





## Abnormal Account Takeover Protection

Use autonomous AI to analyze every human, uniformly detecting and responding to account compromise *across platforms*.

Most organizations maintain an interconnected cloud environment encompassing email platforms, hundreds of SaaS applications, and critical infrastructure. A single account takeover means a user's entire cloud identity has been compromised—giving unfettered access to the cloud ecosystem.

Attackers are leveraging malicious generative AI tools and as-a-service phishing kits that bypass traditional defenses like MFA to gain this access. But stopping cloud account takeover across platforms is ineffective and inefficient with conventional tools and manual analysis.

### Abnormal provides the solution.

-  Cloud-native API architecture centralizes cloud visibility by enabling a simple integration to any cloud app in under five minutes with only a few clicks.
-  Human behavior AI automatically monitors authentication signals, communications, and notable activity, such as unusual locations, IPs, or VPNs or new MFA device registrations, across all integrated platforms—enhancing behavioral models without the need for rule or policy creation.
-  Automatically identifies compromised identities, generating a contextual behavioral case timeline to enable investigation of notable events.
-  Automates remediation, immediately terminating sessions and revoking account access across cloud entities once an account takeover is confirmed.

**\$329**  
Million

Total amount saved by customers in 2023 due to account takeovers stopped by Abnormal.

**>10x**

Reduction noted by customers in incident response time when addressing an account takeover.

**86**

Percentage of security practitioners who feel legacy tools cannot adequately protect against account takeovers.

### Account Takeover Protection at a Glance

#### Provides a single, unified platform.

Simple integration, an easily scalable platform, and automatic learning means minimal SOC overhead and little manual effort.

#### Uncovers undiscovered breaches.

Abnormal bases detection and analysis off of the dynamic behavioral baseline built for each user rather than predefined rules and detections.

#### Accelerates investigation.

By automatically analyzing employee activity across the cloud and creating a behavioral case timeline, Abnormal significantly reduces manual SOC effort and highlights threats that may have gone unnoticed.

#### Achieves uniform detection and response.

Autonomous AI automatically remediates cross-platform compromise, massively reducing the time spent responding to account takeover incidents.