Reveal security

Solution Brief

Detect and Respond to Account Takeover in Applications

Detect Stolen Credential Usage Quickly in SaaS, Cloud and On-Premises Applications with the Reveal Security Platform

Overview

Now that many organizations have enhanced security measures protecting their critical applications and cloud platforms, threat actors increasingly find that hijacking the credentials of a user or entity is a faster and easier path to high-value assets than traditional attack methods. And preventative controls like identity and access management (IAM) and privileged access management (PAM), while beneficial, aren't enough to address the problem on their own.

> “**86%** of web application breaches involve the use of **stolen credentials**[1]”

Reveal Security helps you detect anomalous activity by authenticated identities, accelerating detection and remediation of account takeover attacks in and across applications - SaaS, cloud, and on-premises. Using patented Identity Journey Analytics™ technology, the Reveal Security platform builds detailed micro-personas of all of your human and non-human identities, establishes application-specific and cross-application profiles of normal behavior, and detects anomalies that indicate credential abuse.

Benefits

- Detect account takeover attacks in applications with speed and accuracy
- Reduce exposure to data breaches and fraud
- Identify weaknesses in IAM and PAM policies
- Minimize financial, reputational, and compliance harm

Identity Threats Don't End at Authentication

While preventative measures like IAM and PAM play an important role in governing access, it's been proven time and again that even sophisticated and well-implemented identity controls are not infallible. Ever-resourceful threat actors continue to find ways to circumvent IAM and elevate privileges. And when they succeed, insufficient threat detection capabilities in the application environment allow them to advance their attack efforts undetected for an average of 328 days[2].

[1] Source: “2023 Data Breach Investigations Report,” Verizon, June 6, 2023.
[2] Source: “Cost of a Data Breach Report, 2023,” IBM, July 24, 2023.

The impact of these lengthy dwell times can be devastating, including:

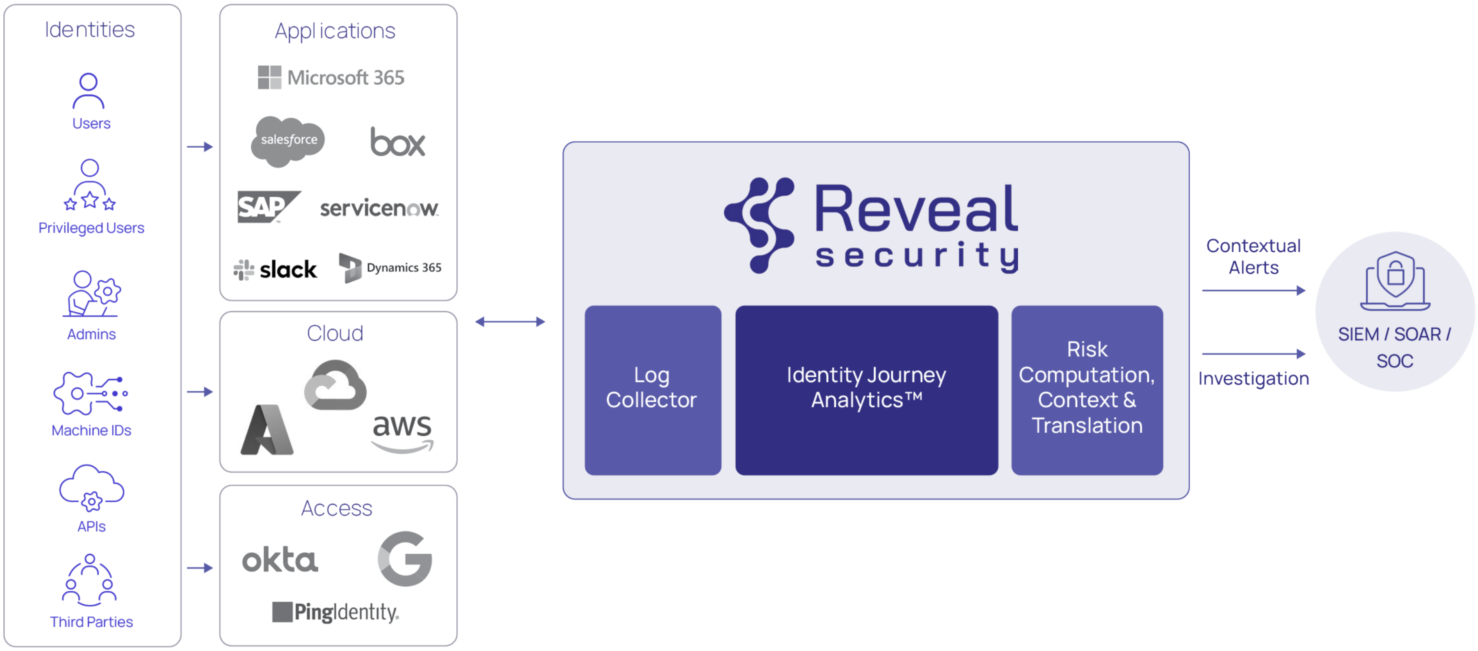
- Financial and reputational loss due to data breaches or fraud.
- Disruption of critical business processes.
- Weakening of security measures from within.
- Negative legal and compliance outcomes.

Many of the most devastating security incidents of the last several years originated with account takeover attacks, including several high-profile examples where prominent IAM providers like Okta[3] and Microsoft[4] were themselves compromised. This is increasing the urgency for identity aware threat detection and response capabilities that extend beyond the point of authentication to detect ongoing account abuse in and across applications.

Reveal Security Detects Anomalous Behavior of Authenticated Identities

The Reveal Security platform models the normal interactions between identities, applications, and cloud services and generates information-rich alerts when suspected account takeovers are detected.

Reveal Security complements preventative identity security measures like IAM and PAM by performing continuous monitoring of identities in and across applications after the point of authentication. And since it uses modern techniques like unsupervised machine learning and anomaly detection instead of rules, it can detect novel threats that legacy approaches miss while delivering very few alerts to the SOC.



Reveal Security's patented Identity Journey Analytics™ uses unsupervised machine learning to learn the usage patterns or typical "journeys" of human and machine identities in and across applications and uses it to accurately detect anomalies. This is the most effective way to quickly detect and mitigate account takeover attacks operating in SaaS, cloud and on-premises applications.

[3] Source: "Hackers Stole Access Tokens from Okta's Support Unit," Krebs on Security, October 20, 2023.
[4] Source: "Microsoft Falls Victim to Russia-Backed 'Midnight Blizzard' Cyberattack," Dark Reading, January 22, 2024.

Business Impact

Reduce time-to-detection for account takeover attacks

Reveal Security takes mean-time-to-detection (MTTD) and mean-time to respond (MTTR) for account takeover attacks from months to hours by combining a more effective, application-aware detection model with a continuous monitoring approach.

Minimize exposure to data breaches and fraud

Rapid detection of account takeovers empowers security teams to respond and recover before threat actors can escalate their attack, significantly reducing the likelihood of business harm.

Ensure compliance with emerging regulations and standards

Continuous monitoring for account takeover supports compliance with emerging regulations and standards, including the EU Digital Operational Resilience Act (DORA), NIST Cybersecurity Framework (CSF) 2.0, and CISA's Zero Trust Maturity Model.

Continuously improve IAM and PAM policies

In addition to enabling faster response, detection of identity-based attacks exposes weaknesses in IAM and PAM policies that can be used to improve these controls continuously.

Enhance security team efficiency and effectiveness

Application-aware anomaly detection provides superior alert accuracy and supporting context-reducing noise in the SOC, and enables detection of application-specific threats without requiring security teams to have specialized application expertise.

About Reveal Security

Reveal Security quickly and accurately detects threats post-authentication in and across SaaS applications and cloud services. The Reveal Security platform is the only solution in the market based on patented Journey Analytics™ technology that uses unsupervised machine learning to continuously analyze the activity of human and machine identities in applications and 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