Abnormal

Abnormal for the Technology Industry

Discover the AI-based email security platform that protects technology companies 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.

Sophisticated Attacks Cause Long-Term Damage

Cybercriminals target technology companies for their data, their funds, and their connections to vendors, partners, and customers. Just one successful attack can have serious and costly consequences for operations, brand reputation, privacy compliance, customer trust, and partner and vendor relationships. And threat actors are becoming more sophisticated, using social engineering to bypass security solutions and trick end users.

Manual Remediation is Time-Consuming and Increases Risk

Tech companies that rely on legacy solutions may find that as attacks increase in complexity, they're spending more time and money on manual email investigations and remediation. These manual processes are often slow and painstaking, allowing threats to sit in inboxes longer and pulling security resources away from other critical initiatives.

Effective, Automated Security for Tech Companies

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 threat indicators in new and ongoing conversations, it immediately detects and remediates threats that legacy solutions miss—eliminating the need for time-consuming manual review.

Email-Based Attacks Lead to Costly Incidents for Tech Companies

$4.97M

Average cost of a data breach in the tech industry.

Source: 2022 IBM Cost of a Data Breach Report

77%

Chance of a tech company receiving a business email compromise attack each week.

Source: H2 2022 Email Threat Report

$2.4B

Business email compromise losses reported to the FBI in 2021.

Source: 2021 FBI IC3 Report

Abnormal for the Technology Industry

Stop the most dangerous attacks that bypass your existing defenses.

Ransomware

More than 75% of ransomware is delivered via email. Ransomware attacks can leave companies without the data they need to deliver business-critical services and cause long-term reputational damage.

How Abnormal Stops 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.

Supply Chain Compromise

Over half of business email compromise attacks in 2022 involved the impersonation of external third parties. Known as supply chain compromise, these attacks can lead to invoice and payment fraud, data breaches, and more.

How Abnormal Stops Supply Chain 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

Once attackers complete a successful credential phishing attack, they can use the compromised account to access company email servers, file-sharing platforms, and other business services. If employees use the same credentials for multiple accounts, the damage can be even more extensive.

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

Credential phishing attacks are the most common advanced email threat technology companies face. Attackers impersonate employees, trusted third parties, and well-known brands to steal login credentials to access sensitive data, divert funds, and more.

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:

abnormalsecurity.com/demo →