Abnormal Account Takeover Protection

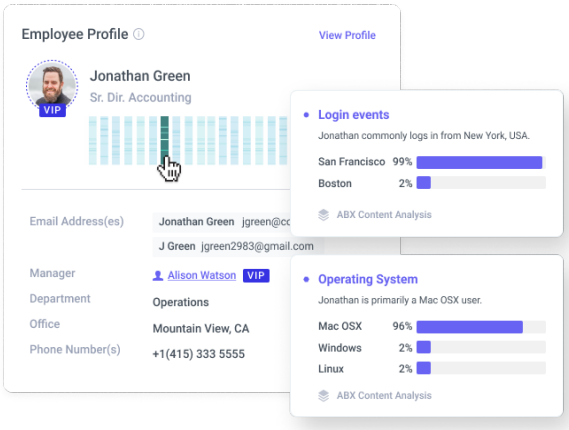
Prevent account takeovers with a solution that deeply understands and baselines normal user behavior.

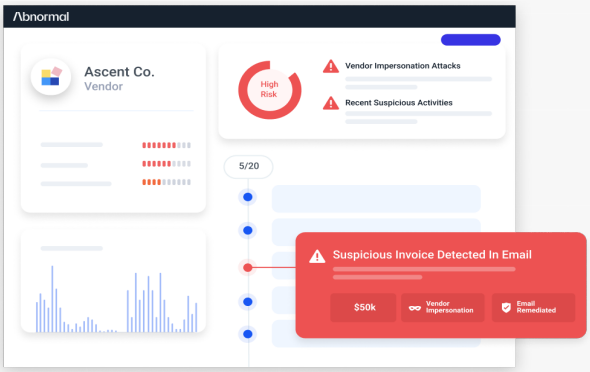
By understanding normal behavior, Abnormal can detect any deviations in these baselines to uncover potentially compromised accounts and then immediately remediate them. When left undetected, attackers can use compromised accounts to exfiltrate sensitive data or send lateral phishing emails. Abnormal protects your end users and their information, no matter how account credentials were stolen.

Baselines Good Behavior with Multi-Channel Analysis

Abnormal deeply understands and baselines normal behavior for every end user by analyzing signals including login frequency, locations, devices, operating systems, browsers used, applications accessed, communication behavior, information shared, and many more.

Understanding the normal allows Abnormal to detect abnormal login behavior, unusual email recipients, changes in tone, lateral phishing messages, and other indicators to recognize potentially compromised accounts. This information is conveniently presented as a 'genome' for analysis by security teams.





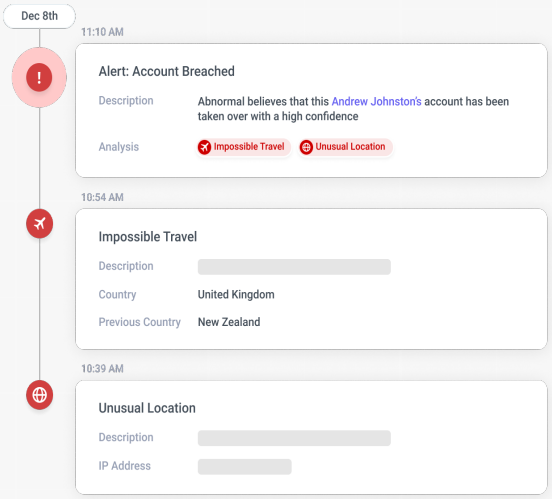
Monitors Vendors for Compromised Accounts with VendorBase

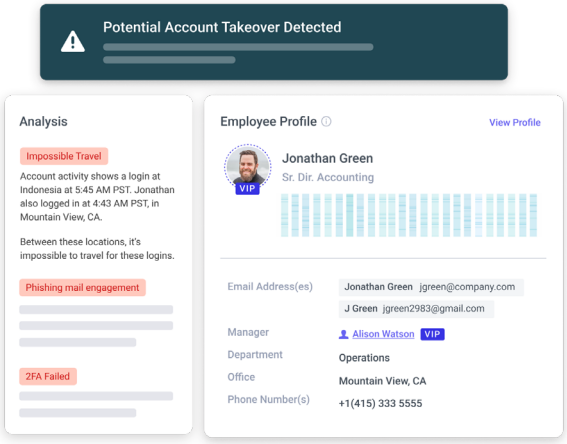
When vendors and partners become compromised, bad actors can use those accounts to send attacks to your end users.. Abnormal automatically correlates thousands of signals to identify and block suspicious emails sent from compromised vendors.

Recreates the Crime Scene in Detail

Abnormal intelligently gathers and organizes all the evidence that led to the diagnosis, along with summarized conclusions.

Its ability to pull together a case file—by drawing signals across email systems, Active Directory, devices, browsers, applications, and more—equips security teams to take immediate action.





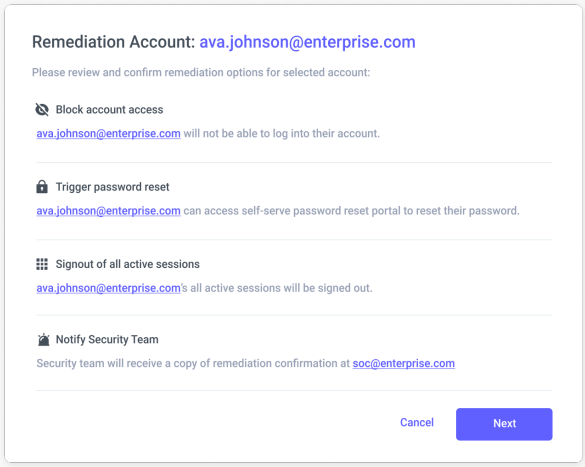
Provides an Explainable Attack Analysis

Abnormal intelligently gathers and organizes all evidence that led to the diagnosis, along with summarized conclusions, and equips security teams to take immediate action.

This analysis enables SOC analysts to understand why an account was judged as compromised. You will see the evidence-based on monitored relevant signals and an event log of unusual events, such as suspicious logins, mail rule changes, or abnormal communication patterns.

Automatically Remediates Accounts

Stop attackers in their tracks by signing users out of active sessions, instantly disabling accounts, triggering Microsoft Office 365 and SSO password resets and creating service tickets.



Abnormal Account Takeover Protection Key Capabilities

- **Automated Remediation**
  Allow Abnormal to disable the account, sign out of active sessions, and reset account passwords.
- **Manual Account Remediation**
  Manually disable the account, sign out of active sessions, and reset account passwords.
- **Automated Alerts**
  Receive alerts via email and your preferred SIEM platform.
- **Compromised Vendor Detection**
  Block emails from compromised vendors and partners and understand vendor risk with VendorBase.
- **Explainable Attack Analysis**
  Receive insight into why accounts have been flagged as compromised.
- **Third-Party Identity Provider Integration**
  Integrate seamlessly with Microsoft Active Directory, Google Workspace, and Okta for additional account compromise signals based on user sign-in behaviors and MFA failures.

Try Abnormal Account Takeover Protection Today

Integrate within minutes via one-click API. Detect compromised accounts, stop attack progression, and remediate them.

www.abnormalsecurity.com/risk →