Abnormal

Email-Like Account Takeover Protection

Available as an Add-On to Abnormal Inbound Email Security

Detect compromised user accounts across your critical communication channels.

All it takes is one. A successful email account takeover is one of the most damaging attacks organizations can face.

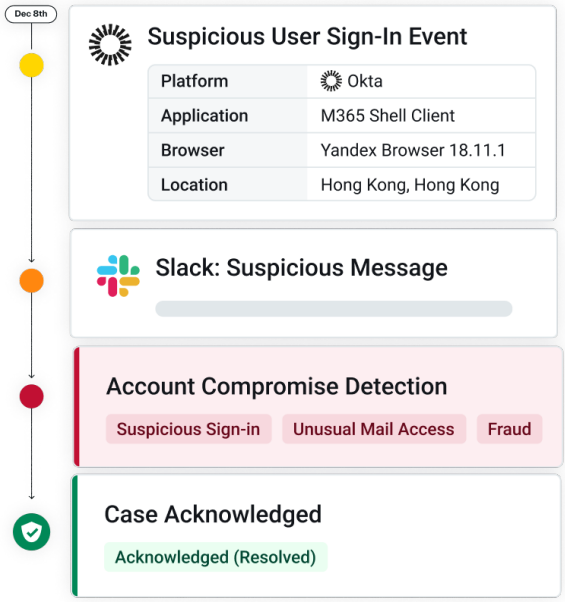
And since corporate email credentials can provide keys to all applications in an organization's cloud environment, one compromised email account could mean attackers suddenly have access to other sensitive platforms such as collaboration apps. Similarly, one compromised collaboration account could then give access to all other connected applications—including email.

Email-Like Account Takeover Protection keeps users safe, wherever they choose to collaborate.

Analyzes authentication data in Slack, Teams, and Zoom to determine when a user's account may have been compromised. Identifiers such as browser, location, and user IP are correlated against known indicators of compromise (IOCs) to flag suspicious events with a high level of confidence.

Once a compromised account has been identified, Abnormal recreates the crime scene in detail, building a case with a timeline of suspicious events across collaboration applications. This case widens the scope of account takeover investigation, giving a more complete snapshot of the attack surface—uncovering where an attacker has gained or attempted to gain access across the cloud environment.

Integrates with major identity providers including Okta and Azure Active Directory to enrich each case with single sign-on activity—giving greater insight into each session. This allows security teams to see discrepancies between IdP sessions and those initiated on each collaboration platform.



The Abnormal Advantage at a Glance

Expands account takeover visibility. Gives expansive visibility. Only Abnormal provides account takeover detection and analysis across email, Slack, Teams, and Zoom all through one integrated platform.

Speeds up investigations. Say goodbye to siloed data and investigate threats to collaboration platforms all in a single case file to better understand the scope and impact of each account takeover attempt.

Enhances detection. Confidently identify account takeover attempts by enriching each case with identity provider data to help determine when legitimate and malicious sessions have been initiated on collaboration platforms.

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

abnormalsecurity.com →