

CloudEagle.ai Brings AI Governance Into the Browser With Real-Time Policy Enforcement

Turns a written AI policy into a live, continuous control, giving security and compliance teams peace of mind

PALO ALTO, CA, UNITED STATES, September 24, 2026 /EINPresswire.com/ -- CloudEagle.ai, an AI-powered AI governance platform, today announces Secure Browser, an [AI policy enforcement capability](#) that prevents employees from accessing unapproved AI tools and uploading sensitive PHI and PII data into LLMs.

“

Blocking AI rarely works. Secure Browsing redirects unapproved tools, flags sensitive data, and routes routine tasks to lighter models instead of burning Opus.”

*Nidhi Jain, CEO of
CloudEagle.ai*

Most enterprises treat AI governance as a policy that exists on paper. But the exposure happens in the browser, someone logs into an AI tool on a personal account, pastes a customer record into a prompt, and the policy never sees it. The browser is the new perimeter. Secure Browsing enforces there, at the moment it happens, not in a document nobody's checking.

"Blocking AI tools rarely works, people just switch to a personal account. Secure Browsing redirects them the moment they open an unapproved tool, flags sensitive data before it reaches the model, and steers routine requests to a lighter model instead of burning Opus on an email. That's the difference between a policy you publish and one that actually holds," says Nidhi Jain, CEO of CloudEagle.ai.

The gap is widest where IT has the least reach. A Gartner survey found that more than half of [employees use personal GenAI accounts](#) for work, and a third admit to entering sensitive company information into tools their employer never approved. Once someone is inside a personal ChatGPT or Gemini tab, that session sits outside SSO, outside logging, and outside every control the security team has configured. Firewalls and CASBs can see that a session reached an AI domain, but they were never built to inspect what goes into a prompt.

The CloudEagle.ai browser extension detects the moment a user logs into a non-corporate AI tenant and acts on it while the session is live, so that activity is governed the same way a sanctioned application would be.

Detection tells a security team that something already happened. Secure Browser acts while it is happening. Through the browser extension, IT and Security teams can now:

1. Redirect employees who open an unapproved AI tool to the company's sanctioned alternative through a flash page, before any prompt is entered.
2. Monitor and block PHI, PII, and other sensitive content from being typed or uploaded into any AI tool not cleared to receive it, sanctioned or shadow.
3. Flag logins to personal and non-corporate AI tenants, so access reviews and audits cover shadow AI the same way they already cover shadow IT.
4. Guide employees to the right model for each task, keeping premium models like Opus for the work that needs them.

The result is AI governance an enterprise can defend in front of an auditor or a board. Teams can show which AI tools are in use, which controls were applied to them, and what happened when someone attempted to work outside policy. DLP signals sit alongside the full AI inventory in the same CloudEagle.ai dashboard, so the apps in use and what happens inside them show up in one view, with no separate DLP tool to run.

With enforcement running in the browser, AI moves from an unmanaged experiment to a governed enterprise capability, and leadership can scale adoption with the security, compliance, and cost controls already in place.

AI policy enforcement through Secure Browser is available now to all CloudEagle.ai customers.

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 enterprises one command center to discover, secure, govern, and optimize their entire SaaS and AI stack, including AI usage control and both human and non-human identities.

Nidhi Jain

CloudEagle.ai

marketing@cloudeagle.ai

This press release can be viewed online at: <https://www.einpresswire.com/article/944848834>

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.