Netskope Threat Labs: Shadow AI Risks Proliferate as GenAI Platforms and AI Agents See Rapid Adoption

August 3, 2025

Latest research indicates increased adoption of on-premises genAI and AI agents is magnifying the challenge despite enterprises safely enabling SaaS genAI apps on a broader scale

SANTA CLARA, Calif., August 4, 2025 – Netskope, a leader in modern security and networking, today released new research showing a 50% spike in genAI platform usage among enterprise end-users in the three months ended May 2025. Despite an ongoing shift toward safe enablement of SaaS genAI apps and AI agents, the growth of shadow AI—unsanctioned AI applications in use by employees—continues to compound potential security risks, with over half of all current app adoption estimated to be shadow AI.

The new data was published within the company's latest Netskope Threat Labs Cloud and Threat Report. It examines the ongoing employee shift to genAI platforms, whether they are delivered from the cloud or on-premises, amid expansive interest to develop AI apps and autonomous agents, creating a new set of cybersecurity challenges that enterprises must address.

The Rise of genAI Platforms

GenAI platforms, which are foundational infrastructure tools that enable organizations to build custom AI apps and AI agents, represent the fastest growing category of shadow AI given their simplicity and flexibility for users. In the three months ended May 2025, users of these platforms increased by 50%. GenAI platforms expedite direct connection of enterprise data stores to AI applications with the popularity in usage creating new enterprise data security risks that place added importance on data loss prevention (DLP) and continuous monitoring and awareness. Network traffic tied to genAI platform usage also increased 73% over the prior three month period. In May, 41% of organizations were already using at least one genAI platform. Approximately 29% of organizations are utilizing Microsoft Azure OpenAI, followed by Amazon Bedrock (22%), and Google Vertex AI (7.2%) respectively.

"The rapid growth of shadow AI places the onus on organizations to identify who is creating new AI apps and AI agents using genAI platforms and where they are building and deploying them," said Ray Canzanese, Director of Netskope Threat Labs. "Security teams don't want to hamper employee end users' innovation aspirations, but AI usage is only going to increase. To safeguard this innovation, organizations need to overhaul their AI app controls and evolve their DLP policies to incorporate real-time user coaching elements."

The Many Facets of On-Premises AI Innovation

From deploying genAI locally through on-premises GPU sources, to developing on-premises tools that interact with SaaS genAI applications or genAI platforms, organizations are evaluating many options to innovate quickly using AI, and, increasingly, they are turning to Large Language Model (LLM) interfaces.

- Today, 34% of organizations are using these interfaces, with Ollama the current clear adoption leader (33%), and others such as LM Studio (0.9%) and Ramalama (0.6%) just scratching the surface.
- Meanwhile, employee end-users are experimenting with AI tools and visit AI marketplaces at a rapid clip. For example, users are downloading resources from Hugging Face at a majority (67%) of organizations.
- The promise of AI agents is driving this behavior as the data shows there is now a critical mass of users across organizations building AI agents and leveraging agentic AI features of SaaS solutions. GitHub Copilot is now used in 39% of organizations and 5.5% have users running agents generated from popular AI agent frameworks on-premises.
- Furthermore, on-premises agents are retrieving more data from SaaS services and are doing so by accessing more API endpoints other than browsers. Two-thirds (66%) of organizations have users making API calls to api.openai.com and 13% to api.anthropic.com.

The Continuation and Evolution of SaaS AI Use

Netskope is now tracking more than 1,550 distinct genAI SaaS applications, up from just 317 in February, indicating the rapid pace at which new apps are being released and adopted throughout the enterprise. Organizations are now using approximately 15 genAI apps, up from 13 in February. Additionally, the amount of data uploaded to genAI apps each month has increased from 7.7 GB to 8.2 GB quarter over quarter.

- Enterprise users are beginning to consolidate around purpose-built tooling, such as Gemini and Copilot, as more security teams work to safely enable these applications and solutions across their business as these chatbots are now better integrated into their productivity suites.
- General-purpose chatbot ChatGPT saw its first decrease in enterprise popularity since Netskope started tracking the popular genAI app in 2023.
- Of the top 10 most popular genAI apps per organization, ChatGPT was the only one to see a decrease since February,

while other popular apps, including Anthropic Claude, Perplexity AI, Grammarly, and Gamma, all saw enterprise adoption gains.
- Additionally, Grok's gain in popularity has seen it enter the top 10 most-used applications for the first time. While it does remain in the top 10 most-blocked apps list, its blockage rates have been trending downward as more organizations evaluate and opt into granular controls and monitoring.

Ensuring AI Governance and Usage Monitoring

CISOs and other security leaders should take necessary steps to ensure safe and responsible adoption amid the accelerated usage of varied genAI technologies. Netskope recommends the following:

- **Assess the genAI landscape:** Determine which genAI tools are in use across the organization and pinpoint who is using these tools and how they are being leveraged.
- **Bolster genAI app controls:** Establish and enforce a policy that only allows the use of company-approved genAI applications, implement robust blocking mechanisms and deploy real-time user coaching.
- **Inventory local controls:** If an organization is running any genAI infrastructure locally, review and apply relevant security frameworks such as OWASP Top 10 for Large Language Model Applications, and ensure adequate protection is in place for data, users and networks interacting with local genAI infrastructure.
- **Continuous monitoring and awareness**: Implement continuous monitoring of genAI use within the organization to detect new shadow AI instances and stay updated on new developments in AI ethics, regulatory changes and adversarial attacks.
- **Assess the emerging risks of agentic shadow AI:** Identify those who are leading the charge in the adoption of agentic AI and partner with them to develop an actionable and realistic policy to limit shadow AI.

To learn more, view the Netskope Threat Labs Cloud and Threat Report Shadow AI and Agentic AI here.

About Netskope
Netskope, a leader in modern security and networking, addresses the needs of both security and networking teams by providing optimized access and real-time, context-based security for people, devices, and data anywhere they go. Thousands of customers, including more than 30 of the Fortune 100, trust the Netskope One platform, its Zero Trust Engine, and its powerful NewEdge network to reduce risk and gain full visibility and control over cloud, AI, SaaS, web, and private applications—providing security and accelerating performance without trade-offs.

Learn more at netskope.com, on LinkedIn, and Instagram.

Media Contacts:
press@netskope.com