Reveal security

Solution Brief

Reveal Security for Okta

Monitor Okta Users to Quickly and Accurately Detect Account Takeover and Insider Threats

okta

Benefits

- Identify the impersonation of Okta administrator accounts
- Uncover anomalous user behavior across business applications
- Detect compromised identities before a breach occurs
- Reduce MTTD for threats that bypass Okta preventative controls

Overview

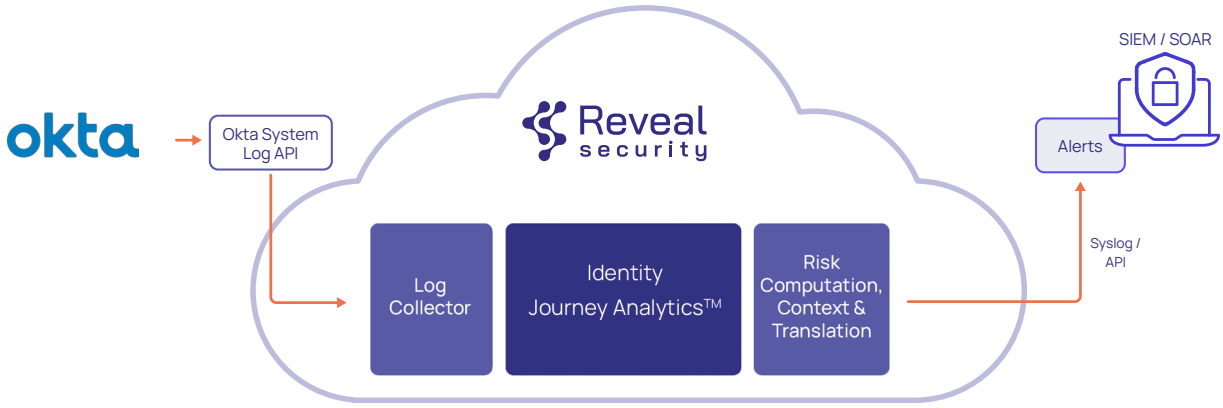
In 2022, over 80% of security breaches were linked to compromised credentials, shifting the threat landscape to identities. Recent breaches such as MGM highlight how easily attackers can assume and misuse a user identity in an Identity and Access Management (IAM) system, including Okta Super Administrator or Org Administrator permissions, the highest permissions in an Okta organization. Preventative IAM security measures are important, but incomplete to prevent a material breach. Monitoring of user behavior is now essential to quickly detect and respond to threats across applications where access and authorization is controlled by IAM systems like Okta.

The Reveal Security platform, monitors user behavior, including highly privileged accounts such as Super Administrators, and detects suspicious activities by analyzing Okta logs within your Okta instance. This allows the accurate detection of abnormal administrator activities, indicating either an insider threat, an account takeover or the impersonation of a privileged administrator. Reveal Security also provides an additional layer of security after login by monitoring user behavior in applications where access and authentication are managed by Okta. This ensures the timely and accurate detection of threats post-authentication that have either bypassed preventative IAM controls or when an Okta identity has been compromised and is being misused or abused to execute an attack.

Specifically, with Reveal Security deployed in your Okta environment, you can:

Monitor administrative activities

Reveal Security offers comprehensive monitoring of administrative activities in Okta, providing detailed insights into user behavior. By analyzing Okta logs, it detects anomalous operations, crucial for identifying external attackers impersonating Okta administrators. This includes IAM operations that grant unauthorized access to enterprise IT infrastructure, both on-prem and in the cloud. This technique, observed in attacks like the MGM incident, highlights the importance of proactive identity detection and response in modern security.



By analyzing Okta logs, Reveal Security enables comprehensive monitoring of administrative activities, detects anomalous operations, and identifies external attackers impersonating Okta administrators.

Detect suspicious user behavior across enterprise applications

Reveal Security swiftly identifies suspicious user behavior in and across applications where access and authentication are managed by Okta. Reveal Security's advanced detection capabilities offer a comprehensive and context-rich approach to monitoring application use by identities after login, empowering security teams to efficiently identify and respond to real threats while minimizing the impact of false alerts. Reveal Security uses patented Identity Journey Analytics™ to model how users interact with business applications and delivers detailed alerts when suspicious behavior is detected.

About Reveal Security Platform

The Reveal Security platform offers organizations a comprehensive solution for detecting and responding to the abuse and misuse of authenticated identities in and across applications. Using unsupervised machine learning, it eliminates the need for manual rule creation and maintenance to detect insider threats and identity-based attacks. Reveal Security excels in providing individual and peer group analysis of identity journeys across various applications, making it a versatile and efficient security solution for SaaS, cloud, and on-premises applications with rapid time-to-value.

About Reveal Security

Reveal Security quickly and accurately detects identity threats post-authentication in and across SaaS applications and cloud services. The Reveal Security ITDR platform is the only solution in the market based on patented Identity 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.