carahsoft

ARCTIC WOLF

End-to-End Human and Infrastructure Threat Protection:

Arctic Wolf + Abnormal AI

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies and a wide range of contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with Arctic Wolf, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.

To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com

Explore More Resources:
carah.io/ArcticWolfResources

Join Events & Webinars:
carah.io/ArcticWolfEvents

Discover Technology Solutions:
carah.io/solve

Learn About Procurement:
carah.io/ArcticWolfContracts

Connect With Our Team:
ArcticWolf@carahsoft.com
888-662-2724

End-to-End Human and Infrastructure Threat Protection: Arctic Wolf + Abnormal AI

Stop the attacks at the source and contain them across your entire attack surface.

The joint solution from Arctic Wolf and Abnormal AI couples AI-powered protection against socially engineered and identity-based threats with 24x7 managed detection and response to deliver measurable risk reduction, operational relief, and business confidence.

The Challenge

Modern cyber attacks increasingly target humans, not just systems. Threats such as phishing, business email compromise (BEC), and social engineering are designed to exploit human behavior through emails, messages, and impersonation tactics. These attacks often serve as entry points for lateral movement across endpoints, cloud environments, and identity systems. When organizations fail to address human-centric threats as part of a broader, interconnected attack surface, they introduce blind spots that lead to incomplete detection, slower incident response, and greater exposure to breaches.

The Solution: Arctic Wolf + Abnormal AI

By combining Abnormal's behavioral AI-powered email and messaging security with Arctic Wolf's 24x7 Managed Detection and Response (MDR) service, organizations gain end-to-end visibility and faster containment, from initial compromise to full remediation.

Abnormal

Uses behavioral AI to detect and automatically remediate advanced phishing, business email compromise, and account takeover attacks that evade traditional solutions.

ARCTIC WOLF

Provides continuous monitoring across endpoints, cloud, network, and identity, guided by the MDR expert that triages alerts, investigates incidents, and drives response.

Abnormal's high-confidence detections — such as phishing, BEC, malware, and account takeover — are seamlessly ingested into Arctic Wolf's SOC, where MDR experts correlate these signals with endpoint, identity, network, and cloud telemetry. This creates a unified and intelligent security ecosystem that enhances threat detection and enables rapid response actions, like forced re-authentication, device isolation, email message deletion, and delivers guided remediation to reduce risk and accelerate recovery.

Key Benefits

Unified Defense Across the Full Attack Chain

Stop socially engineered email attacks at the source and contain downstream compromise across endpoints, identity, and cloud, all through a single integrated workflow.

Reduced Operational Overhead

Automation from Abnormal plus Arctic Wolf's managed SOC operations eliminate manual triage and investigation toil, freeing internal teams to focus on strategic initiatives instead of chasing alerts.

Measurable Risk Reduction

The combined solution delivers quantifiable improvements in breach prevention and containment: fewer successful business email compromise attempts, shorter incident lifecycles, and reduced financial exposure from cyber insurance claims.

Faster, Coordinated Response

High-confidence detections from Abnormal flow directly into Arctic Wolf's SOC, where the MDR experts correlates signals and executes rapid actions like forced re-authentication, device isolation, and malicious email purging, reducing dwell time and limiting lateral movement.

End-to-End Visibility and Context

Gain a consolidated view of email threats alongside endpoint, identity, and cloud telemetry, enabling richer investigations, unified reporting, and audit-ready compliance posture reviews.

The Integration Advantage

CAPABILITY	WHY IT MATTERS	JOINT VALUE
Behavioral AI Email & Messaging Security	Socially engineered threats are the leading entry vector	Abnormal's one-click API integration learns user, vendor, and app behavior — without disrupting mail flow — to block socially engineered attacks before compromise.
24×7 Managed SOC & MDR Experts	Security teams are overwhelmed and understaffed	Arctic Wolf provides expert-led operations and rapid containment
Unified Incident Workflow	Email alerts often stay siloed	Integration ensures instant escalation and coordinated response
Risk-Transfer Assurance	Businesses need financial and operational assurance	Arctic Wolf's warranty + Abnormal AI's prevention = stronger resilience
Cloud + Human Surface Coverage	Attackers move from people to endpoints to cloud	Combined visibility across the full attack chain

Use Cases

Stop Business Email Compromise Before Lateral Movement

- Detect socially engineered BEC attempts in email with Abnormal's behavioral AI.
- Immediately escalate to Arctic Wolf SOC for correlation with identity and endpoint telemetry.
- Trigger forced re-authentication or account disablement before attackers pivot.

Automated Email Threat Remediation + SOC Response

- Abnormal automatically deletes malicious emails from inboxes.
- Arctic Wolf investigates connected indicators (e.g., suspicious logins, MFA bypass).
- SOC executes device isolation or cloud session termination if compromise is confirmed.

Correlate Account Takeover Signals Across Surfaces

- Abnormal flags unusual email behavior (e.g., vendor impersonation, anomalous sending patterns).
- Arctic Wolf correlates with identity anomalies and endpoint EDR alerts.
- Unified workflow accelerates containment and reduces dwell time.

Reduce Noise and Alert Fatigue

- Abnormal provides high-confidence detections, reducing false positives.
- Arctic Wolf SOC handles triage and response, eliminating manual investigation burden for internal teams.

Kill Chain Coverage

- From initial phishing attempt → credential theft → endpoint compromise → cloud lateral movement, the integration ensures visibility and coordinated response at every stage.

Why Now

Email is widely recognized as the primary attack vector and initial entry point for cyber adversaries. As AI-powered phishing and vendor compromise campaigns rise, security teams can no longer rely on separate tools or manual processes. Arctic Wolf and Abnormal AI deliver a unified defense that closes the human-to-infrastructure gap and turns alerts into action.

Outcomes

4x
fewer attacks and unwanted emails land in employee inboxes

60
BEC attacks blocked per customer per month, on average

15+
hours saved for security teams each week through AI Automation

ARCTIC WOLF