Abnormal

Abnormal for Healthcare

Discover the AI-based email security platform that protects healthcare organizations from the full spectrum of email attacks.

$330M in losses prevented by stopping account takeovers.

95% reduction in investigations and response times.

15+ hours saved for security teams each week through AI automation.

Abnormal Overview

- Cloud-native email security platform that protects against the widest range of email attacks with high efficacy.
- API-based solution integrates with Microsoft 365 and Google Workspace in minutes.
- Behavioral AI baselines normal behavior to block deviations from known good.

What Sets Abnormal Apart

- No disruption to mail flow and no changes to MX records required.
- Protection against internal and external account compromise.
- AI-driven triage, investigation, and auto-remediation for more efficient SOC workflows.

Abnormal Integrates Quickly With

- Secure email gateways and existing security layers for advanced protection.
- SIEM, SOAR, and other SOC solutions for fully automated workflows.
- Email security solution dashboards for single-source visibility into email threats, investigations, and trends.

Email Attacks Threaten Patient Data and Safety

Cybercriminals continuously target healthcare organizations via email to steal or ransom patient data. Attackers breach dozens of HIPAA-regulated entities every month, and the average cost is $9.77 million—the highest average data breach cost of any industry, according to IBM's 2024 Cost of a Data Breach Report.

Advanced Attacks Evade Traditional Email Defenses

Advanced email threats like sophisticated credential phishing attacks and business email compromise bypass secure email gateways (SEGs). Without a modern solution, your organization is at greater risk of data breaches, account takeovers, and ransomware attacks that endanger patient privacy and safety.

A Modern Approach to Healthcare Email Security

Abnormal's cloud-native solution integrates with Microsoft 365 and Google Workspace in minutes and uses thousands of signals across identity, behavior, and content to separate legitimate messages from dangerous threats. Because Abnormal can recognize anomalies even in ongoing conversations, it can immediately detect and remediate threats that legacy systems miss.

Real-World Results for Healthcare Organization

$34B
net patient revenue managed with Abnormal protection.

1,438
employee hours saved with graymail filtering in 30 days.

93%
of attacks stopped were sophisticated credential phishing.

Read the Case Study ›

Abnormal for Healthcare

Stop the most dangerous attacks that bypass your existing defenses.

Supply Chain Compromise

39.5% of healthcare organization data breaches in the first half of 2024 involved business associates. When attackers breach trusted vendor email accounts, they can send fraudulent payment requests that make it past secure email gateways.

How Abnormal Stops Supply Chain Compromise:

Knows your vendors

VendorBase™ auto-identifies suppliers, vendors, and partners using past email conversations and signals gathered across all customers.

Continuously monitors vendor risk and reputation

Assigns each vendor a risk score based on the number of domains spoofed, accounts compromised, and suspicious messages detected.

Examines message content, tone, and attachments

Uses AI and ML to inspect emails and attachments for suspicious signals that can indicate supply chain compromise and blocks the threat from reaching inboxes.

Credential Phishing

63% of significant healthcare organization security incidents in 2024 were caused by phishing. Credential phishing attacks can target employees or executives, using social engineering to evade secure email gateway detection.

How Abnormal Stops Credential Phishing:

Inspects email headers to expose impersonations

Identifies when an email domain has been spoofed to impersonate a brand, vendor, or specific person.

Detects suspicious language, tone, and style

Recognizes the language that indicates phishing attacks, even in messages with no malicious links or attachments.

Learns communication patterns

Applies natural language processing (NLP) to learn people's typical tone, behavior, and communication patterns to detect changes that may indicate phishing.

Ransomware

67% of healthcare organizations have received a ransomware attack in 2024. SEGs can miss these attacks when they combine social engineering with other tactics like supply chain compromise to conceal malicious content in a message from a trusted sender.

How Abnormal Stops Ransomware:

Analyzes message content and other signals for credential phishing

Utilizes identity detection and NLP to spot first-stage attacks like phishing, even those coming from trusted senders.

Blocks malicious attachments and links

Reviews all attachments and links for safety, including links that redirect upon clicking.

Gives security teams explainable insights and malware forensics

Automatically prepares detailed analyses of ransomware attempts, enabling teams to preview attachment content and link targets.

Account Takeovers

26% of organizations see at least one account takeover attempt each week. Once attackers acquire login credentials they can glide past standard security solutions, disguised as trusted employees, executives, vendors, or customers.

How Abnormal Stops Account Takeover:

Determines good sender behavior with multichannel analysis

Leverages API integration with Microsoft 365 and Google Workspace to analyze end-user behavior across devices, browsers, and apps.

Actively monitors user behavior and identity

Detects changes in content and tone, attempts to bypass multi-factor authentication, and shifts in normal login signals and then auto-remediates suspect accounts.

Includes unique VendorBase™ analysis and monitoring

Baselines known-good interactions with your vendors and evaluates vendor risk scores across the federated database of all customers to understand when a vendor may be compromised and block suspicious emails.

Abnormal

Request Your Abnormal Demo Now: abnormal.ai/demo