CloudEagle.ai Helps Enterprises Manage the AI Agent Lifecycle, Including the Kill Switch for Rogue AI Agents

Security and IT teams can continuously discover every AI agent, who owns it, its credentials, what it can access, and shut down rogue ones with a kill switch.

PALO ALTO, CA, UNITED STATES, October 1, 2026 /EINPresswire.com/ -- CloudEagle.ai, the leading AI governance platform, announces general availability of its AI agent management capabilities that enable IT and security teams to continuously discover, investigate, and manage the entire lifecycle of every AI agent operating across their environment, from provider consoles to the workflows agents are built into.

> The tools were never the problem; the untethered access agents get is. An agent runs on its own, keeps working long after the person who built it left the organization"
>
> *Nidhi Jain, CEO of CloudEagle.ai.*

A new employee gets a background check, a defined role, access that matches that role, and a manager accountable for it from day one. AI agents arrive with none of that. That gap did not matter much when agents were a few experiments. It matters now that the tools enterprises already pay for ship agents by default, and any employee can stand hundreds of AI agents in an afternoon that access your critical data and apps at AI speed.

Governing an agent comes down to five questions: where are the agents, what are they doing, what can they access, what permissions do they hold, and can it be shut down. Most enterprises cannot answer any of them today.

CloudEagle.ai's AI agent management answers all five, across every provider console and workflow:

1. Agent discovery: Every agent shows up with status, last activity, owner, and credentials in a single view, at both the global and the application level. Security teams get a real agent count instead of an estimate.

2. Agent activity: Activity logs show what each agent did, what it changed, and which resources it touched. An investigation starts with answers instead of a week of digging through consoles.

3. Application context: Each agent appears with the application or environment it belongs to, so teams see agent risk per application rather than as one flat list.

4. Roles and permissions: The roles each agent was given, and the ones it picked up along the way, which is usually where the wider access sits. Over-permissioned agents surface before an audit finds them.

5. Kill switch: Stops a rogue agent the moment it becomes a problem, with no hunting across consoles first. Revoke roles, rotate the secret, or deactivate the agent, and every action is written to the audit log.

"The tools were never the problem; the untethered access agents get is. An agent runs on its own, keeps working long after the person who built it left the organization, and almost never shows up in an access review. Governance has to run continuously, in real time, at AI speed; a quarterly review was never going to catch this," said Nidhi Jain, CEO of CloudEagle.ai.

Agents now go through the same access reviews as employees instead of sitting outside them. Teams can filter for the ones that need attention first: the inactive agents still holding credentials, the ones with no owner, and the ones with more access than their job needs. Every action taken on an agent is logged, so the evidence an auditor asks for is already there.

AI agent management is available to all CloudEagle.ai customers today.

To learn more, visit www.cloudeagle.ai.

About CloudEagle.ai

CloudEagle.ai is an AI-powered AI governance, SaaS management, and SaaS security platform that gives IT, Security, Finance, and Procurement teams unified visibility and control over their SaaS and AI stack, including human and non-human identities.

Nidhi Jain
CloudEagle.ai
marketing@cloudeagle.ai
Visit us on social media:
LinkedIn
YouTube

This press release can be viewed online at: https://www.einpresswire.com/article/946624675

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.