Abnormal

Cloud Email Security for the Modern Workforce

Abnormal Security leverages advanced behavioral AI to stop the full spectrum of email attacks.

The open design of cloud email platforms provides new opportunities for collaboration and extensibility, but it has also opened up new channels for attackers to exploit. In fact, remote work has increased the average cost of a data breach by $1M per incident.

Attackers today are learning how the different identities and applications within an organization interact, then launching targeted attacks that continue to evolve in complexity and efficacy. These sophisticated attacks evade detection by traditional solutions. Increasingly, they also exploit lax security configurations in the email platform itself, using privileged user accounts and third party application integrations as entry points.

Abnormal provides the solution.

Learns the behavior of every identity—employee, vendor, application, and email tenant—in your cloud email environment and analyzes the risk of every event to block even the most sophisticated attacks.

Remediates malicious emails, removing the possibility of end-user engagement.

Fully automates email triage, remediation, and reporting, bringing together all auto-detected and user-reported threats into a single interface.

Helps employees be more productive by automatically moving promotional graymail mail out of the inbox.

Gives visibility into configuration drifts across your cloud email environment, surfacing third-party application misconfigurations, elevated privileges, and other potential risks.

65 Average number of unique business email compromise (BEC) attacks organizations experience per month.

$120k Average cost per business email compromise incident.

4,000 Hours Average SecOps hours saved with Abnormal Abuse Mailbox automation in one year.

60 Seconds To integrate with Microsoft 365 or Google Workspace and begin protecting employees.

The Abnormal Advantage at a Glance

Provides full spectrum protection. Blocks the malicious and unwanted emails that bypass other solutions, including never-seen-before attacks that do not contain traditional indicators of compromise.

Stops account takeovers. Detects internal and external compromised accounts and remediates them.

Personalizes protection. Improves employee and executive productivity with adaptive protection from graymail messages, personalized to each employee's behavior.

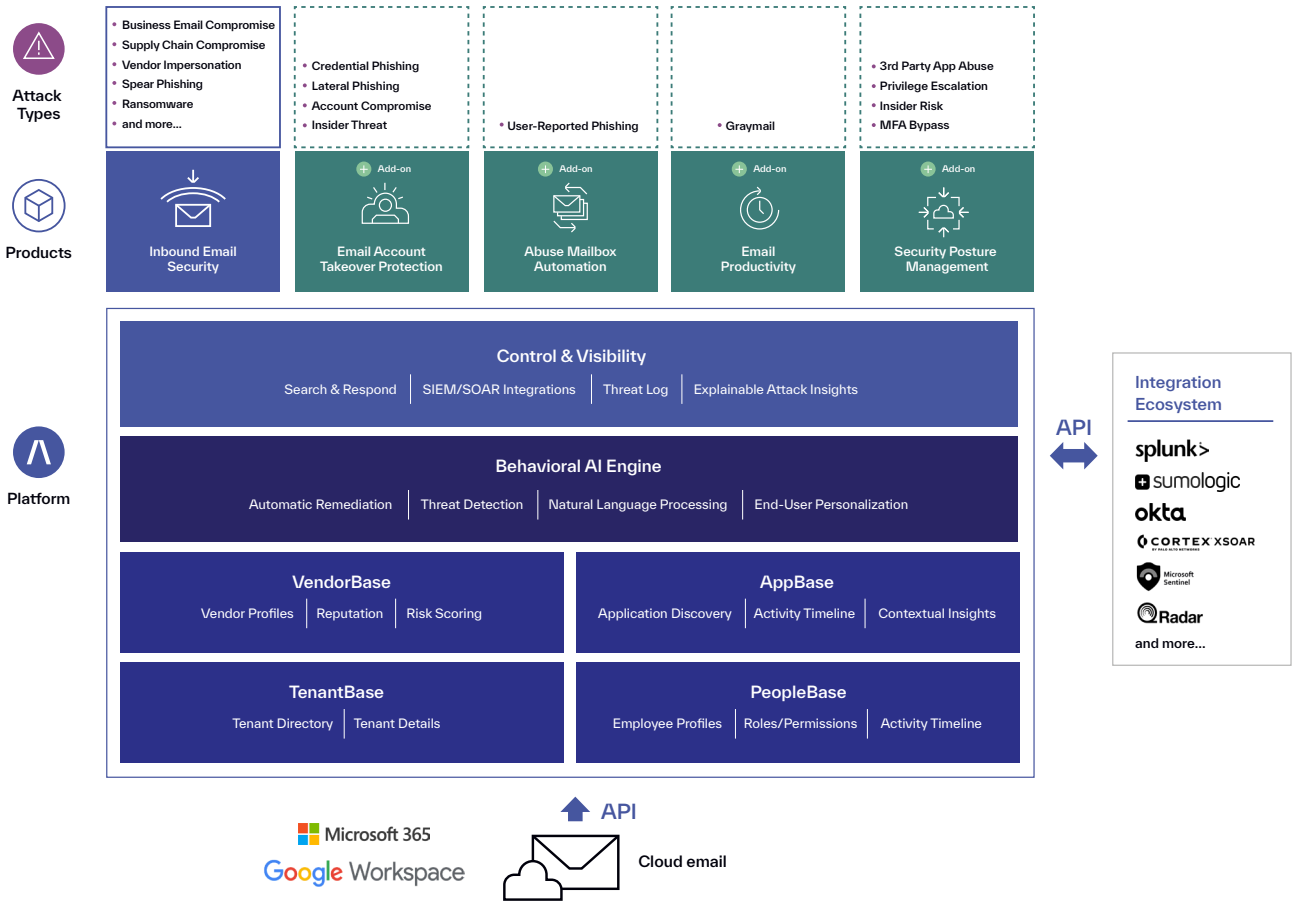
Deploys instantly. No rules, policies or configuration needed. Abnormal integrates via API in only three clicks.

Delivers proactive posture insights. Dynamically monitors for high-risk configuration drifts across users, applications, and tenants.

As a cloud-native email security platform, Abnormal leverages behavioral data science to stop the never-before-seen attacks that evade traditional security tools. Where legacy email security solutions rely on rules and policies to identify attacks, Abnormal delivers a fundamentally different approach that precisely detects and then automatically remediates email threats.

Abnormal integrates with Microsoft 365 or Google Workspace within minutes via API and starts working immediately to develop an organizational baseline of known good behavior. This identity and context awareness enables Abnormal to stop all types of email attacks, from business email compromise to account takeovers to supply chain fraud and more. The platform also provides direct visibility into security posture to uncover and mitigate critical risks introduced by cloud email environments.

Abnormal Behavioral AI Security Platform



The Abnormal Cloud Email Security platform includes:

Inbound Email Security: Harnesses advanced behavioral AI to block socially-engineered attacks and other malicious emails.

Abuse Mailbox Automation*: Centralizes user-reported emails and automatically investigates them, responding to close the feedback loop with users.

Email Account Takeover Protection*: Detects, disables and remediates compromised accounts.

Email Productivity*: Filters time-wasting emails from employee inboxes with an adaptive and policy-free approach.

Security Posture Management*: Discovers and mitigates misconfiguration risks across your cloud email environment.

* Add-on product. Note that Abnormal Inbound Email Security is required to use these features.

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

abnormalsecurity.com →