Abnormal AI for Financial Services

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

$300M 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 full spectrum of attacks and unwanted mail.
- 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.

Data, Reputation, and Revenue at Risk

According to Abnormal data, financial services (FinServ) organizations experienced a 25.2% year-over-year rise in the volume of advanced email attacks and a 17% increase in phishing attacks. A new solution is needed to prevent these advanced threats.

Additional Layers of Defense are Necessary

Advanced email threats like BEC and invoice fraud are built to evade secure email gateways. These threats are increasing and put financial services organizations at risk for data breaches, financial losses, compliance violations, and loss of trust. Responding to advanced threats manually puts stress on fraud and cybersecurity teams and takes their focus away from other security issues.

Stop Advanced Email Threats

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. With Abnormal, you can achieve high-precision protection against all types of email attacks, automate SOC operations, and gain detailed insight into threats that uniquely target your organization.

Email-Based Attacks Lead to Costly Incidents for Financial Services Organizations

25%
Increase in advanced email attacks targeting FinServ organizations year-over-year.

Source: *Abnormal Data*

$2.8B
Total business email compromise losses reported to the FBI in 2024.

Source: *2024 FBI IC3 Report*

17%
Rise in phishing attacks targeting FinServ organizations year-over-year.

Source: *Abnormal Data*

Abnormal for Financial Services

Stop the most dangerous attacks that bypass your existing defenses.

Supply Chain Compromise

When attackers breach trusted vendor email accounts, they can send fraudulent payment requests that make it past your SEG. Every week, your organization faces a 25% chance of a supply chain compromise attack.

How Abnormal Stops Supply Chain Compromise:

Knows your vendors

Abnormal's VendorBase™ automatically identifies your suppliers, vendors, and partners based on past emails and other signals gathered across the enterprise ecosystem.

Continuously monitors your vendors' risk and reputation

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

Analyzes message content, tone, and attachments

Abnormal's AI and ML inspect emails and attachments for suspicious signals to detect supply chain compromise and block the threat from reaching inboxes.

Credential Phishing

Credential phishing represented 80% of advanced email attacks in 2024. Phishing attacks can target general employees, accounting and payroll personnel, or executives, and use social engineering tactics to evade SEG detection

How Abnormal Stops Phishing:

Inspects email headers to expose impersonations

By analyzing header data, Abnormal can determine when an email domain has been spoofed to impersonate a brand, vendor, or specific person.

Detects suspicious language, tone, and style

Even when messages contain no malicious links or attachments, Abnormal recognizes the language that indicates phishing attacks.

Learns communication patterns

Abnormal uses natural language processing to understand people's typical tone, behavior, and communication patterns in order to detect changes that may indicate phishing.

Ransomware

76% of ransomware is delivered via email. 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:

Detects suspicious message signals and credential phishing attempts

Abnormal uses identity detection and natural language processing to spot phishing attempts—even those coming from trusted senders.

Blocks malicious attachments and links

Abnormal reviews all attachments and links for safety, even if those links redirect upon click.

Gives security teams explainable insights and malware forensics

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

Account Takeover

26% of organizations see at least one ATO attempt each week. Once attackers get credentials via phishing, stuffing, or brute force attacks, they can glide past standard security solutions disguised as trusted employees, executives, vendors, or customers.

How Abnormal Stops Compromised Accounts:

Learns good sender behavior with multichannel analysis

API integration with Microsoft 365 and Google Workspace enables analysis of end user behavior, login frequency, devices and browsers used, apps accessed, and other signals.

Continuously monitors behavior and identity

Abnormal 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

Abnormal 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 ›**