AuthMind Data Reveals One in Five AI Agents Operating in Enterprise Environments as Shadow Agents

Expanded agentic AI discovery capabilities identify coding, user-assisted, autonomous and shadow AI agents by observing what they do on the network.



AuthMind

BETHESDA, MD, UNITED STATES, September 29, 2026 / EINPresswire.com/ -- AuthMind, the leader in identity observability-driven agentic AI threat protection, today announced that approximately 20 percent of AI agents running inside enterprise environments are shadow agents that security teams don't know exist, according to the latest AuthMind deployment data. The findings come from AuthMind customer deployments and coincide with the availability of the company's expanded agentic AI discovery capabilities.

Built on personal accounts, unauthorized credentials, consumer AI tools or unsanctioned integrations, shadow agents are AI agents that are not approved or managed by the organization. They hold real credentials and reach corporate data and systems while acting without human oversight. Yet, they never appear in the identity provider, the IAM inventory, or the security team's asset list, which makes each one of them an identity nobody is governing with high access rights, operating at machine speed.

Most approaches to AI agent runtime security start with what's registered: agents provisioned through an IdP, authorized with a vault or secret manager, and monitored by agentic governance tools. Shadow agents are, by definition, the ones that evade those steps. What they can't hide from is their footprint in network traffic. Every agent that calls a model, retrieves data, or touches an application generates traffic. And it’s that traffic where AuthMind discovers them, exposing a blind spot that log-based, API-based and policy-based tools cannot see.

AuthMind's expanded agentic AI discovery uses the company's patented Identity Access Flow Graph to identify and observe AI agents directly in network traffic, correlated with identity, cloud and endpoint telemetry. The platform classifies every AI agent it finds into three categories: coding agents, user-assisted agents acting on behalf of an employee, and autonomous agents

operating independently.

Additionally, each agent is mapped back to the human who created or operates it, the systems it accessed, and the NHIs and secrets it used, giving security teams the who, what, when, where and why behind agent activity. AuthMind is the only identity security platform that discovers and observes AI agents through network traffic, which is what allows it to reveal agents that never registered anywhere else and cannot be discovered by competitive tools.

“Every organization we work with has a handle on the AI agents it approved and can see, and every one of them is increasingly worried about the ones it can’t,” said Shlomi Yanai, CEO and co-founder of AuthMind. “When we looked at what was actually running across our customers' environments, as well as our own, roughly one in five agents was not sanctioned. You can’t write a policy for an agent you don’t know exists. Securing agentic AI has to start with detecting what agents exist, and observing what they actually access and do, not what policies intend.”

And the risk compounds quickly. A shadow agent can inherit the access of the account it runs under. If that access is misused by a compromised agent or by an attacker using the agent as a foothold, there is no owner to alert and no record to investigate. Discovery turns those unknown agents into governed identities with clear ownership and observable behavior.

Expanded agentic AI discovery is available now for AuthMind customers. To see which agents are operating in your environment, schedule a demo at www.authmind.com.

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 static policy-based to dynamic AI-based. AuthMind is headquartered in Bethesda, Maryland and is backed by Ballistic Ventures and IBM. Learn more at www.authmind.com.

Selena Proctor
AuthMind
selena.proctor@authmind.com

This press release can be viewed online at: https://www.einpresswire.com/article/945990218

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.