CloudEagle.ai Now Gives Enterprises GenAI Risk Scores for Every Vendor in Their SaaS Stack

70% of CIOs flag unsanctioned AI tools as their top security concern, according to CloudEagle's IGA Report. Most can't assess the risk those vendors carry.

PALO ALTO, CA, UNITED STATES, April 15, 2026 /EINPresswire.com/ -- CloudEagle.ai today announces that enterprises can now see the full GenAI and security risk profile of every SaaS vendor in their portfolio, including whether vendors meet required compliance standards, without any manual research.

> Security and procurement teams must prove AI vendor risk is under control to boards, auditors, and customers. What took weeks of research, CloudEagle.ai now answers in seconds."
>
> *Nidhi Jain, CEO and Founder of CloudEagle.ai*

Every SaaS vendor has an AI story now, and 7 out of 10 CIOs believe it's a major security risk. Very few make the details easy to verify. Most security and procurement teams struggle to assess AI risk across their full tech stack today.

Boards Are Asking. Most Security Teams Cannot Answer: AI governance has moved from the sidelines to a boardroom priority. 70% of Fortune 500 executives say their companies now have AI risk committees, yet only 14% say they are fully ready for AI deployment.

Boards are forming governance structures and demanding documented evidence that the tools their organizations use are safe, compliant, and governed. Only 37% of organizations have a formal policy for securely deploying AI, according to Darktrace's 2026 State of AI Cybersecurity Report.

The problem is not awareness. It is visibility. Enterprises have approved and deployed hundreds of SaaS tools, many of which have quietly added AI features, AI-assisted workflows, and data training clauses to their terms. No one has had a scalable way to assess what that means across the full portfolio, until now.

The specific questions most teams cannot yet answer across their full portfolio:

1. Which vendors are training AI models on our data, and which are not?
2. Which tools allow AI features to be disabled at the enterprise level?
3. Which applications in our stack are not SOC 2 or ISO 27001 certified?
4. Which tools do not support MFA, and what is the resulting access exposure?
5. Which vendors meet enterprise data center and residency standards?

CloudEagle.ai now answers all of them, across the entire portfolio, precisely when it matters.

"Security and procurement teams are being asked to prove AI vendor risk is under control, by their boards, by auditors, by enterprise customers running their own vendor due diligence. That question used to require weeks of manual research across vendor documentation. CloudEagle.ai answers it in seconds, across every application in the portfolio."

~ Nidhi Jain, CEO, CloudEagle.ai

Every Vendor. Every Risk Signal. One View: CloudEagle.ai now surfaces the following security and GenAI risk information for every application in the portfolio:

1. GenAI usage: Whether the application uses generative AI and whether that use was ever formally assessed before procurement approved it.
2. AI disable controls: Whether AI features can be turned off at the enterprise level, giving security teams the ability to act, not just observe.
3. AI training exposure: Whether customer data is used to train AI models
4. MFA support: Whether multi-factor authentication is enforced
5. SSO support: Whether the app integrates with identity providers
6. Certifications: SOC 2, ISO 27001, and other compliance certifications, so procurement and legal have the evidence they need before a contract is signed.
7. Data standards: The infrastructure and data residency standards the vendor adheres to, relevant for organizations with cross-border data obligations.

All of this is searchable and filterable across the full SaaS portfolio. The same information appears inside each vendor's profile, so risk can be reviewed alongside spend, usage, and licensing data in one place.

This capability is available now to all CloudEagle.ai customers. No additional vendor connections or configuration are required. The information appears automatically across every vendor in the portfolio, alongside the spend, usage, and contract data already in CloudEagle.

About CloudEagle.ai
CloudEagle.ai is an AI-powered SaaS governance platform that gives IT, Security, Finance, and Procurement teams unified visibility and control over their application stack. Backed by leading investors, CloudEagle.ai works with companies like RingCentral and Automation Anywhere to manage SaaS, AI, and identity governance from a single control plane.

Nidhi Jain
CloudEagle.ai
marketing@cloudeagle.ai
