Abnormal

Abnormal for the Transportation Industry

Discover the AI-based email security platform that protects transportation enterprises 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.

Attacks Put Transportation Providers at Risk for Extortion, Disruption

Ransomware groups, fraudsters, and bad actors seeking to worsen supply chain strains or put the public at risk all target the transportation industry. Increasingly, their weapons of choice are sophisticated email attacks designed to bypass legacy security systems and reach employee inboxes.

Socially-Engineered Threats Overpower Legacy Security Tools

Cybercriminals have learned how to bypass traditional email defenses by hijacking trusted relationships. Impersonating executives, vendors, and well-known brands, today's email threats often look remarkably like legitimate messages—down to the branding details and executive signatures.

Modern Email Security for the Transportation Sector

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 immediately detects and remediates threats that legacy systems miss—keeping transportation enterprises secure and on course.

Costly Email-Based Attacks Targeting Transportation Enterprises on the Rise

$1.29 billion

Total ransomware payments made via cryptocurrency by businesses in past two years.

Source: Chainalysis

186%

Increase in weekly ransomware attacks on the transportation industry in past two years.

Source: Security Intelligence

400%

Increase in maritime transportation cyber attacks since 2020.

Source: Nextgov

Abnormal for the Transportation Industry

Stop the most dangerous attacks that bypass your existing defenses.

Credential Phishing

Nearly 70% of email-based attacks involve credential phishing, with threat actors often impersonating a service provider or a social network. When a recipient takes the bait, ransomware, data breaches, and financial fraud can follow.

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

As security teams train employees to beware of business email compromise (BEC), attackers are expanding their BEC playbook to include vendors. In 2022, 52% of BEC attacks impersonated third parties rather than executives.

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

Ransomware is the main concern for many transportation enterprises, including 45% of port and terminal executives in the United States. Transportation disruptions caused by ransomware can have serious negative impacts on businesses, government services, consumer safety, and the wider economy.

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.

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

Once attackers acquire login credentials, they can use the compromised account to glide past standard security solutions, 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 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 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_1.0/Dec_2022