Abnormal Security for Okta

Analyze human behavior to protect Okta identities.

Human identities are a top attack target

Attackers are using legitimate credentials to compromise cloud identities. Okta reports 34% of all authentication traffic is malicious and associated with tactics like credential stuffing.

Attackers attempt to exploit SSO and bypass MFA

Generative AI enables sophisticated social engineering campaigns to steal credentials. MFA Bypass-as-a-service kits are available on the Dark Web. These tools allow even the most amateur hackers to mimic APTs.

Defense-in-depth is critical to identity protection

86% of security leaders feel current identity compromise detection tools are insufficient. While Okta is a best-of-breed identity platform, persistent threats by attackers require more layers of protection.

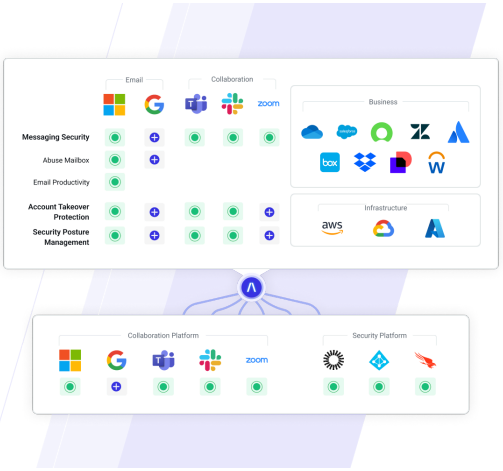
Extend Abnormal Protection to the Identity Platform

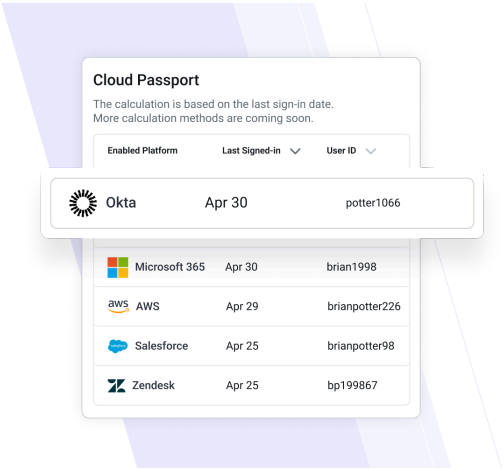
Humans are the biggest vulnerability for any organization, and while email is the primary way those humans are targeted, identity-borne threats are becoming increasingly common and difficult to detect and stop. While Okta is a powerful security platform in its own right, new tactics aimed at exploiting identity platforms like Okta create a need for an additional layer of protection. The key to uncovering compromised Okta identities is analyzing human behavior. Security teams need consistent visibility that not only automates detection and response when identity compromise is detected in Okta but also provides higher fidelity identity threat detection across the entire cloud ecosystem. Abnormal provides that platform.

How Abnormal Secures Okta

Simple API or OAuth Integration to Ingest Okta Events

Connect directly to Okta through your preferred integration method, and automatically ingest authentication signals. Abnormal Human Behavior AI then begins to correlate Okta authentication events against email platform activity.





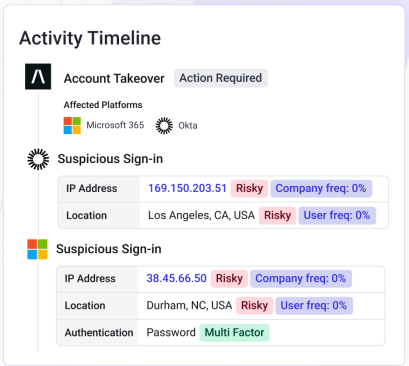
Continuous Monitoring to Detect Unusual Okta Sign-In Events

Abnormal AI automatically learns typical Okta authentication patterns across your organization, creating a dynamic behavioral baseline for each user. Any notable deviation from this baseline triggers an event in Abnormal.

AI Threat Detection and Response*

Abnormal provides two options for Okta threat response: one-click remediation through Abnormal's PeopleBase to kick out suspicious users before they cause harm or automated remediation in the event that a user has truly had their identity compromised. Both options disable the user, terminate sessions, and force a password reset—ensuring the threat is resolved.

*Available for API key integration-only



Try Abnormal Today

See how Abnormal can keep attacks out of your cloud email and connected platforms. Integrate in minutes via API.

abnormalsecurity.com/risk →

Abnormal