Abnormal

Abnormal for the NHS

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

Email Attacks Threaten Patient Data and Safety

The NHS is a magnet for cybercriminals, with 81% of organisations across the UK suffering a ransomware attack in the past year. NHS data claims that 21 million instances of malicious activity are blocked every month, yet 64% of organisations still had to cancel face-to-face appointments due to attacks. A further 65% stated that a cyberattack could cost lives.

Advanced Attacks Evade Traditional Email Defences

Advanced email threats like sophisticated credential phishing attacks and business email compromise are designed to bypass secure email gateways and traditional security tools. The result is more malicious emails in employees' inboxes, and an increased risk of data breaches, account takeovers, and ransomware attacks that endanger patient privacy and safety.

A Modern Approach to NHS Email Security

Abnormal's cloud-native solution integrates with Microsoft 365 and Google Workspace in minutes and uses thousands of signals across identity, behaviour, and content to separate legitimate messages from dangerous threats. Because Abnormal recognises threat indicators in new and ongoing conversations, it immediately detects and remediates threats that legacy systems miss.

Real-World Results for Healthcare Organisation

64

Employee hours saved per month on email assessment and remediation.

4,600

Graymail and spam messages missed by existing SEG but stopped by Abnormal.

$125k

Annual savings by decommissioning SEG.

Read the Case Study →

Abnormal for the NHS

Stop the most dangerous attacks that bypass your existing defences.

Supply Chain Compromise

Threat actors impersonate trusted third parties in 52% of business email compromise attacks. Known as supply chain compromise, these attacks can lead to costly invoice and payment fraud. Cyber-related fraud costs the NHS an estimated £400 million each year.

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.

Credential Phishing

Credential phishing accounted for 58% of all NHS cybersecurity incidents between January and March 2022. Attackers impersonate trusted parties and well-known brands via email to steal login credentials to access sensitive data and launch additional attacks.

How Abnormal Stops Credential Phishing:

Inspects email headers to expose impersonations

Determines when an email domain has been spoofed by analysing header information.

Detects suspicious language, tone, and style

Recognises 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, behaviour, and communication patterns to detect changes that may indicate phishing.

Ransomware

More than 80% of NHS organisations experienced a ransomware attack in 2021. These attacks can encrypt, corrupt, and expose sensitive data as well as disrupt NHS operations, which can lead to delayed response times for vital emergency care across the UK.

How Abnormal Stops Ransomware:

Analyses message content and other signals for credential phishing

Utilises 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.

Account Takeover

Between 2020 and 2021, account takeovers in the UK increased by 288%. Once attackers acquire login credentials, they can bypass standard security solutions, disguised as trusted employees, executives, vendors, or customers.

How Abnormal Stops Account Takeover:

Determines good sender behaviour with multichannel analysis

Leverages API integration with Microsoft 365 and Google Workspace to analyse end-user behaviour across devices, browsers, and apps.

Actively monitors user behaviour 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:

Abnormal

abnormalsecurity.com/demo →