Abnormal

Cloud Account Takeover Protection

Use autonomous AI to analyze every human in your cloud environment, uniformly detecting and responding to account compromise.

84% of organizations use at least one private cloud. Cloud providers are responsible for the security of the cloud—not security of your data in the cloud. When asked which platforms are the most concerning when it comes to protecting against account compromise, security leaders uniformly cited cloud infrastructure.

To compromise these platforms, attackers are leveraging malicious generative AI tools and as-a-service phishing kits that bypass traditional and native defenses. But stopping cloud account takeover, especially across platforms, is ineffective and inefficient with conventional tools and human analysis.

$329 Million Total amount saved by customers in 2023 due to account takeovers stopped by Abnormal.

71 Percentage of security teams noting that preventing cloud account takeover is their top concern.

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

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.

*remediation will be available in Q3, 2024

Cloud 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.

See Abnormal in Action. **Request a Demo.**

abnormalsecurity.com →