Reveal security

Solution Brief

TrackerIQ 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

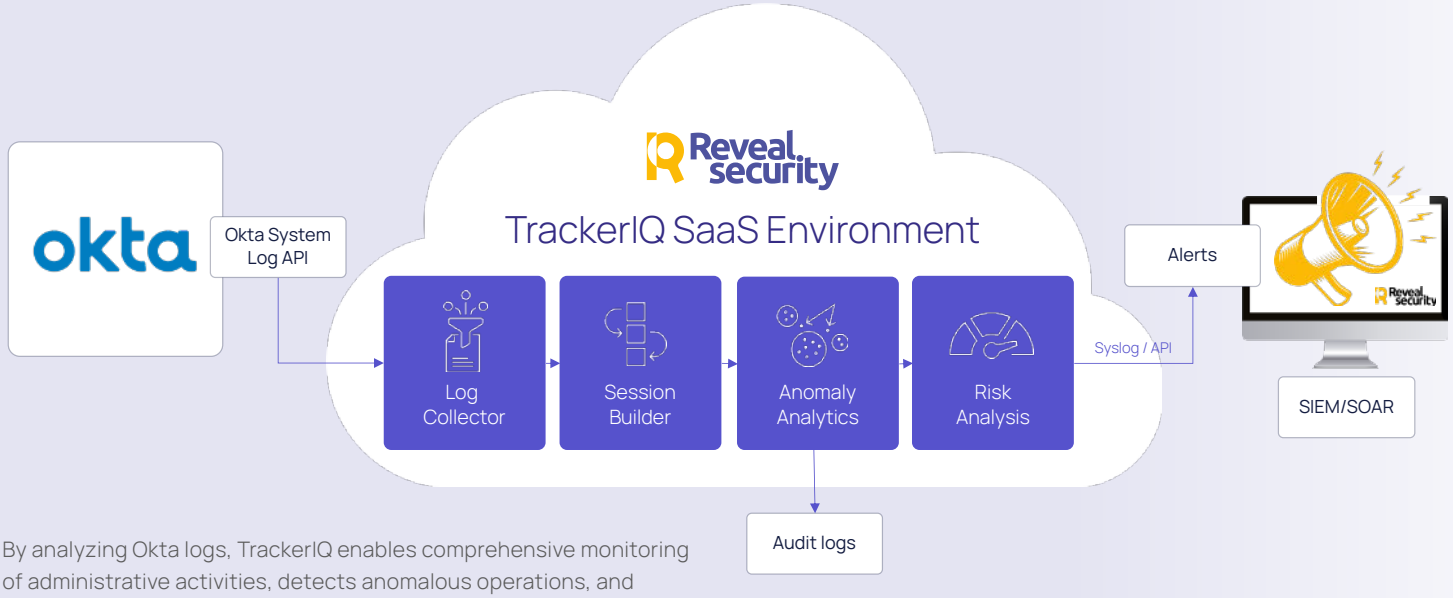
In 2022, over 80% of security breaches were linked to compromised credentials, shifting the threat landscape to identities. Recent breaches such as MGM highlight how easily attackers can assume and misuse a user identity in an Identity and Access Management (IAM) system, including Okta Super Administrator 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.

TrackerIQ, by RevealSecurity, 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, and account takeover or the impersonation of a privileged administrator. TrackerIQ 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 TrackerIQ deployed in your Okta environment, you can:

Monitor administrative activities

TrackerIQ 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.



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

This technique, observed in attacks like the MGM incident, highlights the importance of proactive identity detection and response in modern security.

Detect suspicious user behavior across enterprise applications

TrackerIQ swiftly identifies suspicious user behavior in and across applications where access and authentication are managed by Okta. TrackerIQ'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. TrackerIQ uses patented User Journey Analytics to model how users interact with business applications and delivers detailed alerts when suspicious behavior is detected.

About TrackerIQ

TrackerIQ, by RevealSecurity, offers organizations a comprehensive solution for detecting and responding to the abuse and misuse of trusted identities in and across applications. Using unsupervised machine learning, it eliminates the need for manual rule creation and maintenance to identify threats. TrackerIQ excels in providing individual and peer group analysis of user 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 RevealSecurity

Reveal Security is an application and identity threat detection company that delivers accurate behavior-based user analytics without rules. This allows organizations to cost effectively detect, alert and quickly respond to the abuse and misuse of trusted identities operating inside and across the mission-critical applications that drive their business.

For more information, visit www.reveal.security