Abnormal AI for Retail

Discover the AI-native human behavior security platform that protect retailers from the full spectrum of email threats.

$300M In losses prevented by stopping account takeovers

95% Reduction in investigation and response time

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.

Criminals Target Retailers for Cardholder Data and Funds

Large retailers operate vast digital ecosystems with thousands of employees and vendors alongside millions of customers. Threat actors exploit this complexity with email attacks targeting sensitive data or funds. Beyond immediate financial losses, successful breaches and fraud can trigger customer churn, with nearly 25% of consumers abandoning a brand after a single negative experience.

Modern Email Attacks Bypass Traditional Security

Advanced credential phishing and vendor email compromise attacks routinely bypass secure email gateways (SEGs) by masquerading as legitimate communications from trusted partners. When these malicious messages successfully reach employee inboxes, they create immediate pathways to data breaches, account takeovers, and malware infections that directly threaten customer information security.

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.

Email Attack Insights for the Retail Industry

$129,193
Average losses resulting from successful BEC attack

Source: *FBI IC3 Report*

$3.54M
Average cost of a data breach in retail organizations

Source: *IBM Cost of a Data Breach Report 2025*

41%
Retail employee post-read interaction rate with VEC attacks

Source: *Abnormal Internal Data*

Abnormal for Retail

Protect your organization from evolving threats that target human behavior.

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.

Vendor Email Compromise

Retailers have a nearly 80% chance of receiving at least one vendor email compromise (VEC) attack on any given week. In VEC attacks, threat actors impersonate trusted vendors to fulfill fraudulent financial requests.

How Abnormal Stops Vendor Email 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 vendor email compromise and block the threat from reaching inboxes.

Credential Phishing

A successful credential phishing attack grants threat actors access to usernames and passwords that can be leveraged to compromise other accounts and launch additional, more damaging attacks.

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.

Malware & Ransomware

Email remains a primary delivery method for malware and ransomware. These 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 Malware & 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.