Abnormal AI for Federal Government

Behavioral AI that stops phishing, impersonation, and vendor fraud targeting federal agency workflows. Deployed via API in minutes, with no MX changes required, and backed by FedRAMP Moderate authorization.

$300M+ In losses prevented by stopping account takeovers and fraud

95% Reduction in investigation and response times

15+hrs Saved for security teams each week through AI automation

Abnormal Overview

- Behavioral Security Platform that uses Behavioral AI to protect against BEC, impersonation, advanced phishing, vendor fraud, account takeover, and unwanted mail.
- API-based solution integrates with Microsoft 365 and Google Workspace in minutes.
- Behavioral AI learns normal identity, relationship, and communication patterns to detect deviations that rules-based defenses miss.

What Sets Abnormal Apart

- No disruption to mail flow and no changes to MX records required.
- FedRAMP Moderate authorized, built for federal deployment.
- Protection against internal and external account compromise.
- Autonomous triage, investigation, and remediation reduce manual SOC work.

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

Federal agencies are targeted as much for how they operate as for the data they hold. Public procurement records, org charts, and vendor contracts can give attackers the context they need to impersonate known contractors or senior leaders and build attacks around the routine workflows federal agencies rely on every day.

Legacy Security Tools Can't Block Advanced Threats

Secure email gateways aren't built to catch socially engineered attacks. Modern threat actors exploit trusted names, familiar relationships, and routine workflows, such as a document share or a vendor invoice, to pressure recipients into sharing information, downloading malware, or transferring funds.

Modern Email Security for Federal Agencies

Abnormal's Behavioral Security Platform 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 inside ongoing conversations, it detects and remediates threats that legacy systems miss. The platform is FedRAMP Moderate authorized, aligning with Executive Order 14390's emphasis on hardening financial and digital systems and drawing on commercial cybersecurity capabilities against cyber-enabled fraud.

Cybercrime Creates Significant Financial Risk

40.8%

Billing account update fraud accounts for 40.8% of vendor email compromise (VEC) targeting government agencies, the highest share of any industry and nearly double the 23.6% sample average

Source: 2026 Attack Landscape Report

$32.3M

Ransomware losses reported to the FBI in 2025, up from $12.5M the year before

Source: 2025 FBI Internet Crime Report

$3.05B

Total business email compromise losses reported to the FBI in 2025

Source: 2025 FBI Internet Crime Report

Abnormal AI for Federal Government

▸▸ Stop the most dangerous attacks that bypass your existing defenses.

Ransomware

Ransomware remains a significant threat to government operations, disrupting emergency services, critical utilities, educational facilities, and other public services. Phishing emails, malicious links, and attachments can provide attackers with an initial foothold, making prevention at the inbox an important layer of defense.

How Abnormal Helps Stop Ransomware:

- Combines behavioral and content analysis to detect and remediate phishing and malicious payloads before users engage.
- Analyzes links and attachments, including redirects, for malicious behavior.
- Automatically remediates malicious messages and gives security teams explainable threat context for investigation.

Vendor Email Compromise

Federal agencies often publish contract details publicly, giving attackers the context they need to impersonate a real vendor and request a change to payment details. Billing account update fraud accounts for 40.8% of vendor email compromise targeting government agencies, the highest share of any industry and nearly double the sample average.

How Abnormal Stops Vendor Email Compromise:

- 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, assigning each vendor a risk score based on domains spoofed, accounts compromised, and suspicious messages across Abnormal's federated network of customers.
- Examines message content, tone, and attachments to spot signals of vendor fraud and block the threat from reaching inboxes.

VIP Impersonation

Federal agencies are large and dispersed, so many employees never interact directly with senior leadership, and a message that appears to come from the front office is more likely to get a fast response than a careful look. More than 41% of internal impersonation BEC reaching executives involves VIP impersonation, about five times the sample average.

How Abnormal Stops VIP Impersonation:

- Builds behavioral baselines for every identity, including executives, based on how they normally write and communicate.
- Correlates sender identity, communication history, and timing to flag messages that deviate from known patterns.
- Evaluates urgency and financial intent alongside identity signals to catch social-engineering attempts before they land.

Credential Phishing

Credential phishing remains a persistent threat to government agencies. Attackers impersonate trusted parties and well-known brands, often through fake document-share notices or Microsoft 365 security alerts, to steal login credentials and access sensitive data.

How Abnormal Stops Credential Phishing:

- Inspects email headers and domains to expose impersonation and spoofing attempts other tools miss.
- Detects suspicious language, tone, and style, recognizing phishing attempts even without malicious links or attachments.
- Baselines each person's typical communication patterns to flag deviations that may indicate phishing.

Abnormal

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