Abnormal

We Protect Organizations From the Attacks That Matter Most

Modern Email Security for Microsoft 365 and Google Workspace

Abnormal Overview:

- Cloud-native email security platform that stops all modern email attacks
- Protects Fortune 100 companies; largest deployment is 600,000 mailboxes
- Strategic Microsoft partnership

Key Differentiators:

- Precisely blocks all email attacks using behavioral AI
- Protects you from internal and external compromised accounts
- Deploys in minutes via API; no configuration needed
- Simplifies email security

An Exponential Increase in Modern Email Attacks

Modern attacks, including business email compromise, supply chain fraud, and ransomware, are on the rise. According to the FBI, business email compromise alone accounted for **nearly 35% of all cybercrime losses** in 2021, and that number is only growing as threat actors become more effective.

Modern Attacks Evade Secure Email Gateways

Traditional defenses rely on conventional threat intelligence and known bad indicators to block email threats. Modern attacks bypass secure email gateways because they come from trusted sources and do not contain malicious links or attachments.

You Need a Modern Approach to Email Security

Abnormal provides a fundamentally-different approach that precisely blocks all email attacks. Our modern, cloud-native API architecture continuously baselines known good behavior by leveraging identity, behavior, and content to detect and remediate anomalies.

Why You Should Care:

10x more effective solution for email security

3x fewer attacks get through

2x faster threat response time

Gartner peerinsights™

4.9 ★★★★★

for **92** reviews on Gartner Peer Insights™ as of 3 Mar. 2022

Read all reviews →

★★★★★

"Email Security Is Broken. Abnormal Security Is the Fix."

Read review >

★★★★★

"Say Goodbye To Under-Performing SEGs."

Read review >

★★★★★

"Securing the Email Channel Within Seconds."

Read review >

We Protect Organizations From the Attacks That Matter Most

Supply Chain Compromise

There's a **25%** chance of your organization being targeted by a supply chain attack this week. These attacks evade secure email gateways because they come from trusted senders whose accounts have been compromised.

How Abnormal Stops It:

Automatically knows your vendors
Abnormal's VendorBase auto-identifies suppliers, vendors, and partners based upon past email communications and other signals gathered across the entire enterprise ecosystem.

Continuously assesses vendor risk and reputation
We assign a risk score for each vendor based on domains spoofed, accounts compromised, and suspicious business.

Inspects content, tone, and attachments
Abnormal inspects emails and attachments for suspicious information and identifies when a vendor has been compromised.

Executive Impersonation

29% of all socially-engineered attacks are a result of impersonation. These emails slip by secure email gateways because they are often text-based and rarely contain links or attachments.

How Abnormal Stops It:

Inspects email headers to expose impersonations
By analyzing header information, Abnormal can determine when an email domain has been spoofed.

Detects suspicious language, tone, and style
Even when messages contain no links or attachments, Abnormal recognizes language that is typical of phishing attacks.

Understands communication patterns
Abnormal uses natural language processing to understand individual behaviors, communication patterns, typical tones, and usual message content.

Account Takeover

26% of companies are targeted by account takeover attacks each week. When successful, threat actors receive access to sensitive information and can use these compromised accounts to launch further attacks.

How Abnormal Stops It:

Detects compromised accounts
By understanding and baselining normal login frequency, locations, devices, browsers, and IP addresses, Abnormal can determine when an account has been compromised.

Disarms takeovers automatically
Logs users out of active sessions, requires password resets, and helps affected users regain access.

Provides incident management and reporting
Allows teams to streamline remediation via integrations with IAM, SIEM, and SOAR tools.

Ransomware

76% of ransomware is delivered via email. Secure email gateways often miss these attacks when attackers combine social engineering with their ransomware schemes.

How Abnormal Stops It:

Detects suspicious correspondence patterns and credential phishing attempts
Abnormal uses identity detection and natural language processing to detect phishing attempts and other suspicious emails.

Blocks malicious attachments and links
The platform reviews all attachments and links to ensure they are safe, even if those links redirect upon click.

Provides explainable insights and malware forensics to security teams
Abnormal automatically prepares a detailed analysis of ransomware attempts, allowing teams to preview the content of attachments and link targets.