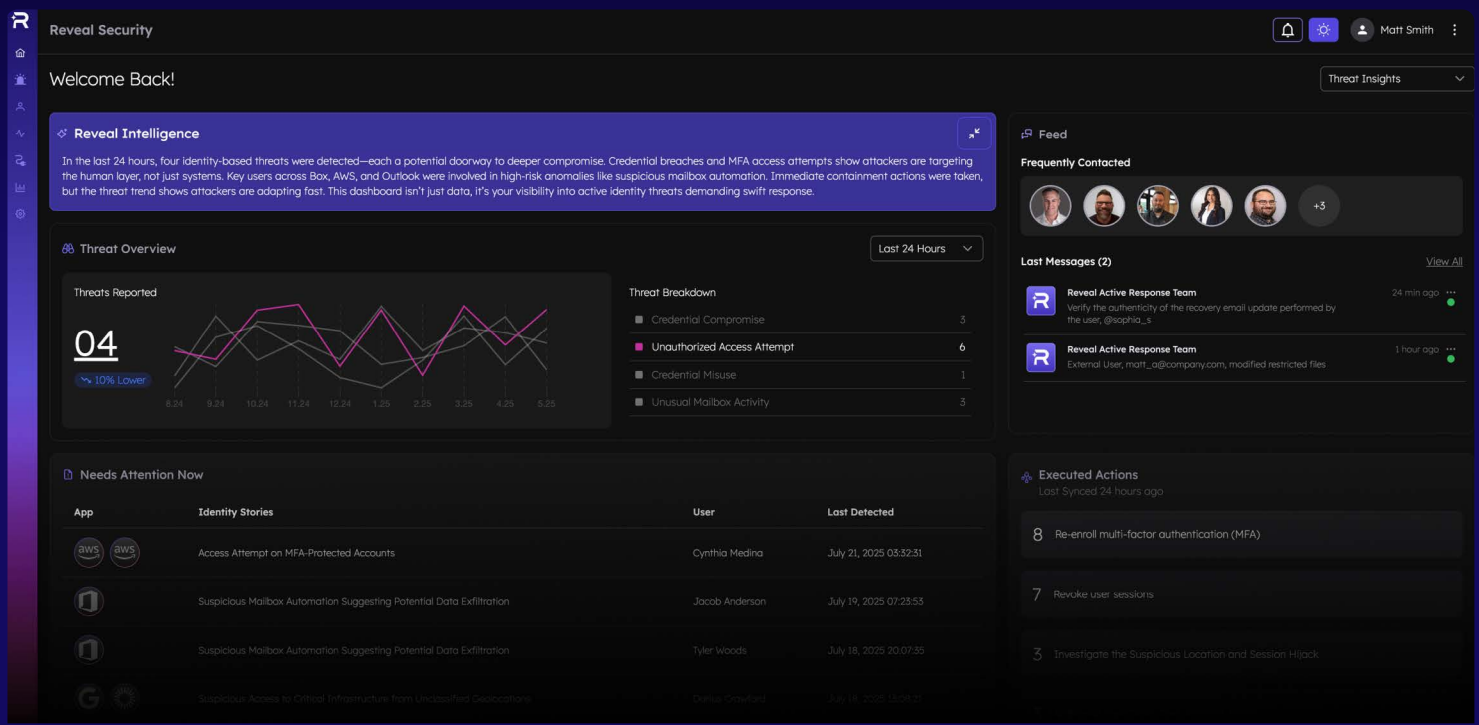
Preemptive Identity Security for Critical Applications

Reveal's preeemptive cybersecurity platform offers unparalleled visibility into post-authentication identity behavior across enterprise applications and cloud ecosystems.

With Reveal's Preemptive Identity Security, organizations now have a way to defend against identity intrusions, credential abuse and insider threats.

Using rich data from the continuous monitoring of human and machine identities, application threat modeling, ML, and AI, the Reveal platform correlates identity behavior across SaaS, cloud, and custom apps for complete identity stories and reduced noise.

The platform understands who or what is behind every action and why. This attribution and predictive intelligence is what unlocks preemptive response. With this context, automated one-shot responses can be set to instantly suspend users, revoke sessions or trigger other policy-based actions to preempt threats.



How Reveal Works

Preemptive Defense, Powered by Identity Attribution & Intelligence

STEP 1

Attribution determines whether an identity is human, AI, or rogue automation

STEP 3

Findings are enriched with context to automate the right response

STEP 2

Predictive intelligence reveals misuse vs. mistake

> “Without preemptive cybersecurity, no organization is safe. The increasing speed, sophistication and scope of an AI-enabled threats is destroying the reliability of existing stand-alone detection and response (DR) cybersecurity methods.”

Gartner, May 2025

Reveal connects to existing SIEMs, ticketing systems, and Slack for fast, seamless integration into security workflows to protect against identity-based attacks and insider threats without burdening SOC teams with alerts.

The Reveal Platform uses audit logs as its source of truth, ingesting and analyzing those logs to detect anomalies and threats inside authenticated sessions. Reveal protects your SaaS ecosystem from the inside out by detecting complex, suspicious identity activity using behavior monitoring, identity attribution and predictive intelligence.

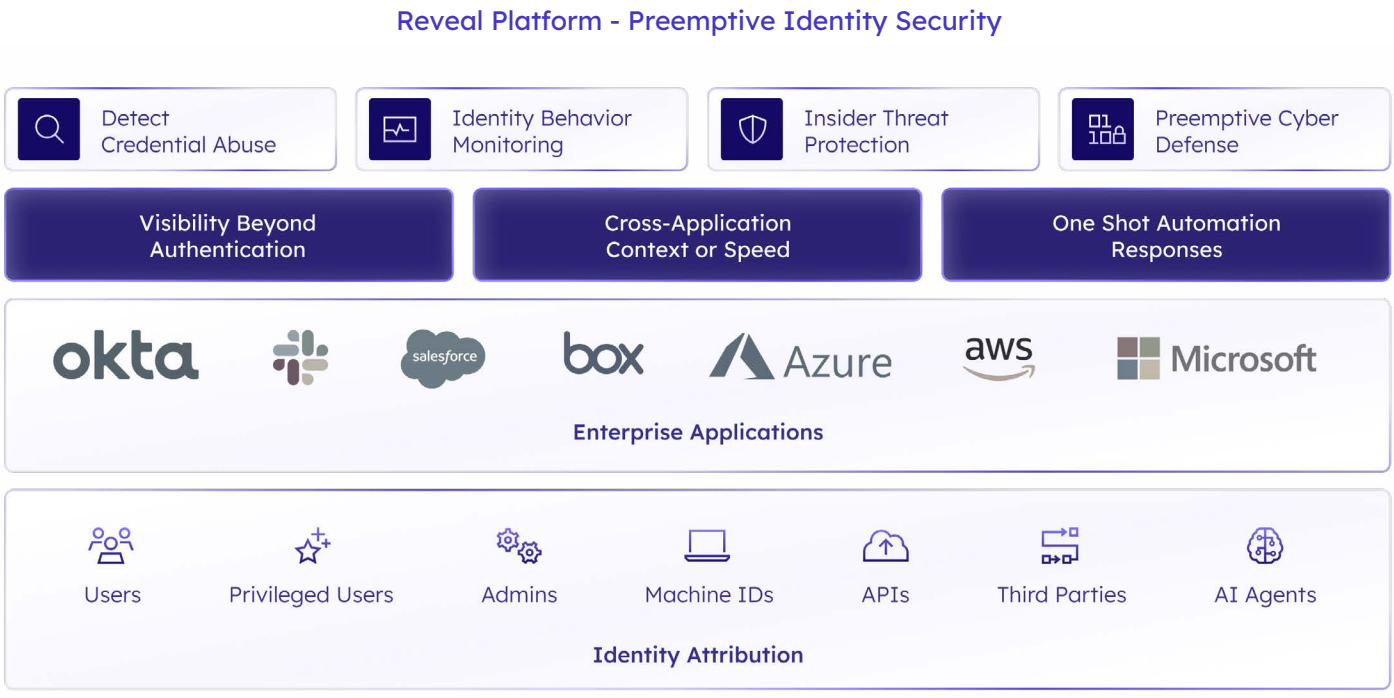
06 How to Get Started

Don’t Wait Until Your Identities or SaaS Becomes the Next Breach Headline

Behind every identity is a story worth telling. Get ahead of threat actors that infiltrate your ecosystem using stolen credentials with the Reveal Preemptive Identity Security platform. Because once inside authenticated sessions, adversaries are nearly impossible to discover with traditional identity tools. The news is full of breach headlines that link back to the preferred methods of threat actors (watch out for 16 billion passwords exposed in record-breaking data breach) – so be prepared.

Reveal is different from traditional identity tools because it brings deep visibility to post-authentication identities with precise intent analysis, attribution, behavior context, and automation to preempt identity threats in enterprise applications.

Reveal is agentless and can support any identity provider, application, or cloud that has audit logs. It is easy to implement and works with your existing security stack to reduce analyst workloads and detect credential abuse left of boom.



Why choose the Reveal Preemptive Identity Security platform?

Easy way to bring the identity signal to your SOC

- Bridge the gap between your identity, SOC teams, and tech

Easy to deploy

- Agentless, frictionless deployment
- Seamless integration into SIEM, Slack, and other SOC tools
- Implementation in days, not weeks or months

Easy to use

- No need to write detection rules or understand application logging
- High signal detection means very low alert volume… no alert fatigue
- Intuitive dashboard that delivers insights to L1 analysts, threat hunters, and CISOs

Easy to justify

- Affordable
- No new operational overhead needed
- Rapid time to value
- Enables security teams and/or automation to respond with confidence

Schedule a demo today and get ahead of the breach

SCHEDULE A DEMO TODAY

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 at www.reveal.security.

REVEAL