carahsoft

Abnormal

Identity Threat Protection Data Sheet

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

Identity Threat Protection

Autonomous AI understands how every identity behaves across email, identity providers, and cloud applications to reduce identity risk, stop compromise, and provide complete visibility into identities and access.

Identity-based attacks have become the leading cause of modern breaches. Security teams struggle to understand which identities are vulnerable, what access those identities have, and how attackers move through cloud environments once credentials are compromised. Traditional security tools focus on authentication events and static policies, creating fragmented visibility across identity, access, and risk.

Identity Threat Protection reduces identity risk and stops identity attacks in real time.

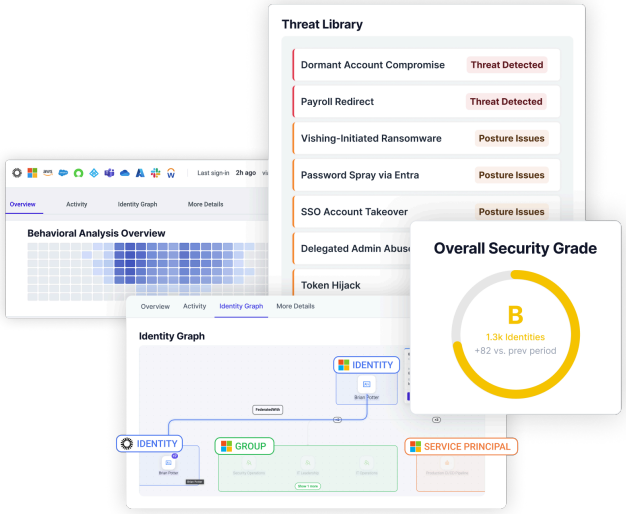
Behavioral AI learns how every identity normally behaves across email, identity providers, and cloud applications to detect compromised accounts, suspicious activity, service account misuse, and other identity threats. Automated remediation helps contain threats and eliminate attacker persistence.

Identifies high-risk exposures including weak MFA, dormant privileged accounts, excessive permissions, risky access paths, and vulnerable service accounts. Behavioral AI prioritizes the risks attackers are most likely to exploit.

Provides visibility into identities, permissions, relationships, and access across the organization. Security teams can quickly understand access, blast radius, and potential attack paths.

Protects password and MFA reset processes using behavioral intelligence to verify users and prevent help desk impersonation attacks. Risk-based verification helps stop unauthorized access while minimizing friction for legitimate users.

Threat Library maps identity attack scenarios to your environment, showing where you are protected, exposed, or actively detecting suspicious activity.



Abnormal Advantage at a Glance

Stops identity attacks. Detects and contains threats across the identity lifecycle using Behavioral AI.

Reduces identity risk. Prioritizes posture gaps based on the exposures attackers are most likely to exploit.

Provides complete visibility. Understand human and non-human identities, permissions, access relationships, and potential blast radius across your environment.

Accelerates response. Automate remediation actions and secure identity recovery workflows to minimize impact.

See Abnormal in action. **Request a demo.**

abnormal.ai ›