Abnormal

Cloud Email Security for the Modern Workforce

Abnormal Security combines a cloud-native API architecture and behavioral AI to stop the full spectrum of email and collaboration application 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.

Attackers today are learning how the different identities within an organization interact, then launching targeted attacks that continue to evolve in complexity and efficacy. These sophisticated attacks evade detection by traditional solutions, using privileged user accounts and third-party application integrations as entry points. More attackers are even setting their sights on adjacent, email-like channels including collaboration apps to infiltrate the organization.

Abnormal provides the solution.

- Block targeted inbound email attacks including credential phishing, business email compromise, supply chain fraud, and more.
- 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 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.

$125k Average cost per business email compromise incident.

5,000 Average SecOps hours saved annually with Abnormal Abuse Mailbox Automation.

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

$4M Average organization's savings in mitigated risk annually with Abnormal.

The Abnormal Advantage at a Glance

Protect more.

Defend against the full spectrum of attacks, including costly business email compromise, vendor fraud, malware, and more.

Spend less.

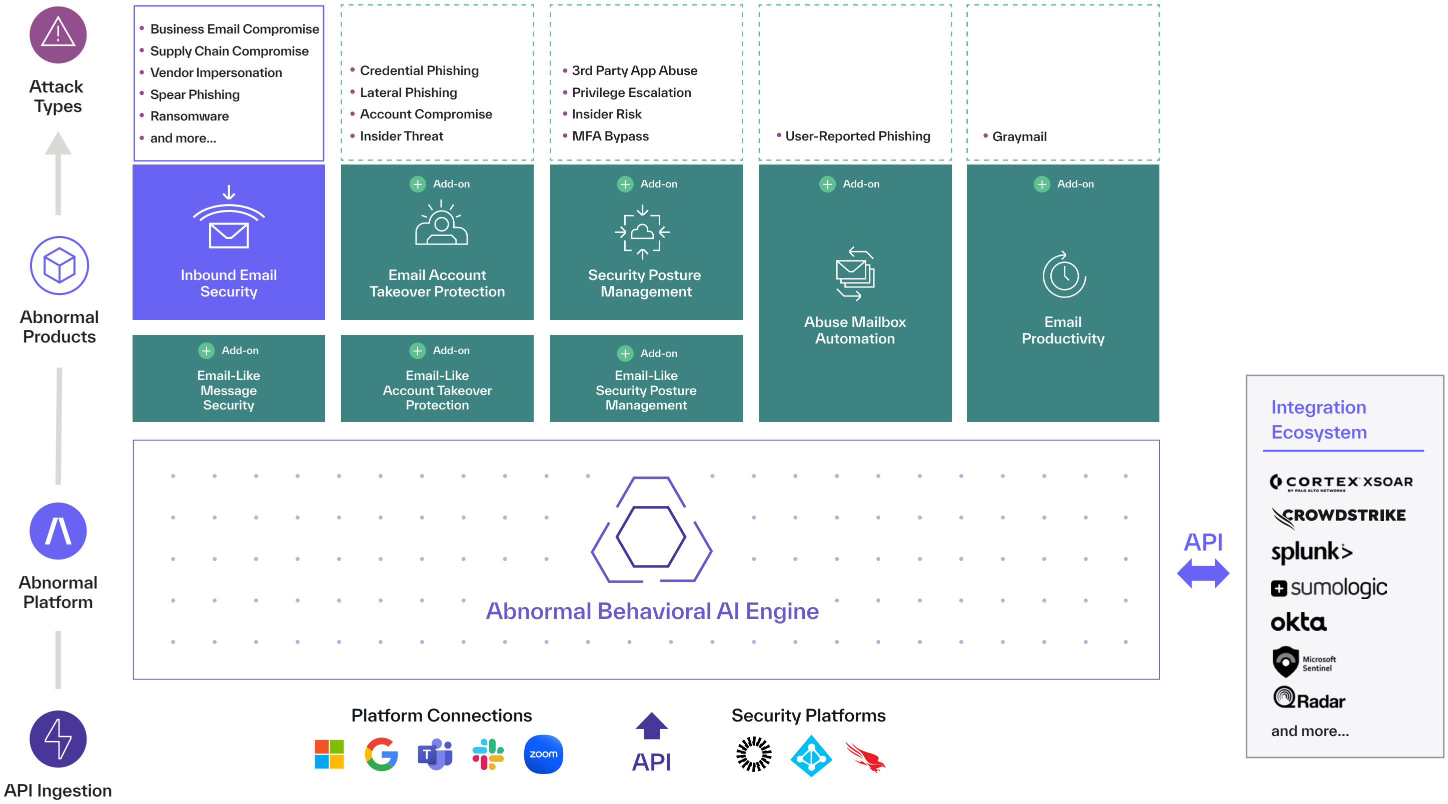
Eliminate costs of redundant software, including secure email gateways, and fully automate email security operations.

Secure the future.

Implement a single, extensible platform to stop emerging email attacks, including account takeovers, attacks emanating from third-party apps, collaboration application abuse, and more.

As a cloud-native, API-based 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.



Attack Types

- Business Email Compromise
- Supply Chain Compromise
- Vendor Impersonation
- Spear Phishing
- Ransomware
- and more...

- Credential Phishing
- Lateral Phishing
- Account Compromise
- Insider Threat

- 3rd Party App Abuse
- Privilege Escalation
- Insider Risk
- MFA Bypass

- User-Reported Phishing

- Graymail

Abnormal Products

Inbound Email Security

Add-on Email Account Takeover Protection

Add-on Security Posture Management

Add-on Abuse Mailbox Automation

Add-on Email Productivity

Add-on Email-Like Message Security

Add-on Email-Like Account Takeover Protection

Add-on Email-Like Security Posture Management

Abnormal Platform

Abnormal Behavioral AI Engine

API

Integration Ecosystem

CORTEX XSOAR

CROWDSTRIKE

splunk>

sumologic

okta

Microsoft Sentinel

QRadar

and more...

API Ingestion

Platform Connections

zoom

API

Security Platforms

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.

Email-Like Messaging Security*: Detects and surfaces malicious URLs discovered within Slack, Teams, and Zoom messages.

Email-Like Account Takeover Protection*: Alerts security teams of suspicious authentication activity in Slack, Teams, and Zoom that may indicate an account takeover.

Email-Like Security Posture Management*: Monitors for changes in user privileges in Slack, Teams, and Zoom, surfacing those that are high impact.

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

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

abnormalsecurity.com →