Abnormal

Inbound Email Security

Stop advanced email attacks with behavioral AI that understands intent, not just indicators.

Modern email attacks exploit human behavior with tailored messages that mimic legitimate communication and bypass traditional defenses. Each successful business email compromise attack costs organizations an average of $137k[1] and 86% of business leaders report at least one AI-related incident in the past year.[2]

Only Abnormal is built to understand attacker intent, using behavioral context to identify malicious activity even when traditional indicators are absent.

The Abnormal Solution

- **Detects targeted BEC, VEC, and phishing by analyzing tens of thousands of behavioral signals to identify attacker intent.**
- Automatically remediates malicious email before user engagement, reducing manual triage without ongoing detection tuning.
- Extends protection from reported messages to related attack variants, continuously improving detection precision.
- Explains every verdict with detailed logs, categorization, investigative tools, and the behavioral signals that drove the decision.
- Gives teams control over policies and priorities unique to their organization, without requiring them to engineer the underlying detection.
- Deploys in minutes through API integration, with no manual tuning or mail-flow disruption.

60 BEC attacks blocked per customer per month, on average

15+ Hours Saved for security teams each week

60 Seconds To integrate Abnormal with your cloud email platform

33% Lower average breach costs for companies using AI and automation

The Abnormal Advantage at a Glance

Stops attacks others miss. Behavioral AI understands attacker intent to detect sophisticated threats without relying on known indicators or static rules.

Delivers hands-free automation. Automatically detects and remediates threats before users engage, eliminating repetitive triage.

Explains every decision. Surfaces the behavioral signals and reasoning behind each verdict so analysts can understand why a message was actioned without recreating the investigation.

Simplifies email security operations. Works natively with M365 and GWS, with unified quarantine management that keeps analysts in one workflow without adding gateway complexity.

[1] Internet Crime Complaint Center (IC3). 2023. FBI Internet Crime Report. https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf
[2] Cisco 2025 Cybersecurity Readiness Index (survey of 8,000+ security leaders globally) 2025 Cisco Cybersecurity Readiness Index

See Abnormal AI in action. **Request a demo.** abnormal.ai ›