Abnormal

AI-Powered Protection Against Fraud and Waste

Safeguard federal funds with intelligent email threat prevention.

As fraud, waste, and abuse attract heightened federal oversight, email continues to serve as a primary entry point for advanced cyberattacks targeting federal systems. Breaches driven by phishing, business email compromise (BEC), and vendor fraud have already led to serious operational and national security consequences.

In an era of digital transformation, zero-trust mandates, and evolving geopolitical threats, federal agencies must adopt proactive email security measures that go beyond static rules and traditional secure email gateways. The strategic use of AI to detect and stop socially engineered attacks before they reach the inbox is no longer optional—it's essential to protect public funds, national security, and the integrity of mission-critical operations. Forward-leaning federal cybersecurity leaders are deploying AI-native defenses to prevent invoice fraud, impersonation of trusted contractors, and insider compromise—ensuring taxpayer dollars are secured, not stolen.

360% Increase in phishing attacks on government agencies in 2024.
Abnormal Data, 2024

$1B Safeguarded from vendor fraud by Abnormal AI.
Abnormal R&D Data, 2025

94% Improvement in security efficacy by switching to Abnormal.
Abnormal Data, 2025

Abnormal provides the solution for federal governments.

Uses behavioral AI to understand normal communication patterns across government employees and vendors, flagging anomalies like tone shifts, new bank requests, or impersonation attempts.

Automatically profiles users and vendors to detect behavioral changes that signal risk—helping agencies spot compromise without manual effort.

Removes malicious emails in milliseconds, moving them to a hidden folder before employees can engage, preventing financial loss from fraud or account takeover.

Fully automates email triage, remediation, and reporting, bringing together all auto-detected and user-reported threats into a single interface.

Clears graymail and distractions from the inbox, helping teams stay focused on mission-critical work without manual filtering.

The Abnormal Advantage at a Glance

Full spectrum protection. Blocks the malicious and unwanted emails that bypass other solutions, including never-seen-before attacks that do not contain traditional indicators of compromise.

Stops account takeovers. Detects internal and external compromised accounts and remediates them based on your preferences.

Increases efficiency. Improves employee and executive productivity with adaptive protection.

Deploys in minutes. No rules, policies, or configuration needed. Abnormal integrates via API in only three clicks.