Abnormal SECURITY

Solution Brief:

Abnormal Security
Enterprise-Grade Email Security

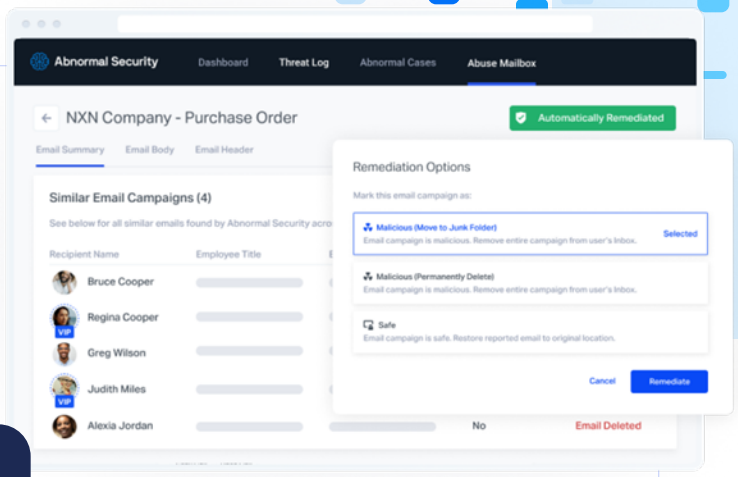
Enterprises are at the forefront of modern BEC attacks, due in part to the financial transactions they have in-motion, but also because of their complex supply chains that can be compromised and leveraged to successfully exploit businesses.

Abnormal Security meets the unique challenges of enterprises with industry-leading BEC protection built on a scalable platform that can handle large brand deployments through multi-tenant administrative controls.

What makes Abnormal Security enterprise-grade?

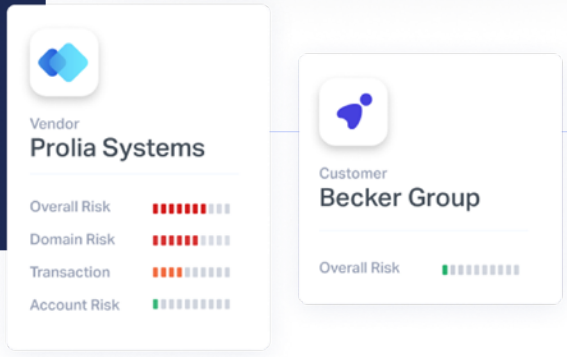
No ongoing policy configuration or manual remediation

Abnormal's AI-powered decision engine provides organizations with unparalleled effectiveness in stopping BEC threats, including difficult to detect account compromise attacks. As a result, SecOps gains valuable time back from not having to manually evaluate and remediate threats on a case-by-case basis.

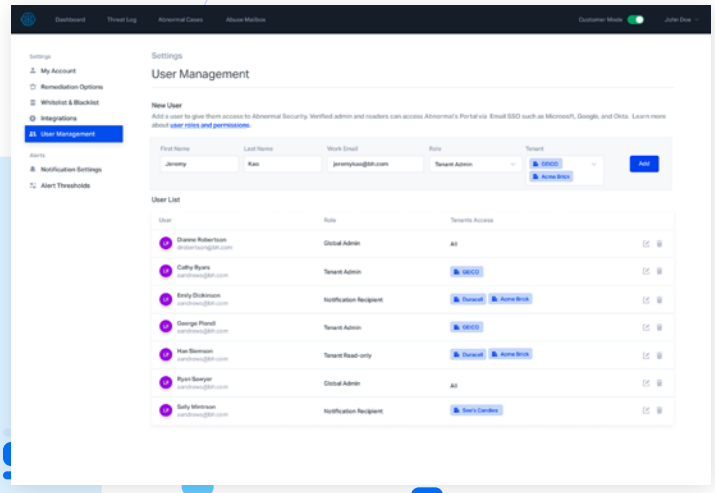


Abnormal Security provides unique visibility into supply chain partners and stops compromised vendor attacks with VendorBase, Abnormal's global, federated database of vendors and customers.

Learn more



Abnormal SECURITY



Role-based Access Control for Multi-Tenancy

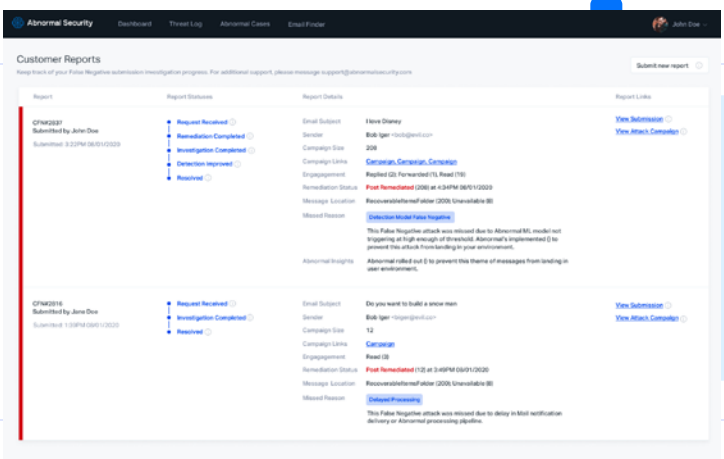
Gives organizations the ability to assign global admins, tenant admins, or tenant readers that have various privileges access options to the portal. Enterprises gain added control over user-role assignments and data-sharing.

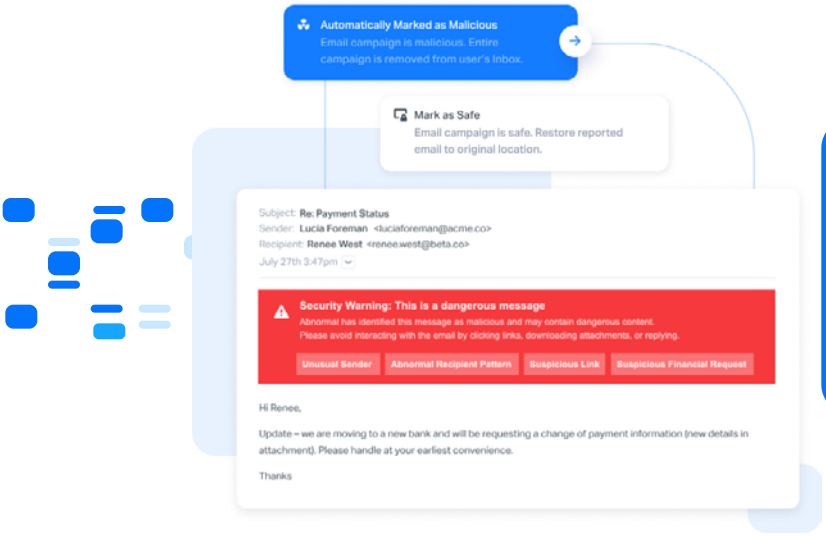
Cross-Tenant Abuse Mailbox Support

Enterprise customers with multiple tenants that leverage a unified phishing mailbox to collect employee reported attacks can now set up Abnormal's Abuse Mailbox without altering their workflow. Save time by searching and remediating message campaigns across all tenants.

Customer Report Portal

A centralized customer report dashboard that handles false negative reports submitted by an organization to Abnormal. SecOps can keep track of the issues they file, check detailed report status, investigation details, read improvements and reasons behind the made from each report.





Incident Response Automation

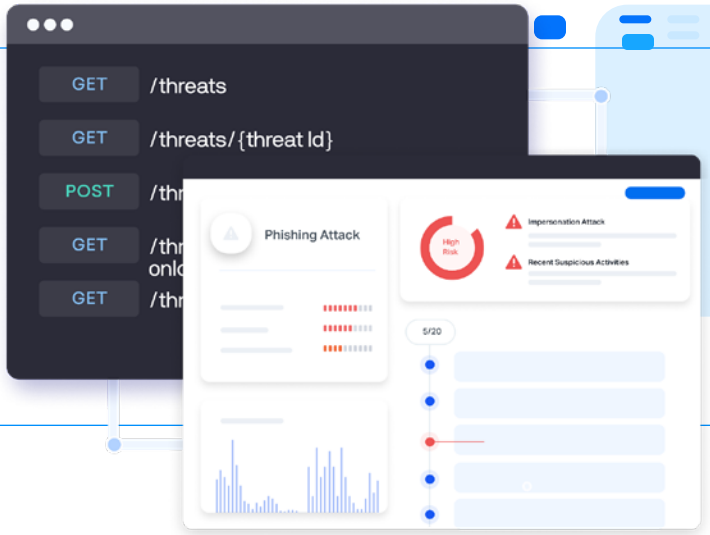
Abnormal Security provides a SOC platform for email on top of Microsoft APIs to automate common tasks and quickly surface coordinated attacks to security operations teams.

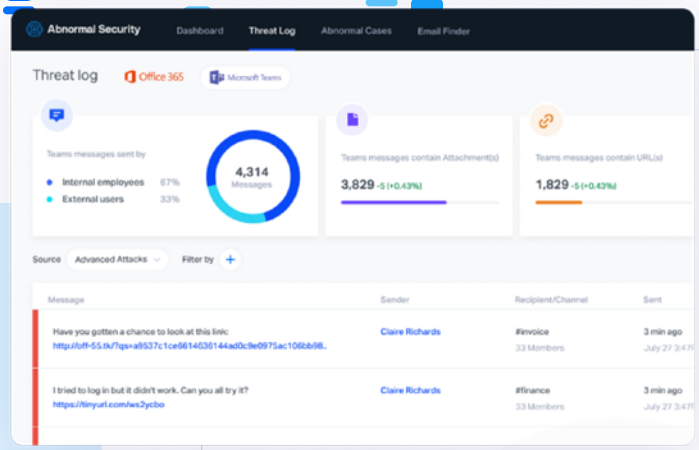
Abnormal SECURITY

Integrations

Seamless integration into your existing security stack: SIEM, SOAR, detection tools and ticketing systems. Connect into Microsoft Outlook, Microsoft Teams, G Suite, Slack, Splunk, Proofpoint TAP and others.

Learn more





Microsoft Preferred Partner for BEC Protection

Augments and enhances the native security protection capabilities of Microsoft EOP and ATP to stop the full range of Business Email Compromise (BEC) and account takeover attacks.

Additionally, Abnormal detects malicious content, such as URLs and malicious attachments, that surface through Microsoft Teams. Automatically remove any malicious content.

Abnormal Security is available in the Azure Marketplace where enterprises can self-serve deploy directly from the Azure Marketplace (qualified customers only) and receive Azure consumption credits when they purchase Abnormal. Also available via Microsoft Sellers.

Microsoft

Abnormal SECURITY

About Abnormal Security

Abnormal Security is a next-generation email security company that protects enterprises from advanced targeted attacks including business email compromise. Abnormal Security's cloud-native architecture integrates directly into cloud office APIs and requires no configuration. Its innovative AI provides enterprises with an inside-out understanding of its people, organizational processes and the extended supply chain to stop targeted email attacks and detect compromised accounts. Backed by Greylock Partners, Abnormal Security is based in San Francisco, CA. More information is available at: www.abnormalsecurity.com.