Abnormal

Abnormal for Retail

Discover the AI-based email security platform that protects retailers 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 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.

Criminals Target Retailers for Cardholder Data and Funds

Major retailers have enormous email ecosystems with thousands of employees and vendors and millions of customers. Criminals exploit that complexity to launch email attacks seeking customer data and company funds. Successful attacks that lead to fraud or data breaches can drive customer churn: About 20% of consumers will leave a brand after one bad experience.

Advanced Email Attacks Bypass Traditional Security

Sophisticated credential phishing and vendor email compromise attacks slip through email filters and secure email gateways (SEGs) by posing as messages from trusted senders. As these malicious emails reach employees' inboxes, the risk rises for data breaches, account takeovers, and malware attacks that put customer data at risk.

A Retail Email Security Solution Built to Stop Advanced 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. Because Abnormal can recognize threat indicators in new and ongoing conversations, it can immediately detect and remediate threats that traditional email security solutions won't stop.

A High Risk for Retailers

$183,000
Average cost of a supply chain compromise attack.

81%
Chance of retailers receiving a business email compromise attack each week.

123%
Increase in socially-engineered attacks targeting retailers between 2018 and 2022.*

Source: * Verizon Data Breach Investigations Report

Abnormal for Retail

Stop the most dangerous attacks that bypass your existing defenses.

Account Takeover

Email account takeovers can lead to data breaches, payroll fraud, and invoice fraud. Attackers can also use compromised accounts to spy on email conversations and identify the right time to launch the next stage of their attacks.

How Abnormal Stops Account Takeovers:

Determines good sender behavior with multichannel analysis

Leverages the 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 suspicious 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.

Supply Chain Compromise

52% of email compromise attacks in 2022 used vendor names rather than executive names to dupe victims into wiring funds to scammers, misdirecting payroll deposits, and paying fraudulent invoices.

How Abnormal Stops Supply Chain Compromise:

Knows your vendors

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

Continuously assesses 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 block the threat from reaching inboxes.

Credential Phishing

Phishing reached an "all-time high" of more than 1 million attacks in Q1 2022, and it's still trending upward. Phished credentials are the keys to account takeover and financial supply chain compromise.

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.

Understands 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

76% of ransomware is delivered via email. Ransomware attacks can disrupt business operations and leave retailers without the data they need to operate—not to mention cause significant damage to their reputation.

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.

Provides explainable insights and malware forensics to security teams

Automatically prepares a detailed analysis of ransomware attempts, allowing teams to preview the content of attachments and link targets.

Abnormal

Request Your Abnormal Demo Now:

abnormalsecurity.com/demo →