Abnormal

Abnormal for the Hospitality Industry

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

Hospitality Industry Targeted for Valuable Data

Threat actors know that hotels, resorts, and other hospitality businesses have troves of personally identifiable information (PII) on guests—such as passport numbers and dates of travel as well as cardholder data and other financial details. This information makes hospitality organizations an ongoing target for attackers.

Complex Ecosystems Require New Security Strategies

Hospitality employees are always ready to help. Criminals exploit that impulse with socially-engineered attacks that evade secure email gateways and traditional tools. One hotel chain found that even layering two SEGs didn't stop advanced threats such as credential phishing and invoice fraud.

Modern Email Security for the Hospitality Industry

Abnormal's cloud-native solution quickly integrates with Microsoft 365 and Google Workspace, using thousands of signals across identity, behavior, and content to separate legitimate messages from dangerous threats. Because Abnormal recognizes anomalies even in ongoing conversations, it instantly detects and remediates advanced threats to protect hotels, resorts, their guests, and their vendors.

Abnormal Protects Leading Lodging Franchisor from Advanced Threats

36%

Reduction in IT response efforts needed to address email threats during peak booking season.

120+

Compromised vendor email accounts detected by Abnormal VendorBase™

97

Email attacks stopped on average each day.

Read the Case Study →

Abnormal for the Hospitality Industry

Stop the most dangerous attacks that bypass your existing defenses.

Credential Phishing

Credential harvesting and phishing attacks comprised 59% of advanced email threats targeting hospitality and retail from May through August 2022. These attacks often impersonate company executives and vendors to manipulate employees' helpfulness and trust.

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

Because hotel and other hospitality enterprises have thousands of vendors, attackers often impersonate them to commit invoice and payment fraud or to capture login credentials for access to sensitive data.

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

More than 75% of ransomware is delivered via email. Ransomware attacks can cause costly, brand-damaging business interruptions, especially when reservation data is affected by an attack.

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

A single successful credential phishing email can enable an account takeover, and with a compromised account, attackers can expose PII about guests, internal financial data, and vendor contacts.

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