Reveal security

Solution Brief

Insiders are an Attack Vector for External Threat Actors

Detect and Stop Them with the Reveal Security Platform

The term insider threats can be deceiving. While it often brings to mind malicious employees or partners, the reality is that most insider threats are attempts by external threat actors to exploit otherwise trustworthy members of your team. These tactics have played a central role in some of the highest-profile security breaches of the last several years. Yet, only about 10 percent of organizations have a formal effort to detect and stop insider threats.[1]

The Reveal Security Platform helps you detect and stop insider threats through a new and more effective approach that focuses on the primary target of attackers: identities operating in your applications and cloud. Reveal Security uses sophisticated ML-based behavioral analytics to learn typical user and identity journeys in your applications and cloud services and detects anomalous journeys that usually indicate insider threat or other malicious activity

Benefits

- Accelerate time to detection for insider threats.
- Detect novel threats that traditional security approaches miss.
- Reduce false positive alerts and other noise.
- Improve team efficiency and communication.

Why Insiders are a Target of External Attackers

While malicious insiders do exist, some of the most devastating examples of insider threats aren't international acts by insiders. More commonly, they are the result of:

- Theft and abuse of user credentials.
- Errors or carelessness that lead to negative consequences.
- Social engineering attacks that cause insiders to unwittingly assist a threat actor.

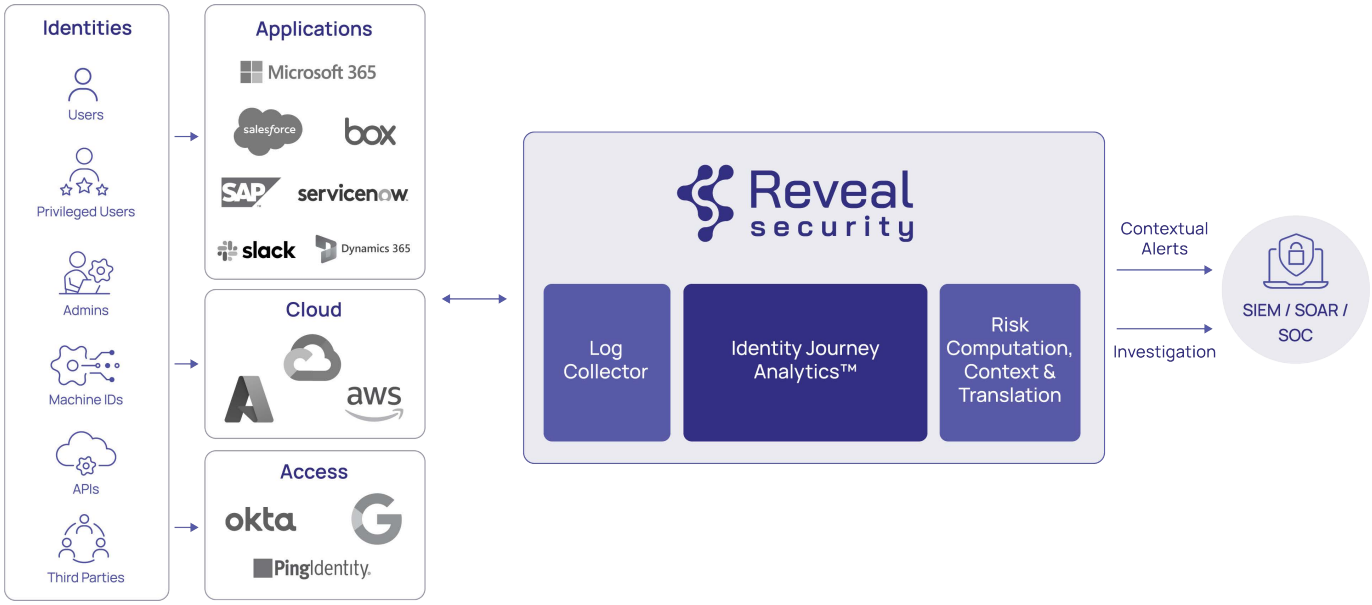
These types of threats play an ever-increasing role in successful security breaches. For example, the exploitation of legitimate user credentials played a role in an estimated 86 percent of security breaches[2]

One of the primary reasons for this is that most traditional security approaches trust authenticated users implicitly and aren't capable of distinguishing between normal and unsanctioned activity in applications and cloud services.

Reveal Security Learns Typical Identity Behavior in Applications and Detects Anomalies

Reveal Security uses sophisticated ML-based behavioral analytics to learn how users interact with applications (SaaS, Cloud, On-Premises) and delivers detailed alerts when suspicious behavior is detected. Reveal Security operates out-of-band using log data integrations, so it's completely non-disruptive to your critical business applications.

1 "Predicts 2023: Cybersecurity Focuses on the Human Deal," Gartner Inc.
2 "2023 Data Breach Investigations Report," Verizon.



Reveal Security's application-agnostic technology ingests the logs from any application and turns them into a normalized format for analysis. From there, the solution's patented **Identity Journey Analytics™**, based on unsupervised machine learning, learns the typical behaviors and 'journeys' of your users and identities. This includes identity journeys that span multiple applications. New identity journeys are compared to past journeys by the same individual and comparable peers, and contextual alerts are generated when high-risk anomalies are detected.

Reveal Security Business Impact

Accelerate time to detection for insider threats

Reveal Security reduces the time to detection for insider threats from months to a few hours, reducing the likelihood that they will escalate into a major incident that causes financial damages or business disruption.

Detect novel threats that traditional security approaches miss

Since Reveal Security does not require manual rule creation and works across all of your applications (SaaS, Cloud, On-Premises), it makes it easy for security teams to expand their threat detection coverage.

Reduce false positive alerts and other noise

Because Reveal Security has full application context and detects statistical anomalies rather than matches to imperfect, manually created rules, hundreds of alerts of ambiguous validity and criticality are reduced to 1 to 3 accurate, high-fidelity alerts per week.

Improve team efficiency and communication

Reveal Security's ability to learn identity behaviors and journeys and provide detailed insights into threats at the application layer reduces the security team's dependence on application owners, IAM teams and other subject matter experts.

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**