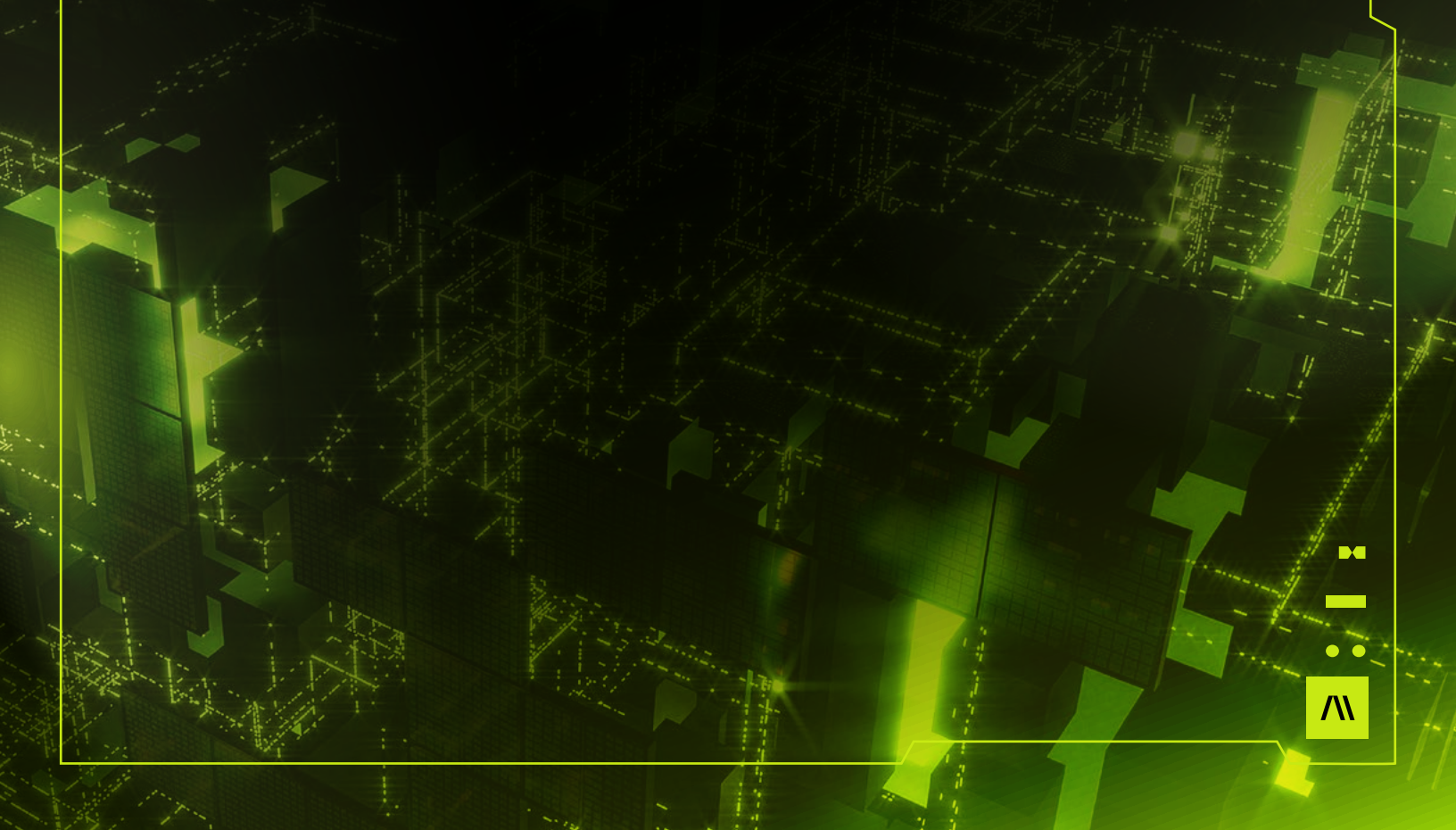
Abnormal

CMMC LEVEL 2

How Abnormal AI Supports CMMC Compliance for Defense Industrial Base Contractors

ABNORMAL AI · FEDERAL SALES



Executive Summary

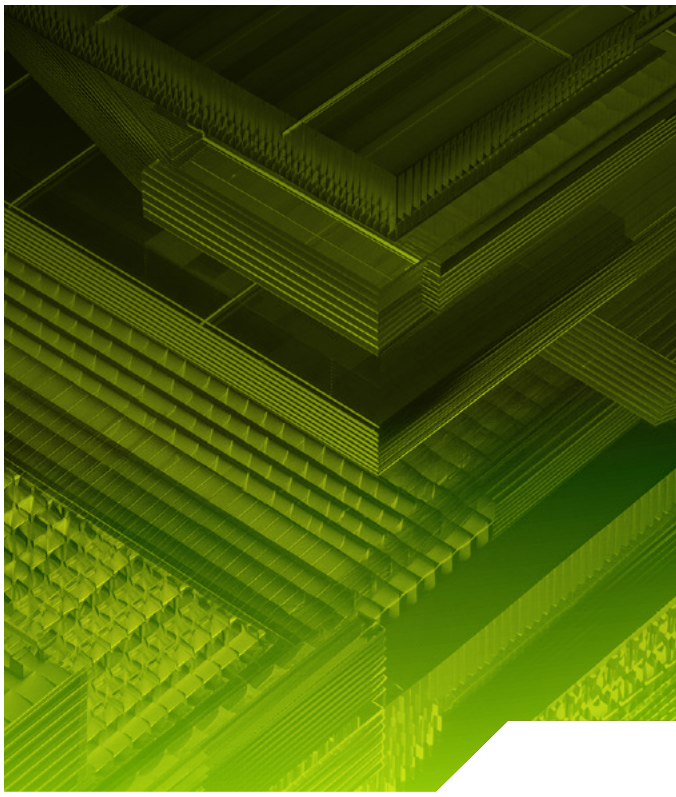
Nation-state adversaries have fundamentally changed how they conduct cyber operations. AI has removed the friction from targeted attack campaigns: adversaries can now profile thousands of individuals, craft contextually convincing spearphishing emails at scale, and execute multi-stage intrusions that generate no malware signature and evade rule-based detection.

For Defense Industrial Base (DIB) contractors, this is not a theoretical risk. Volt Typhoon,[1] APT40,[2] APT41,[3] and Sandworm[4] are documented to be targeting cleared personnel, defense contractors, and critical infrastructure operators with campaigns designed to bypass conventional email security.

This whitepaper maps Abnormal AI's product portfolio to 32 practices in National Institute of Standards and Technology's Special Publication 800-171 Rev. 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (NIST SP 800-171 Rev. 2) where Abnormal provides support for CMMC Level 2 compliance. Abnormal supports practices across ten CMMC domains, including Incident Response, Audit and Accountability, Identification and Authentication, System and Information Integrity, and more.

Abnormal does not replace a complete CMMC compliance program. Organizations must implement controls across all applicable systems and domains. What Abnormal provides is AI-native, behavioral detection and response for the email and identity attack surface—a primary initial access vector for major federal breaches.

This whitepaper describes Abnormal AI's commercial product capabilities. Abnormal's GovCloud environment is purpose-built for federal and Defense Industrial Base customers, and certain features, integrations, and capabilities may differ from those described here. Please contact Abnormal AI's federal sales team for details on GovCloud-specific capabilities and compliance authorizations.



Addressing nation-state-level threats to Controlled Unclassified Information (CUI) requires detection capabilities that go beyond signature-based filtering. It requires behavioral AI on defense.

[1] Cybersecurity and Infrastructure Security Agency, PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure, February 7, 2024.

[2] https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-200a

[3] U.S. Department of Justice, *Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally*, September 16, 2020

[4] Cybersecurity and Infrastructure Security Agency, *Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*, May 9, 2022.

The Threat Landscape: AI Has Changed the Equation

Nation-State Adversaries Are Using AI to Attack

Modern adversarial campaigns against DIB contractors share a common characteristic: they look legitimate. AI has made it possible for threat actors to generate spearphishing emails that reference actual projects, actual colleagues, and actual operational context. These messages carry no payload. They contain no malicious links. They use correct grammar and precise terminology. Legacy secure email gateway controls were not designed to detect attacks that look legitimate on every measurable surface.

Three threat actor groups are most active against the DIB:

- **Volt Typhoon (PRC-linked)** — targets maritime, aviation, defense logistics, and operational networks. Specializes in living-off-the-land techniques that produce no malware signature, and pre-positions inside critical infrastructure for potential activation.
- **APT40 and APT41 (PRC-linked)** — APT40 targets maritime and defense sectors; APT41 runs parallel espionage and financially motivated campaigns.[5] Both have extensively targeted cleared personnel and defense contractors.
- **Sandworm (Russian GRU)** — responsible for the most destructive cyberattacks in recorded history (NotPetya, Ukraine power grid attacks). Actively targets NATO-adjacent defense networks and critical infrastructure.

Why Conventional Email Security Fails

Secure email gateways were designed for a different threat model: block known-bad domains, scan attachments for malware signatures, and filter bulk phishing runs. Against an AI-generated spearphishing email from a legitimate-looking sender address, with no attachment and no link, these controls provide limited protection.

The SVR's May 2021 spearphishing campaign against more than 150 organizations—including federal agencies, NGOs, and think tanks—illustrates why this matters.[6] Operating through the legitimate Constant Contact mass-mailing service and spoofing real USAID sender addresses, the attackers delivered malicious payloads from infrastructure that, by every conventional signal, looked authentic. The sender domain matched a legitimate service. The branding matched a real federal agency. Reputation-based filters had nothing to flag. Some of the earlier, lower-volume waves were delivered to recipients before detection rules caught up.[7]

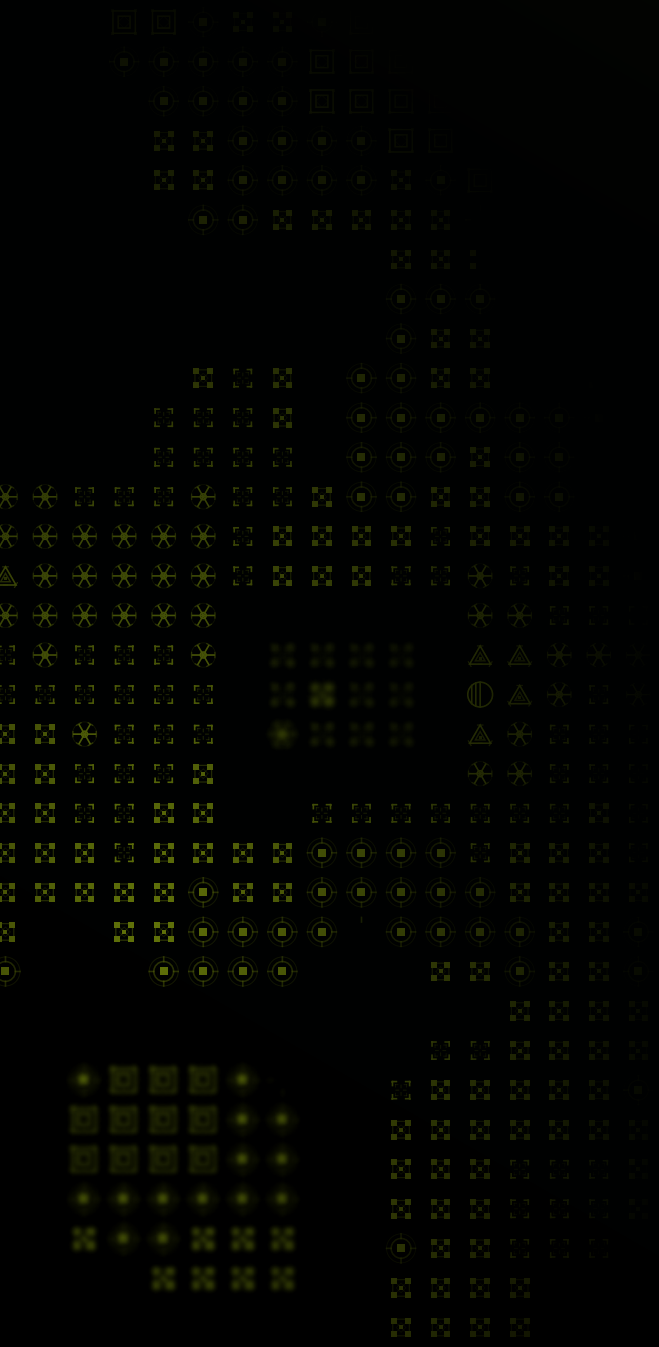
The gap is architectural. Gateway-based filtering evaluates message attributes. Behavioral AI evaluates identity—whether this message, from this sender, to this recipient, at this time, represents normal behavior for the environment. Behavioral AI is uniquely positioned to catch attacks that look legitimate on the surface.

[5] Mandiant, *APT41, A Dual Espionage and Cyber Crime Operation*.

[6] NSA, CISA, and FBI, *Russian SVR Targets U.S. and Allied Networks*, Joint Cybersecurity Advisory, April 15, 2021.

[7] Microsoft Threat Intelligence Center, *New sophisticated email-based attack from NOBELIUM*, May 27, 2021.

The Abnormal Approach: Behavioral AI on Defense



Abnormal AI does not use signatures, rules, or reputation lists. It builds a behavioral baseline of normal activity across identities, vendors, and workflows in the environment and detects deviations that indicate account compromise, impersonation, or fraud. This architecture is effective against AI-generated attacks because it evaluates the sender's behavioral history, not message content.

Abnormal's key capabilities include:

- Inbound email protection against spearphishing, impersonation, business email compromise, vendor fraud using behavioral AI
- Core Account Takeover Protection with session termination, password reset, and MFA anomaly detection
- Security Posture Management for M365 configuration drift, risky admin changes, and compliance validation
- AI Security Mailbox for 24/7 automated triage of user-reported suspicious emails
- AI Phishing Coach for real-time, contextual security awareness training
- Misdirected Email Prevention to reduce inadvertent CUI exposure via misaddressed messages
- IntelBase, PeopleBase, VendorBase, and AppBase for enriched behavioral context
- SIEM/SOAR integrations and Integrated SecOps Case Timelines for audit, investigation, and reporting

CMMC Level 2: What DIB Contractors Must Demonstrate

CMMC Level 2 requires implementation of all 110 security practices from NIST SP 800-171 Rev. 2 across 14 domains. These practices protect Controlled Unclassified Information (CUI) on contractor information systems. Unlike CMMC Level 1 (self-attestation), Level 2 requires third-party assessment for contractors on prioritized acquisition programs.

Email remains one of the most consistently significant attack vectors for federal civilian agencies, ranking among the top reported categories of attack vectors in annual reporting[8] and featured prominently in several major federal breaches.[9] The practices most directly relevant to email-based threats span Incident Response, Audit and Accountability, System and Information Integrity, Identification and Authentication, and Configuration Management.

32 of 110 CMMC Level 2 practices are supported by Abnormal AI products. This document maps each practice to the specific Abnormal capability that contributes to its implementation.

Important Scoping Notes

This matrix reflects how Abnormal AI products contribute to CMMC practice implementation. Organizations should note:

- Abnormal provides detective and preventive controls at the email and identity layer. It does not replace network access controls, endpoint protection, cryptographic controls, or other domains not covered in this matrix.
- CMMC assessors evaluate the totality of an organization's compliance program. Abnormal's contribution is one component of a broader set of required controls.
- CMMC is applicable to Federal Civilian Executive Branch (FCEB) contractors and defense contractors handling Controlled Unclassified Information (CUI). The Office of Management and Budget's Federal Zero Trust Strategy (M-22-09) and the Cybersecurity and Infrastructure Security Agency (CISA) Binding Operational Directives (BODs) apply to federal civilian agencies.

[8] Office of Management and Budget, *Federal Information Security Modernization Act of 2014: Annual Report Fiscal Year 2023*. See also, Office of Management, *Federal Information Security Modernization Act of 2014: Annual Report Fiscal Year 2022.*

[9] "The adversary gained access to OPM's network using credentials stolen from a KeyPoint contractor...It remains unclear precisely how the credentials were stolen from the KeyPoint contractor, but some evidence suggests it may have been the result of a phishing attack." Committee on Oversight and Government Reform, U.S. House of Representatives, The OPM Data Breach: *How the Government Jeopardized Our National Security for More than a Generation*, September 7, 2016.

"The bad actors gained access to PSC's Payment System by using fake grant recipient email addresses to request access. Once they gained access, the bad actors masqueraded as grant recipients and requested account changes such as deleting valid users and changing bank accounts and other account contact information." Department of Health and Human Services, Office of Inspector General, *HHS's Grant Payment System Lacked Effective Internal Controls To Prevent $7.8 Million in Fraud, and HHS Has Begun Taking Corrective Actions To Reduce Fraud Risk*, June 2025.

"The threat actors accessed the official email accounts of many of the most senior U.S. government officials managing our country's relationship with the People's Republic of China." Cyber Safety Review Board, *Review of the Summer 2023 Microsoft Exchange Online Intrusion*, March 20, 2024.

"On February 11, 2025, the OCC learned of unusual interactions between a system administrative account in its office automation environment and OCC user mailboxes." Office of the Comptroller of the Currency, *News Release 2025-30: OCC Notifies Congress of Incident Involving Email System*, April 8, 2025.

CMMC Level 2 Compliance Matrix

The tables below map each supported CMMC Level 2 practice to the Abnormal AI product(s) that contribute to its implementation. Controls where Abnormal provides no coverage are excluded. Practices are organized by CMMC domain.

Access Control

Control ID	Practice Title	Abnormal Product(s)	How Abnormal Supports
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices	**Core Account Takeover Protection**	**Supports** — behavioral monitoring across identity and device signals to detect and flag unauthorized access attempts.
3.1.3	Control the flow of CUI in accordance with approved authorizations	**Misdirected Email Prevention**	**Supports** — designed to prevent wrong-recipient emails to reduce inadvertent CUI exposure across email boundaries.
3.1.8	Limit unsuccessful logon attempts	**Core Account Takeover Protection**	**Supports** — monitors sign-in anomalies and detects brute-force and credential stuffing patterns across identity platforms.
3.1.11	Terminate user sessions automatically after a defined condition	**Core Account Takeover Protection**	**Supports** — designed to automatically block account access, triggers password reset, and signs out all active sessions upon confirmed compromise.
3.1.22	Control CUI posted or processed on publicly accessible systems	**Misdirected Email Prevention**	**Supports** — reduces risk of exposing CUI via misaddressed emails to public domains or unintended external recipients.

Awareness and Training

Control ID	Practice Title	Abnormal Product(s)	How Abnormal Supports
3.2.1	Ensure managers, system administrators, and users are aware of security risks associated with their activities and of the policies, standards, and procedures related to the security of those systems	**Inbound Email Security** **Core Account Takeover Protection** **AI Phishing Coach**	**Supports** — sends explanatory responses to email reporters, improving real-time awareness of active attack techniques. **Supports** — behavioral monitoring of identity and device signals to detect and flag unauthorized access attempts. **Supports** — delivers contextual security awareness feedback to users who report or interact with suspicious emails.
3.2.2	Ensure personnel are trained to carry out their information security duties	**AI Phishing Coach**	**Supports** — provides ongoing automated security awareness training tailored to real threats observed in the environment.
3.2.3	Provide training on recognizing and reporting indicators of insider threat	**AI Security Mailbox** **AI Phishing Coach**	**Supports** — educates users via AI-generated explanations and supports insider-threat reporting workflows.

Audit and Accountability

Control ID	Practice Title	Abnormal Product(s)	How Abnormal Supports
3.3.1	Create and retain audit logs to enable monitoring, analysis, investigation, and reporting	**Abnormal Behavior Platform**	**Supports** — streams email security events to SIEM for retention and monitoring of unauthorized or anomalous activity
3.3.2	Ensure actions of individual users can be uniquely traced for accountability	**Abnormal Behavior Platform**	**Supports** — streams email security events to SIEM with individual event attribution for traceability. **Supports** — case timelines link actions to individual users during security investigations. **Supports** — tracks individual user reporting activity and streams events for audit.
3.3.3	Review and update logged events	**Abnormal Behavior Platform**	**Supports** — enables review of logged events across M365; surfaces configuration and admin activity for audit.
3.3.5	Correlate audit records for investigation and response to unusual activity	**Abnormal Behavior Platform**	**Supports** — behavioral engine correlates signals across email, identity, device, and browser to detect unusual activity. **Supports** — monitors configuration drift and alerts on admin role changes or conditional access exceptions. **Supports** — correlates events across sources for review and investigation of anomalous activity.
3.3.6	Provide audit record reduction and report generation for on-demand analysis	**Abnormal Behavior Platform**	**Supports** — enriches SIEM with Abnormal event data to enable on-demand reporting and analysis.

Configuration Management

Control ID	Practice Title	Abnormal Product(s)	How Abnormal Supports
3.4.1	Establish and maintain baseline configurations and inventories of organizational systems	**Security Posture Management (M365)**	**Supports** — provides visibility into baseline configuration changes across M365 users, applications, and tenants.
3.4.3	Track, review, approve or disapprove, and log changes to organizational systems	**Security Posture Management (M365)**	**Supports** — logs configuration changes and provides workflows for acknowledging and acting on detected changes.
3.4.4	Analyze the security impact of changes prior to implementation	**Security Posture Management (M365)**	**Supports** — highlights high-risk configuration changes to enable security impact analysis prior to remediation.
3.4.6	Employ the principle of least functionality by configuring systems to provide only essential capabilities	**Security Posture Management (M365)**	**Supports** — identifies over-permissive configurations across M365 that violate least-privilege principles.

Identification and Authentication

Control ID	Practice Title	Abnormal Product(s)	How Abnormal Supports
3.5.1	Identify system users, processes acting on behalf of users, and devices	**Core Account Takeover Protection** **Abnormal for Okta**	**Supports** — monitors identity and device signals to detect and flag unauthorized system access patterns and misuse. **Supports** — detects unusual Okta sign-in patterns and supports one-click and automated remediation of compromised accounts.

Incident Response

Control ID	Practice Title	Abnormal Product(s)	How Abnormal Supports
3.6.1	Establish an operational incident-handling capability including preparation, detection, containment, and recovery	**AI Security Mailbox** **Abnormal Behavior Platform**	**Supports** — provides 24/7 AI triage of user-reported emails, supporting detection, analysis, and containment workflows. **Supports** — centralizes evidence and event timelines to aid investigation, recovery, and case documentation.
3.6.2	Track, document, and report incidents to designated officials and authorities	**AI Security Mailbox** **Abnormal Behavior Platform**	**Supports** — centralizes user-reported incidents and documents automated response actions for stakeholder review. **Supports** — exports alerts and events to SIEM/SOAR platforms to support incident tracking and reporting.
3.6.3	Test the organizational incident response capability	**AI Phishing Coach**	**Supports** — deploys incident response exercises via phishing simulation handling and automated security awareness training delivery.

Risk Assessment

Control ID	Practice Title	Abnormal Product(s)	How Abnormal Supports
3.11.1	Periodically assess risk to organizational operations, assets, and individuals	**Security Posture Management (M365)**	**Supports** — assesses posture risk by surfacing misconfigurations and risky role changes across M365.

Security Assessment

Control ID	Practice Title	Abnormal Product(s)	How Abnormal Supports
3.12.1	Periodically assess the security controls in organizational systems to determine effectiveness	**Security Posture Management (M365)**	**Supports** — continuous validation of identity, email, and configuration controls to verify that required settings remain effective.
3.12.3	Monitor security controls on an ongoing basis to ensure continued effectiveness	**Security Posture Management (M365)**	**Supports** — continuously monitors configurations and control drift, alerting when deviations from baseline occur.

System and Communications Protection

Control ID	Practice Title	Abnormal Product(s)	How Abnormal Supports
3.13.1	Monitor, control, and protect communications at the external and internal boundaries of organizational systems	**Inbound Email Security** **Account Takeover Protection**	**Supports** — protects email communications at the organizational boundary; stops phishing, BEC, and vendor fraud before user interaction. **Supports** — designed to automatically block account access, trigger password reset, and sign out all active sessions upon confirmed compromise.
3.13.4	Prevent unauthorized and unintended information transfer via shared system resources	**Misdirected Email Prevention**	**Supports** — designed to block misaddressed or mis-attached emails containing sensitive data, preventing inadvertent information transfer.

System and Information Integrity

Control ID	Practice Title	Abnormal Product(s)	How Abnormal Supports
3.14.1	Identify, report, and correct system flaws in a timely manner	**Security Posture Management (M365)**	**Supports** — continuously surfaces risky misconfigurations and provides guided remediation to correct identified flaws.
3.14.2	Provide protection from malicious code at designated locations within organizational systems	**Inbound Email Security**	**Supports** — detects and removes malicious emails at the email boundary; complements endpoint anti-malware protection.
3.14.3	Monitor system security alerts and advisories and take action in response	**Core Account Takeover Protection** **Security Posture Management (M365)**	**Supports** — detects compromised accounts across email and identity platforms and ejects attackers by automatically blocking account access, triggering password reset, and signing out of active sessions. Administrators can choose to auto-remediate compromised accounts or manually review cases. **Supports** — continuously surfaces risky misconfigurations and provides guided remediation to correct identified flaws.
3.14.5	Perform periodic and real-time scans of files from external sources as files are accessed	**Inbound Email Security**	**Supports** — performs real-time scanning of external email and attachments; auto-remediates malicious messages post-delivery.
3.14.6	Monitor organizational systems to detect attacks and indicators of potential attacks	**Inbound Email Security** **PeopleBase** **VendorBase** **AppBase**	**Supports** — monitors inbound email using behavioral AI to detect attacks and indicators of compromise. **Supports** — organizational relationship context and communication patterns improve attack detection accuracy across communication channels. **Supports** — vendor relationship modeling improves detection of vendor fraud and supply chain anomalies. **Supports** — application context aids detection of suspicious OAuth and app-based abuse patterns.
3.14.7	Identify unauthorized use of organizational systems	**Core Account Takeover Protection** **Abnormal for Okta**	**Supports** — detects unauthorized account use and can automatically reset passwords and terminate active sessions. **Supports** — detects unusual Okta sign-in patterns and supports one-click and automated remediation of compromised accounts.

About Abnormal AI

Abnormal AI is recognized as a Leader and was positioned highest for Completeness of Vision in the 2025 Gartner® Magic Quadrant™ for Email Security, protecting more than 4,500 organizations from sophisticated email attacks including spearphishing, business email compromise, vendor fraud, impersonation, and account takeover. Abnormal's behavioral AI platform builds a behavioral baseline for every identity in the environment and detects deviations that indicate attack, without relying on signatures, rules, or reputation-based filtering.

For Defense Industrial Base contractors, Abnormal provides the AI-native defense capability required to address AI-assisted nation-state attack campaigns targeting CUI systems and cleared personnel.

For more information about Abnormal AI's federal program, contact:

John Sourk
Director of Federal Sales | jsourk@abnormal.ai