Abnormal

Abnormal for Federal Government

Discover the AI-based email security platform that protects federal governments from the full spectrum of email attacks.

$300M in losses prevented by stopping account takeovers.

95% reduction in investigations and response times.

15+ hours saved for security teams each week through AI automation.

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.

Attackers Target Government Agencies for Valuable Data

Threat actors know that federal governments have troves of data and access to critical operational processes. Unfortunately, they're also aware that these organizations often don't have enterprise-level security tools to keep them out. The result is an ongoing wave of disruptive, costly incidents involving city, county, state, and federal agencies.

Legacy Security Tools Can't Block Advanced Threats

Traditional email security tools like secure email gateways aren't designed to detect advanced socially-engineered attacks. Modern threat actors exploit common psychological vulnerabilities as well as trusted names and relationships to trick or pressure recipients into sharing information, downloading malware, or transferring funds.

Modern Email Security for Federal Governments

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 anomalies even in ongoing conversations, it immediately detects and remediates threats that legacy systems miss—keeping governments secure and operational.

Email-Based Attacks Lead to Costly Incidents for Federal Governments

360%

Increase in phishing attacks on government agencies in 2024.

Source: *Abnormal Data, 2024*

$12.5M

Cost of ransomware payments in 2024.

Source: *2024 FBI IC3 Report*

$2.8B

Total business email compromise losses reported to the FBI in 2024.

Source: *2024 FBI IC3 Report*

Abnormal for Federal Government

Stop the most dangerous attacks that bypass your existing defenses.

Ransomware

In 2024, Central & Federal Government was among the top three industries targeted by ransomware. These attacks can disrupt educational facilities, emergency services, critical utilities, and other government-run services.

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 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.

Supply Chain Compromise

Because federal government agencies often share details of their current and past contracts on their websites, it's easy for attackers to gather the information they need to impersonate vendors via email to commit invoice and payment fraud.

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.

Credential Phishing

Credential phishing attacks are the most common advanced email threat government agencies face. Attackers impersonate trusted parties and well-known brands 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 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.

Account Takeover

After a successful credential phishing attack, attackers can use compromised accounts to steal private information about citizens and sensitive public safety data, commit financial fraud, launch ransomware attacks, and more.

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.

Abnormal

Request Your Abnormal Demo Now: **abnormal.ai/demo ›**