Abnormal

Abnormal for Financial Services

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

10x More Effective Solution for Email Security

3x Fewer Attacks Get Through

2x Faster Threat Response Time

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 the Anti-Phishing Working Group (APWG), financial institutions were consistently the most targeted industry for phishing attacks in 2022. Further, financial organizations had a 70% probability of being targeted with a business email compromise (BEC) attack every week last year.

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.

Modern Email Security for the Financial Sector

Abnormal's cloud-native solution quickly integrates with Microsoft 365 and Google Workspace, using thousands of signals across identity, behavior, and content to separate legitimate messages from dangerous threats. Because Abnormal recognizes anomalies even in ongoing conversations, it immediately detects and remediates threats that legacy systems miss—keeping financial institutions safe from attacks.

Email-Based Attacks Lead to Costly Incidents for FinServ Organizations

$5.97MM

Average cost of a data breach in the financial sector in 2022.

Source: IBM Cost of a Data Breach 2022 Report

2,527

Number of successful data compromise attacks targeting the financial sector in 2022.

Source: Verizon 2022 DBIR

$2.4B

Total business email compromise losses reported to the FBI in 2021.

Source: FBI 2021 Internet Crime Report

Abnormal for Financial Services

Stop the most dangerous attacks that bypass your existing defenses.

Credential Phishing

Credential phishing represented 71% of advanced email attacks in 2022. Phishing attacks can target general employees, accounting and payroll personnel, or executives, and use social engineering tactics to evade SEG detection.

How Abnormal Stops Credential Phishing:

Inspects email headers to expose impersonations

Determines when an email domain has been spoofed by analyzing header information.

Detects suspicious language, tone, and style

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

Understands communication patterns

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

Supply Chain Compromise

In supply chain compromise attacks, threat actors impersonate trusted vendors to commit payment fraud and steal sensitive data. The average cost of this type of attack is $183,000, with fake invoices as large as $2.1 million.

How Abnormal Stops Supply Chain Compromise:

Automatically knows your vendors

VendorBase™ auto-identifies suppliers, vendors, and partners via past email conversations and other signals gathered across the enterprise ecosystem.

Continuously monitors vendor risk and reputation

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

Examines message content, tone, and attachments

Uses AI and ML to inspect emails and attachments for suspicious signals that can indicate vendor fraud and block the threat from reaching inboxes.

Ransomware

More than 75% of ransomware is delivered via email. Ransomware attacks can leave companies without the data they need to deliver business-critical services and cause long-term reputational damage.

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 Takeover

A single successful credential phishing email can enable an account takeover, and with a compromised account, attackers can access company email servers, file-sharing platforms, and other business services.

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.

Request Your Abnormal Demo Now:

abnormalsecurity.com/demo →

Abnormal

 v_1.1/Feb_2023