Abnormal

Abnormal for the Legal Industry

Discover the AI-based email security platform that protects law firms 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.

Outdated Security Endangers Data, Funds, and Trust

Law firms must safeguard sensitive client information, their own financial and operational data, and their reputations. Criminals target legal organizations for this data, launching increasingly sophisticated email attacks that are difficult to detect. A single successful attack can cause data exposure, financial losses, legal liability, and erosion of trust.

Sophisticated Attacks Bypass Legacy Solutions

Firms with legacy security tools face heightened risk from modern email attacks designed to evade them. As law offices move data and processes to the cloud, these solutions become even less effective because they're designed for on-premises email rather than cloud environments.

Modern Security to Protect Law Firms 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 threat indicators in new and ongoing conversations, it immediately detects and remediates threats that secure email gateways miss.

Email-Based Attacks Lead to Costly Incidents

35%

Percentage of large law firms that have experienced a data breach.[1]

$4.35M

Average cost of a data breach in 2022.[2]

$2.4B

Total business email compromise (BEC) losses reported to the FBI in 2021.[3]

Sources: [1] ABA TechReport 2021, [2] Cost of a Data Breach 2022 Report, [3] 2021 FBI IC3 Report

Abnormal for the Legal Industry

Stop the most dangerous attacks that bypass your existing defenses.

Supply Chain Compromise

More than half of business email compromise attacks involve the impersonation of external third parties. Known as supply chain compromise, these attacks can lead to invoice and payment fraud.

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 your vendors' risk and reputation

Assigns each vendor a risk score based on domains spoofed, accounts compromised, and suspicious business.

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

Email is a major vector for ransomware that can encrypt, corrupt, and expose client data. Nearly 30% of law firms have reported malware infections, and 32% don't know whether they've been infected.

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 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.

Account Takeover

One in four law firms have reported data breaches. Account takeovers enabled by credential phishing are a common precursor to breaches because once attackers have gained access to a firm's systems, they can find and exfiltrate sensitive data.

How Abnormal Stops Account Takeovers:

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 emails are often the first step in business email compromise and supply chain compromise. By impersonating a trusted party, attackers can trick recipients into sharing credentials for SharePoint, DocuSign, and other enterprise applications.

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.

Abnormal

Request Your Abnormal Demo Now:

abnormalsecurity.com/demo →