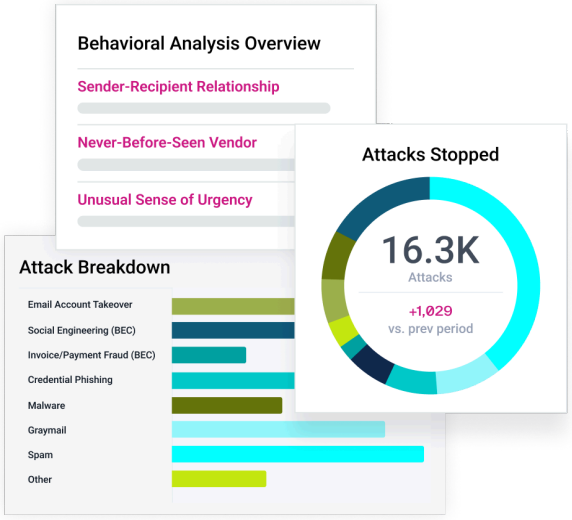
Abnormal

Abnormal AI for Government

Security and Compliance Overview

Abnormal AI for Government delivers AI-native human behavior security to federal and regulated public sector environments, protecting against socially engineered threats across email and connected cloud applications. The controls below define how Abnormal's FedRAMP-authorized environment is secured and operated.



Security and Compliance Controls

Identity and Access Management
Phishing-resistant, FIPS-compliant YubiKey 5C authentication with SAML SSO and PIV/CAC integration, leveraging established identity and MFA controls within an IDaaS Gov Cloud environment.

Encryption and Data Protection
TLS 1.2+ and FIPS 140-2+ validated cryptography, with AES-256 encryption at rest via AWS KMS (SSE-KMS) across RDS, S3, and EBS.

Data Storage and Retention
Customer-authorized, least-privilege API ingestion with strict per-tenant data isolation and behavioral baselines enforced.

Logging and Monitoring
Centralized audit logging to internal SIEM for continuous monitoring and incident response, with export to customer-managed SIEM platforms.

Incident Response and Remediation
Dedicated Government IR team with annual testing exercises and defined vulnerability SLAs: Critical 15 days, High 30 days, Moderate 90 days, Low 180 days.

FedRAMP and Government Deployment

- Dedicated Government tenant with all model processing confined within the FedRAMP authorization boundary
- Hosted exclusively in AWS GovCloud; mapped to NIST SP 800-53 Rev. 5
- Compatible with Microsoft GCC High to support CMMC Level 2 and CUI
- 98% assessment score with zero high findings
- GenAI operates only on sanitized metadata; per-tenant behavioral baselines enforce strict data isolation

See Abnormal in action. **Request a demo.** abnormal.ai ›