carahsoft

Abnormal

Infiltration Prevention Data Sheet

Stop malicious attackers before they get in

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 through GSA Multiple Award Schedule (MAS), NASPO ValuePoint, The Quilt and a wide range of other 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 Abnormal AI, 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/abnormalresources

Join Events & Webinars:
carah.io/abnormalevents

Discover Technology Solutions:
carah.io/abnormal

Learn About Procurement:
carah.io/abnormalcontracts

Connect With Our Team:
AbnormalAI@carahsoft.com
844-214-4790

Abnormal

Infiltration Prevention

Stop malicious actors before they get in.

Nation-state actors have industrialized a new attack vector: the fake hire. Using stolen identities, fabricated resumes, and AI-generated interview personas, threat actors are applying for and landing legitimate jobs inside your organization, then using that access to steal data, plant malware, or fund sanctioned weapons programs.

Most identity and access tools were never built to catch this. They're designed to flag suspicious behavior after someone becomes an employee, not to verify who's actually behind a candidate before they're hired. By the time a background check turns up something wrong, or a first login trips an alert, the attacker already has a badge, a laptop, and legitimate access.

Organizations need a way to catch fraudulent identity at the moment it matters most: when it enters the hiring pipeline.

220% Increase in nation-state-led infiltration campaigns over the past year.

$600M Generated by DPRK IT-worker programs in a year.

Abnormal Has the Solution

Security tool designed to prevent fraudulent candidates from entering your organization.

Integrates with your Applicant Tracking System (ATS), so every new identity is analyzed once it enters the pipeline, before anyone is provisioned.

Accurately identifies fabricated credentials, VoIP burner numbers, VPN-masked locations, and more to uncover large-scale campaigns.

Sends your SOC clear evidence of impersonations for further review.

The Abnormal Advantage at a Glance

Behavioral AI to discover campaigns
Correlates candidate signals across your entire ATS to reveal when the same actor is applying to multiple roles or departments at once.

Evidence-backed briefs
Cited, evidence-backed briefs that turn a suspicious application into a documented case your SOC can act on in minutes, not days.

Federated detection network
Fraud patterns identified in one organization's hiring pipeline sharpen detection across Abnormal's entire customer base.

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