Abnormal

Core Account Takeover Protection

Autonomous AI analyzes every human across cloud email and identity platforms, uniformly detecting and responding to account compromise.

Compromised accounts have become the most common cause of data breaches. Traditional email security solutions cannot effectively detect account takeovers because they lack visibility into identity, behavior, and device attributes that indicate a user's account has been hijacked.

Core Account Takeover Protection stops takeovers in real time.

Detects compromised accounts across email and identity platforms like Google Workspace, Microsoft 365 and its 85+ associated apps, Entra ID, and Okta—observing end-user behavior for activity that deviates from their known normal, including login patterns, MFA methods, too-fast-to-travel locations, mail rule changes, identity events ingested through Abnormal's Crowdstrike integration, and more.

Recreates the crime scene by creating a case file of the account takeover diagnosis to organize the evidence for manual review.

Kicks attackers out of hijacked accounts by automatically blocking account access, triggering a password reset, and signing out of all active sessions. Administrators can choose to auto-remediate compromised accounts or manually review cases.

Immediately remediates lateral emails sent from compromised accounts to hidden folders, so other employees cannot see or engage with them.

Stop Email Account Takeovers.
Request a Demo.

abnormalsecurity.com →

$329M	Total amount saved by customers due to account takeovers stopped by Abnormal in 2023[1]
1,454	Average number of hours saved to remediate compromised account.
6	Seconds to remediate compromised accounts post-detection.

The Abnormal Advantage at a Glance

Enhanced detection. Uncover subtle anomalies in user behavior to precisely detect compromised accounts.

Mitigates potential damage. Leverage signals across the email and identity ecosystem and allow administrators to make decisions about the remediation action.

Eliminates dwell time. Reduce compromised account remediation to six seconds post-detection.

Provides visibility. Get insight into identity, behavior, and device attributes across your user base.

[1](Abnormal Security Research, 2024)