AuthMind Announces Agentic AI Identity Protection Capabilities to Detect and Stop Anomalous AI Agent Access in Real Time

AuthMind's platform is the first to discover, classify and automatically remediate all unknown AI agents via network traffic activity observability

AuthMind

BETHESDA, MD, UNITED STATES, June 11, 2026 /EINPresswire.com/ -- AuthMind, the leader in identity observability–driven agentic AI threat protection, today announced general availability of its enhanced agentic AI identity protection capabilities within the award-winning AuthMind Agentic AI Identity Observability & Protection Platform. AuthMind now delivers the industry's first approach to AI agent security grounded in deep network activity observability rather than outdated methods of provisioning records or identity system events.

According to AuthMind data, more than 60% of enterprises already have significant agentic AI usage. Moreover, approximately 50% of AI agents operating in production environments are unknown to security teams, and agentic AI usage is growing by at least 25% every two months. Existing identity and security tools were not built to find or govern agents that were never formally provisioned.

“AI agents are identities with production-level access, and most organizations have no idea where and what those identities are actually doing,” said Shlomi Yanai, CEO at AuthMind. "We find the agents nobody told us about, classify them by type, and detect and remediate when they stray from their intended purpose, all without a human getting involved.”

AuthMind's patented identity observability approach discovers shadow agents, unmanaged integrations, unauthorized AI Agents access activity, and agents spawned by other agents operating entirely outside established governance frameworks. Using proprietary AI and ML models, AuthMind automatically classifies every discovered agent by type and behavioral profile, and maps each one back to its human owner, delivering a continuously updated inventory of every AI agent operating in the environment without requiring prior knowledge that any of them existed.

When an agent violates policy, such as accessing production assets, misusing assumed IAM roles, or retrieving secrets outside intended scope, AuthMind triggers a prioritized incident with the complete access path already reconstructed. The platform then automates remediation, disabling credentials, creating ITSM tickets with full context, and notifying security teams, without waiting for analyst escalation.

To schedule a demo of the AuthMind Agentic AI Identity Observability & Protection Platform, visit:
https://www.authmind.com/schedule-a-demo

About AuthMind:
AuthMind empowers organizations to secure agentic AI, non-human (NHI), and human identities by continuously observing every access and understanding every activity across every environment. Unlike traditional identity tools, AuthMind's patented observability provides real-time visibility into identity behavior, eliminating blind spots and shadow IT while transforming identity security from a static policy-based approach to dynamic AI-based solution. Founded in 2020, the Maryland-based company also has R&D operations in Pune, India. Visit www.authmind.com.

Selena Proctor
AuthMind
selena.proctor@authmind.com
