Abnormal

Never Trust. Always Verify. Especially in Email.

AI-Driven Email Security for the Department of War

Email remains the most targeted and exploited communication channel across the Department of War. Modern adversaries rely on socially-engineered attacks that exploit trust by impersonating commanders, mission partners, and vendors rather than deploying malware. These attacks routinely bypass traditional secure email gateways (SEGs) and place mission assurance at risk.

Why Email Represents a Mission Risk

Identity-based email attacks such as business email compromise and credential phishing are among the most damaging cyber threats facing government organizations. Email is targeted because it enables access, authority, and lateral movement across operational environments.

Why Legacy Secure Email Gateways Are Not Enough

Traditional secure email gateways focus on known indicators such as malware signatures, URLs, and sender reputation. While necessary, these controls are not designed to evaluate intent, behavior, or abuse of trusted identities—allowing impersonation, account compromise, and lateral phishing to evade detection.

An API-Based Behavioral Layer That Increases SEG Effectiveness

Abnormal AI operates as an API-based behavioral intelligence layer that integrates directly with existing email platforms and security controls. Rather than replacing secure email gateways, Abnormal AI augments them, enhancing detection of socially-engineered threats without introducing mail flow disruption, latency, or additional tuning burden.

360%

increase in phishing activity targeting government organizations

Abnormal Internal Data

$2.8B

in business email compromise losses reported in 2024

FBI IC3

Advancing DoW Zero Trust Objectives

Zero Trust strategy assumes threats exist both inside and outside the network and requires continuous verification of identity and behavior. Email is the most widely used identity-driven system in the DoW and one of the least continuously verified attack surfaces.

Mission Outcomes Aligned to DoW Priorities

- Continuous verification of identity and behavior at the email layer
- Improved enterprise visibility and analytics into trust-based threats
- Automation and orchestration that reduce analyst workload and response time
- Increased resilience against insider threat and lateral movement
- Enhanced mission assurance without disrupting operations

Designed to Integrate Without Disruption

- API-based deployment that integrates with existing email platforms and security controls
- No inline mail-flow changes or MX record modifications required
- Augments secure email gateways to improve overall detection efficacy
- Reduces policy sprawl, rule maintenance, and tuning overhead
- Scales across large, distributed, and federated DoW environments

Operational Benefits for Cyber and Mission Teams

- Reduces alert volume by filtering low-value and false-positive email events
- Automates detection and response for socially-engineered threats
- Enables analysts to focus on proactive defense and threat hunting
- Improves response speed for identity-based and trust-abuse attacks
- Strengthens confidence in trusted communications across the enterprise

> Zero Trust assumes threats can exist both inside and outside the network and therefore requires continuous verification of every user and device attempting access."
>
> — Department of the Navy CIO

Abnormal AI is not simply another security product. It is an operational enabler that strengthens Zero Trust, improves the effectiveness of existing defenses, and protects the missions that depend on trusted communications.

Abnormal