Abnormal

Abnormal for the Energy & Infrastructure Industries

Discover the AI-based email security platform that protects energy and infrastructure organizations 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.

Energy and Infrastructure are High-Stakes Targets

Pipelines, water treatment facilities, utility grids, and power plants are routinely targeted by ransomware groups, BEC actors, and other cybercriminals seeking to shut down, disrupt, or hijack critical operational technologies. Increasingly, these attacks arrive packaged as emails designed to evade standard security solutions.

Traditional Tools are No Match for New Threats

Traditional email security tools can't detect today's socially-engineered attacks. That creates risks that multiply when IT and OT converge. An email threat that in the past wouldn't have affected operations at all can now have far-reaching consequences for production, distribution, and safety.

Advanced Email Security for Energy and Infrastructure Providers

Abnormal's cloud-based solution integrates with Microsoft 365 and Google Workspace in minutes to analyze thousands of signals across identity, behavior, and content and then separate legitimate messages from threats. Because Abnormal can spot anomalies in ongoing conversations, it detects and remediates threats that legacy systems miss—keeping energy and infrastructure organizations safe and operational.

Email-Based Attacks Threaten Operations and Public Safety

30%

Portion of critical infrastructure enterprises forecasted to experience a major security breach by 2025.

Source: Gartner Newsroom

3,900%

Increase in cyberattacks on critical infrastructure organizations from 2013 through 2020.

Source: Gartner Insights

4.35M

Average cost of a data breach in 2022.

Source: Cost of a Data Breach 2022 Report

Abnormal for the Energy & Infrastructure Industries

Stop the most dangerous attacks that bypass your existing defenses.

Credential Phishing

Credential phishing may have led to the Colonial Pipeline ransomware attack in 2021. That attack cost the company close to $5 million in ransom—only some of which was recovered by law enforcement.

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

Supply chain attack emails impersonate trusted vendors to commit invoice fraud and other financial fraud. The average cost of this type of attack is $183,000, with fake invoices as large as $2.1 million.

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 represented 25% of attacks on energy enterprises in 2021, while phishing was the most-used method for breaching energy networks. Victims may pay expensive ransoms for decryption tools that may not work—and they're often targeted again within months.

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

Account takeovers enabled by credential harvesting and brute-force attacks can lead to data breaches, ransomware attacks, and potentially dangerous real-world consequences. One Florida city's water treatment plant was targeted by a sabotage attempt in 2021 via account takeover.

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