Abnormal

Abnormal for Manufacturers

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

Outdated Security Puts Manufacturing Processes and Productivity at Risk

Cybercriminals go after manufacturers to steal data, engage in corporate or nation-state espionage, and commit financial fraud. The risks are pervasive: Each company has an 89% chance of experiencing a financial supply chain email attack each week, and there was a 60% increase in the number of business email compromise attacks in 2022.

Advanced Attacks Bypass Legacy Email Solutions

Manufacturers who rely on legacy security solutions like secure email gateways and air gaps to defend OT/ICS systems face elevated risks. Advanced email attacks that are designed to bypass legacy systems can lead to ransomware, operational interruptions, fraud, lost revenue, and compromised data.

Modern Security Shields Manufacturers from 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 recognizes anomalies even in ongoing conversations, it can immediately detect and remediate threats that legacy systems miss, keeping manufacturers safe from attacks.

Real-World Results from an Industrial Manufacturer

30

Hours per week saved on email investigations and remediation.

50

High- and medium-risk vendor accounts identified.

97%

Decrease in daily unsafe user email engagements.

Read the Case Study →

Abnormal for Manufacturers

Stop the most dangerous attacks that bypass your existing defenses.

Supply Chain Compromise

Manufacturers have a 78% chance of receiving a business email compromise attack each week. Successful email compromise attacks can result in invoice fraud, payroll diversion, and other financial crimes.

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.

Ransomware

65% of all industrial ransomware incidents in 2021 targeted manufacturers. Ransomware attacks can have impacts far beyond the plant—disrupting supply chains, jeopardizing partners, and compromising sensitive data.

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 when they come 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.

Account Takeover

Successful credential phishing attacks can lead to takeovers of employee email and file-sharing accounts, with damage ranging from invoice fraud and payroll diversion to data breaches and espionage.

How Abnormal Stops Account Takeover:

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.

Credential Phishing

Phishing attacks made up more than 68% of all advanced email attacks on businesses during H1 2022. When these attacks succeed at stealing employee credentials, they pave the way for ransomware, data breaches, and other 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.

Abnormal

Request Your Abnormal Demo Now:

abnormalsecurity.com/demo →