Abnormal

Inbound Email Security

Stop the email attacks that bypass other solutions when you pair behavioral data science with risk-adaptive detection.

Modern email attacks are circumventing traditional email security solutions with increasing sophistication and severity. Each successful business email compromise attack costs organizations an average of $120k and socially-engineered attacks are responsible for 35% of all cybercrime losses.

Abnormal Inbound Email Security stops advanced attacks with a fundamentally different approach.

- Baselines known good behavior across employees and vendors with an AI-based anomaly detection engine.
- Detects and remediates malicious emails in milliseconds to prevent end-user engagement.
- Offers explainable attack insights with in-depth reviews referencing email forensics like the location and timing, frequency of communication, topic and tone, and intent of the email attack.
- Deploys in minutes via API. No configuration or policies required.

Secure Your Inbound Email.
Request a Demo.

abnormalsecurity.com →

4X	Fewer attacks and unwanted emails land in employee inboxes.
15+	Hours saved for security teams each week.
60	Seconds to integrate Abnormal with your cloud email platform.
36	BEC attacks blocked per customer per month, on average.

The Abnormal Advantage at a Glance

Detects novel attacks. Identifies anomalies to prevent never-before-seen attacks that legacy solutions miss.

Automatically remediates malicious emails. Instantly removes the email from the inbox to prevent interaction.

Adapts to changing vendor risk. Updates protection based on evolving risk levels across partners.

Understands attacks. Provides high-level trends and deep dives into advanced attacks.