Abnormal

Abnormal AI for the Technology Industry

Discover the AI-native human behavior security platform that protects technology companies 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 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.

Breaches Threaten Revenue, Reputation, and More

Cybercriminals prize technology companies for their intellectual property, customer data, and access to downstream supply chains. A single successful attack can trigger cascading consequences—from regulatory penalties and customer churn to compromised partner ecosystems. Meanwhile, threat actors increasingly use AI-powered social engineering to bypass traditional security controls and manipulate employees directly.

Legacy Email Security Leaves Tech Companies Exposed

Technology companies are high-value targets for IP theft and supply chain attacks, yet many rely on legacy email security that can't keep pace with sophisticated threats. Further, manual investigation and remediation processes leave malicious emails active in inboxes longer while pulling security teams away from protecting critical IP, customer data, and development infrastructure.

Stop Social Engineering Attacks with Behavioral AI

Abnormal's platform utilizes machine learning to stop attacks and detect compromised accounts across email and connected applications. The anomaly detection engine leverages identity and context to analyze normal behavior and assess the risk of every cloud email event, detecting and stopping socially engineered attacks that target a tech organization's most valuable cybersecurity asset: its people.

Email Attack Insights for the Technology Industry

$129,193

Average losses resulting from successful BEC attacks

FBI IC3 Report

$4.79M

Average cost of a data breach in tech organizations

IBM Cost of a Data Breach Report 2025

29%

Tech employee post-read interaction rate with VEC attacks

Abnormal Internal Data

Abnormal AI for the Technology Industry

Protect your organization from evolving threats that target human behavior.

Malware & Ransomware

Email remains a primary delivery method for malware and ransomware. These attacks can disrupt business operations and leave tech organizations 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 natural language processing (NLP) to spot first-stage attacks, 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.

Vendor Email Compromise

Tech enterprises have a more than 60% 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:

Automatically Knows Your Vendors

VendorBase™ auto-identifies suppliers, vendors, and partners using past email conversations and other signals gathered across the entire 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.

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 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.

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

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 NLP to understand people's typical tone, behavior, and communication patterns to detect changes that may indicate phishing.

Abnormal

Request Your Abnormal Demo Now: abnormal.ai/demo ›