

wiz^{*}

The State of AI in the Cloud 2025

As DeepSeek surges and AI adoption rates stabilize,
security and governance challenges persist




Table of Contents

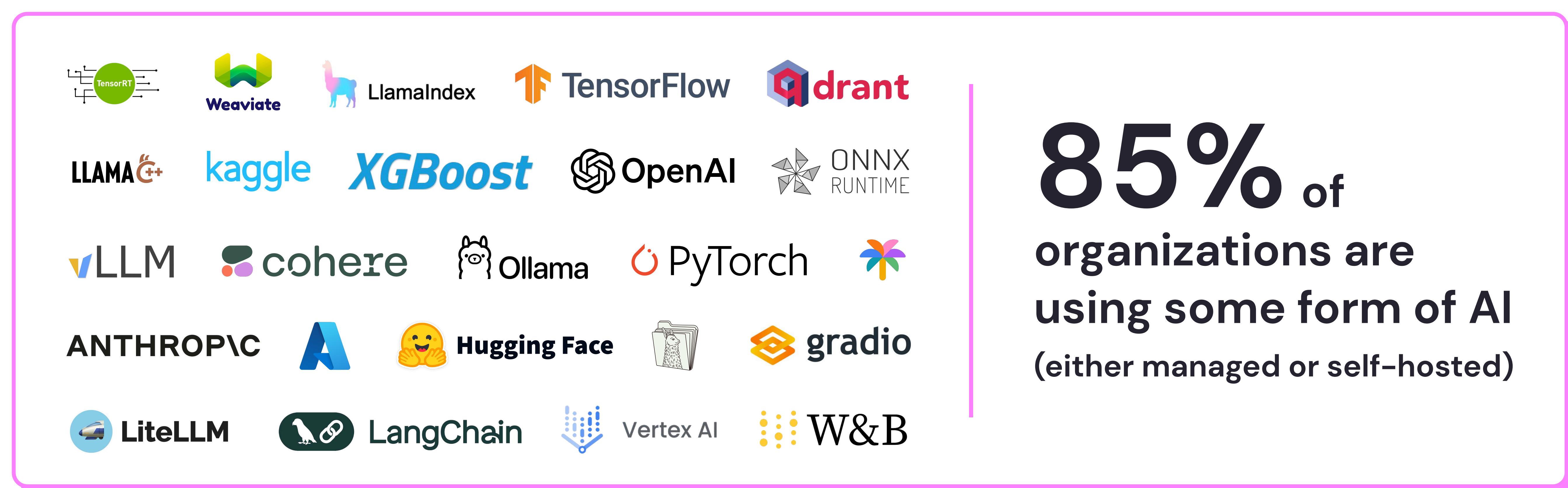
Introduction	3
<hr/>	
Key Takeaways	4
<hr/>	
DeepSeek's staggering growth rate	4
<hr/>	
AI adoption rates rise, but OpenAI holds onto the #1 spot	5
<hr/>	
Mix of open & closed source AI	6
<hr/>	
Self-hosted AI gains popularity	6
<hr/>	
AI managed service adoption stabilizes	7
<hr/>	
Conclusion	7

Introduction

In our second annual State of AI in the Cloud report, the Wiz research team explores the continued explosion of AI in cloud environments. Based on the sample size of hundreds of thousands of public cloud accounts, our data reinforced many of the takeaways from last year, yielded some noteworthy year-over-year trends, and – such as with DeepSeek – surfaced new developments in the AI boom. These developments raise necessary questions about the delicate balance between speed, innovation, and risk. A major theme of last year's report edition was lightning-fast adoption for both managed and self-hosted AI tools, with more than 70% of cloud environments using AI services. Many organizations were in the early adoption stages, with 32% deploying fewer than 10 instances and favoring experimentation over large-scale production use.

Here's the TL;DR of what we've seen in this year's data:

- 1 **AI is now a key player in cloud operations.** In our first report, **70%** of organizations were using managed AI services – now it's up to **74%**. Furthermore, over **85%** of organizations are currently using either managed or self-hosted AI services or tools. All in all, this represents continued but stable interest in experimentation and development.
- 2 **DeepSeek enters with a bang.** This new player in the AI scene saw a big spike in growth. Thanks to the release of DeepSeek-R1, adoption amongst organizations using self-hosted AI models more than doubled to **7%** in January alone.
- 3 **Security continues to play catch up.** The AI story is a lot like the early days of cloud: an emerging technology with incredible disruptive power draws the focus to development and adoption over standards and governance. Security must find a way to match the pace.



AI's benefits are clearer than ever. Many amazing examples exist of businesses that have seen real, game-changing results. But with great progress comes great responsibility. Gartner puts a finer point on mounting AI security threats, asserting that "AI technology usage is increasing risk, and without effective governance and security controls they will have damaging unforeseen impacts on organizations¹."

Wiz shares that viewpoint. We believe that this inflection point must be approached correctly. AI's omnipresence, coupled with its relatively young code base, carries serious cybersecurity implications. Exactly what those implications are is something the Wiz Research team has investigated in great depth. Over the last 12 months our work has uncovered multiple examples of the risks inherent to AI software and services:

- [DeepLeak](#), an exposed DeepSeek database leaking sensitive information – including usage history and over a million lines of log streams – and allowing full control over database operations.

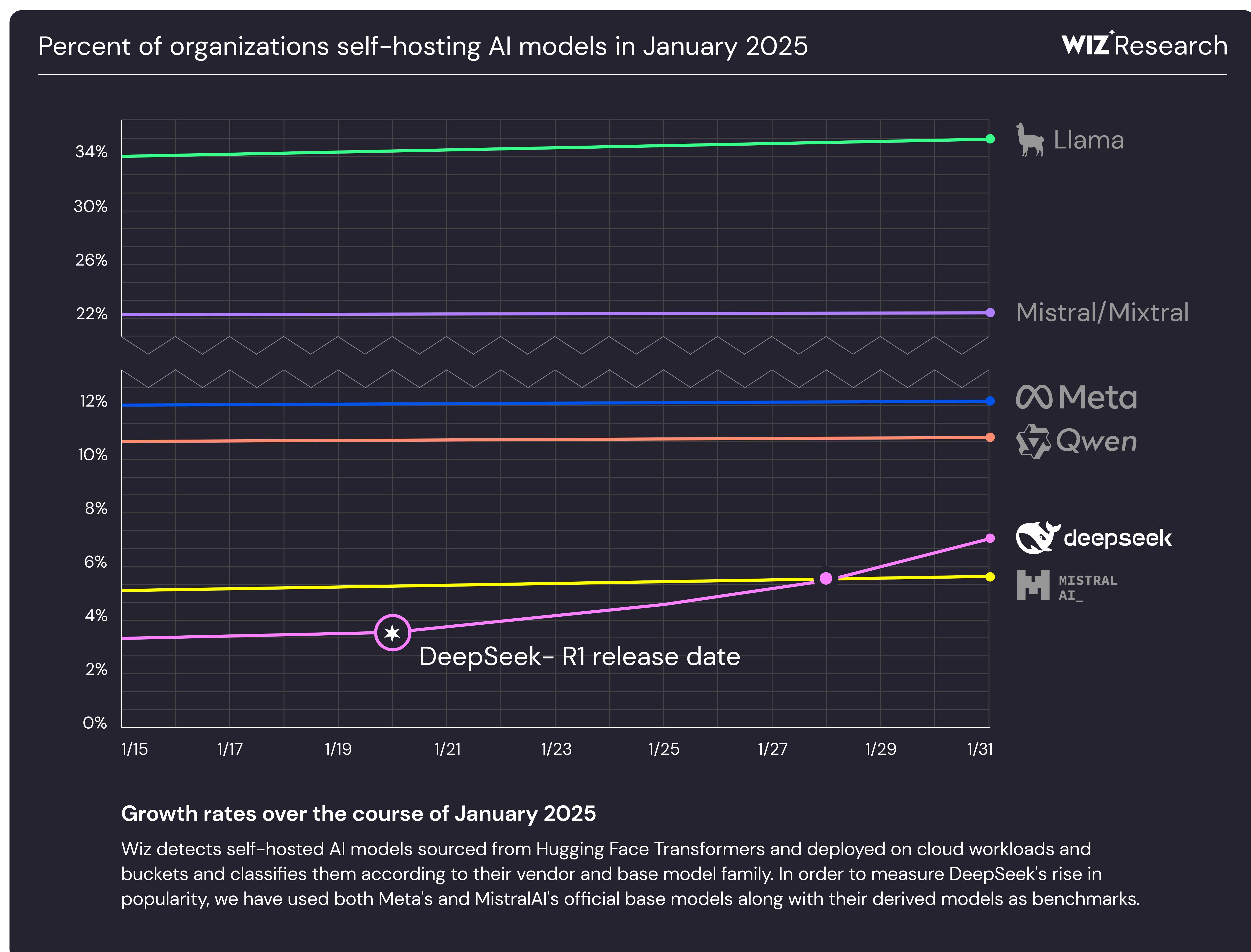
1. Source: [2025 Planning Guide for Security](#) by William Duper, Patrick Hevesi et al, Gartner, October 2024

- A critical NVIDIA AI vulnerability that affected containers using NVIDIA GPUs, including over 35% of cloud environments. CVE-2024-0132 presented a high level of risk to AI workloads and environments.
- SAPwned, vulnerabilities in SAP AI Core that would allow malicious actors to take over the service and access customer data, including private AI artifacts and cloud keys.
- Problama, an easy-to-exploit Remote Code Execution vulnerability in the open-source AI infrastructure project Ollama.
- Our work with AI-as-a-service providers Hugging Face and Replicate revealed that without proper isolation, malicious models pose a major risk to AI systems and customer data in particular.

With that, let's take a closer look at what this year's findings reveal about the state of AI, cloud, and security.

Key Takeaways

1 DeepSeek's staggering growth rate

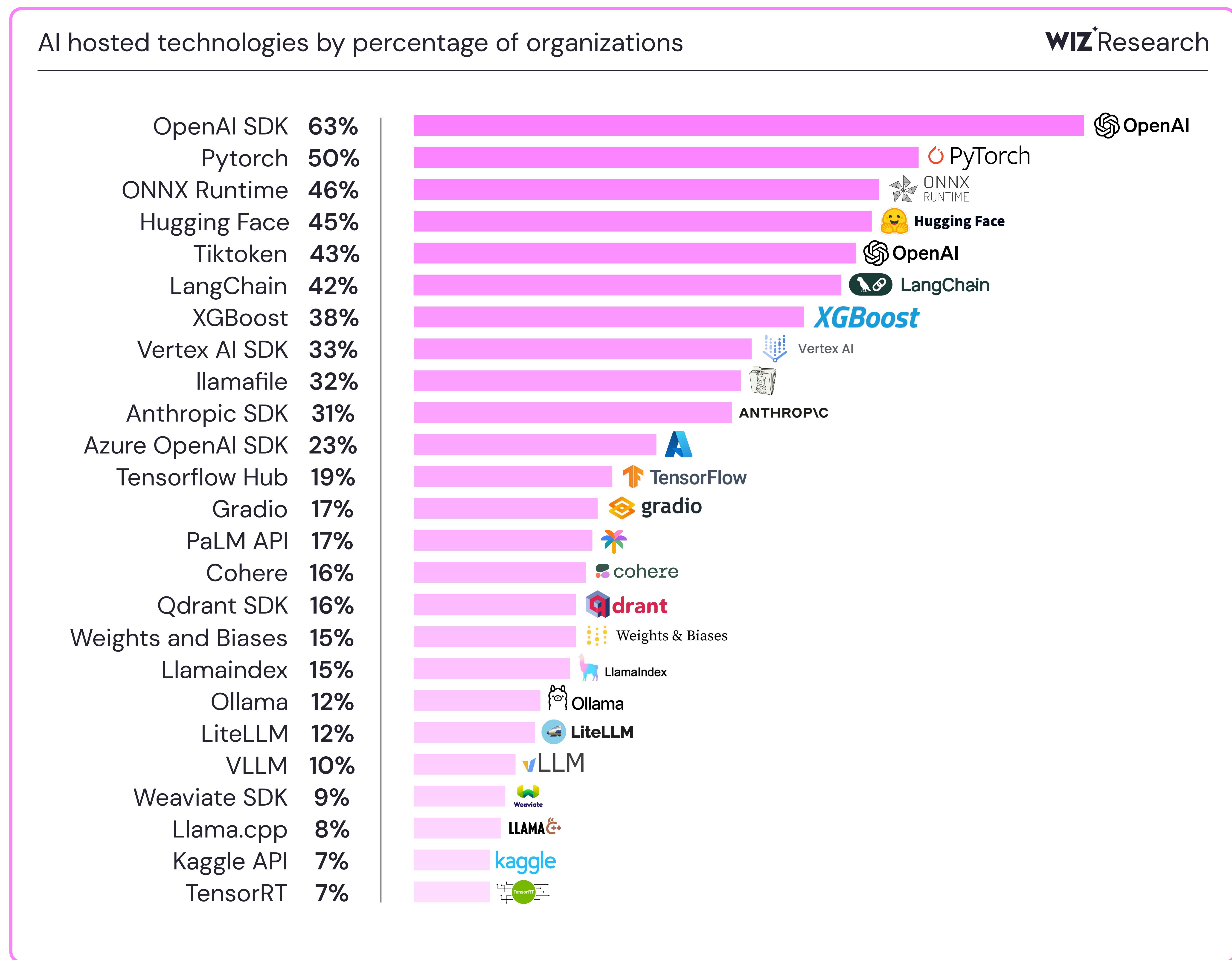


The latest entrant into the AI race more than doubled adoption in January alone.

- The release of DeepSeek-R1 prompted a surge in adoption, with its newest model securing around 130,000 downloads on HuggingFace. At the time of this report's publication, roughly 7% of organizations using self-hosted AI models are currently using models developed by DeepSeek, with approximately 4% using R1 in particular.

- DeepSeek quickly gained widespread attention for its cost-effectiveness and rapid pace of innovation. However, as evidenced by [the exposure of data](#) in their service our research team uncovered in January 2025, the rise of DeepSeek also underscores a stark corollary of the AI gold rush: that innovation should not come at the cost of safety, and AI systems on the whole warrant much closer security oversight.
- This graph also demonstrates that while relatively few organizations may use a vendor's official models, many more organizations use models derived from those official ones.

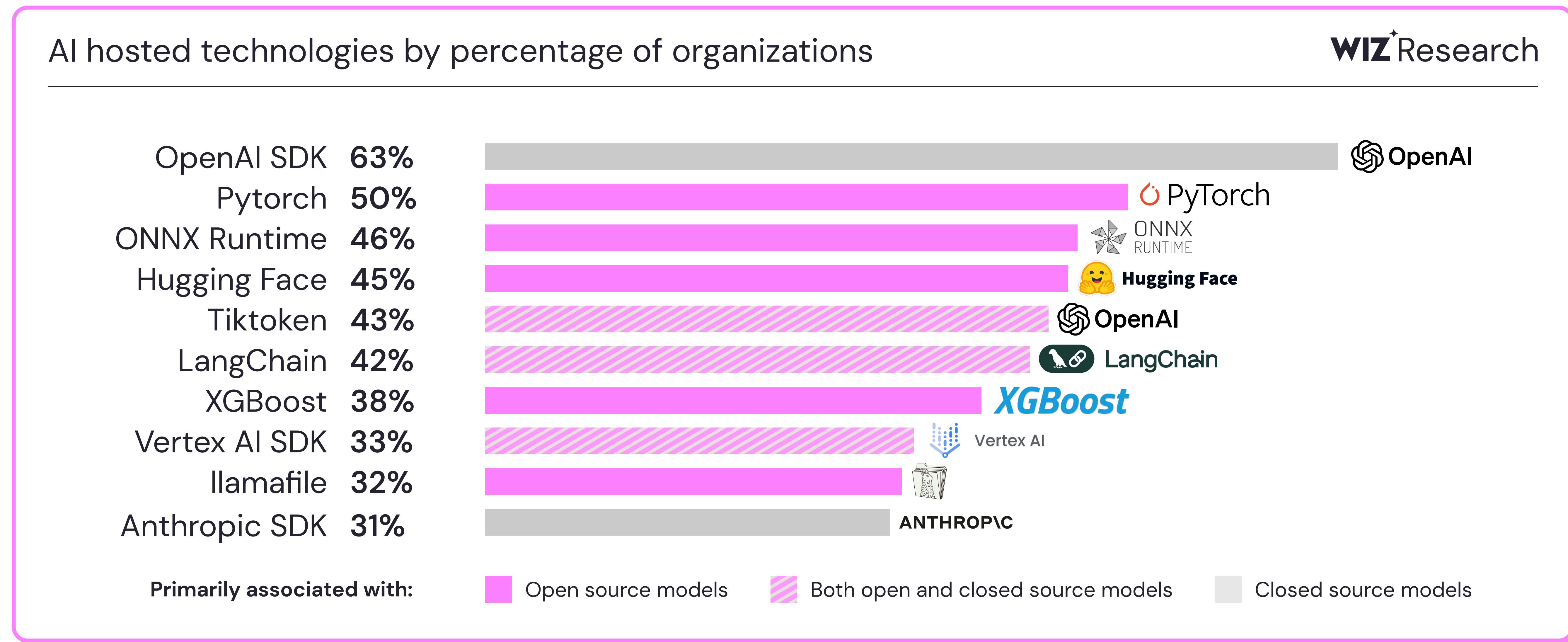
2 AI adoption rates rise, but OpenAI holds onto the #1 spot



More than half of organizations still use OpenAI or Azure OpenAI SDKs.

- AI tools are common in business use cases. Several key data points reinforce this reality: first, the percentage of organizations using self-hosted AI models in their cloud environments rose steeply from 42% last year to 75% in 2025, with much of this growth attributed to increased adoption of AI in third-party software. Similarly, usage of dedicated AI and ML software rose from 69% to 77% of environments year over year.
- 67% of cloud environments are using OpenAI or Azure OpenAI SDKs, up from 53% last year. Rounding out the top 5 are Pytorch (50%), ONNX Runtime (46%), Hugging Face Transformers (45%), and Tiktoken (43%).

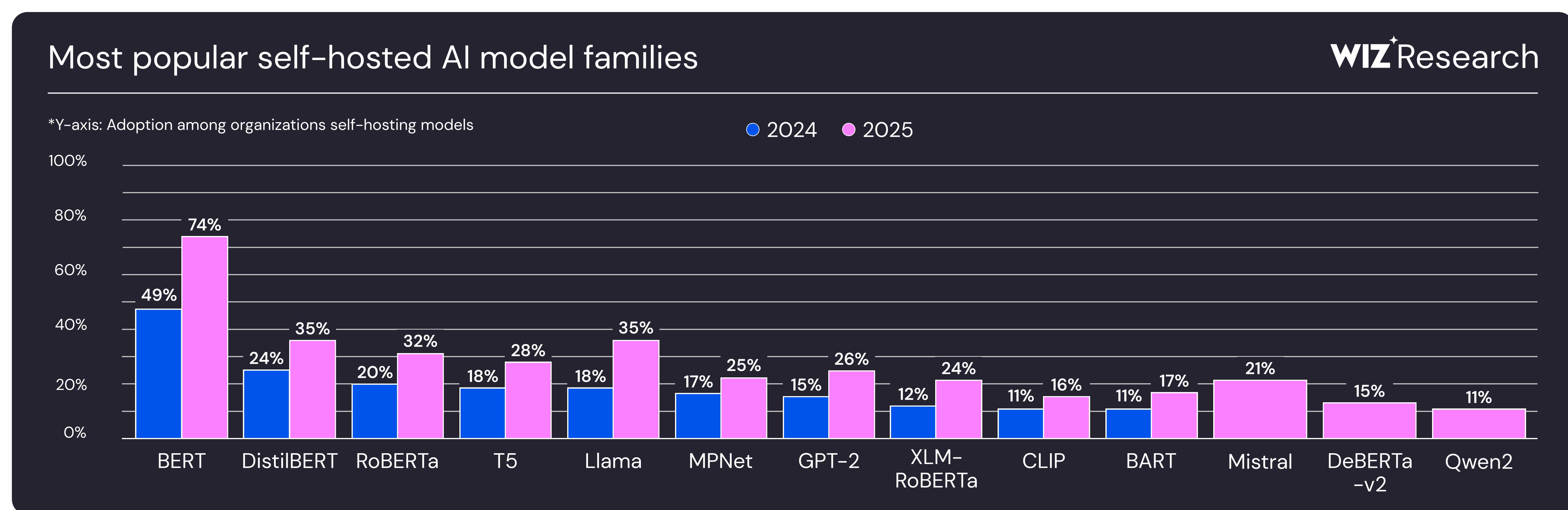
3 Mix of open & closed source AI



8 out of the 10 most popular hosted technologies are associated with open-source

- Our top 10 list includes both open and closed-source AI technologies, though the majority are associated with open-source.
- These AI hosted technologies also demonstrate the interplay of open and closed-source; Providers of closed-source models like OpenAI and Anthropic publish open-source tools that are used generically, like Tiktoker. Open-source toolchains like Langchain offer paid platforms. Vertex AI lets users make their choice between models from vendors like Anthropic and popular open source models developed by companies like DeepSeek and Alibaba.
- Open source models can see explosive adoption, as we saw recently with DeepSeek. But they also have staying power, with Llama growing from 18% to 35% since our last report (see below).

4 Self-hosted AI gains popularity

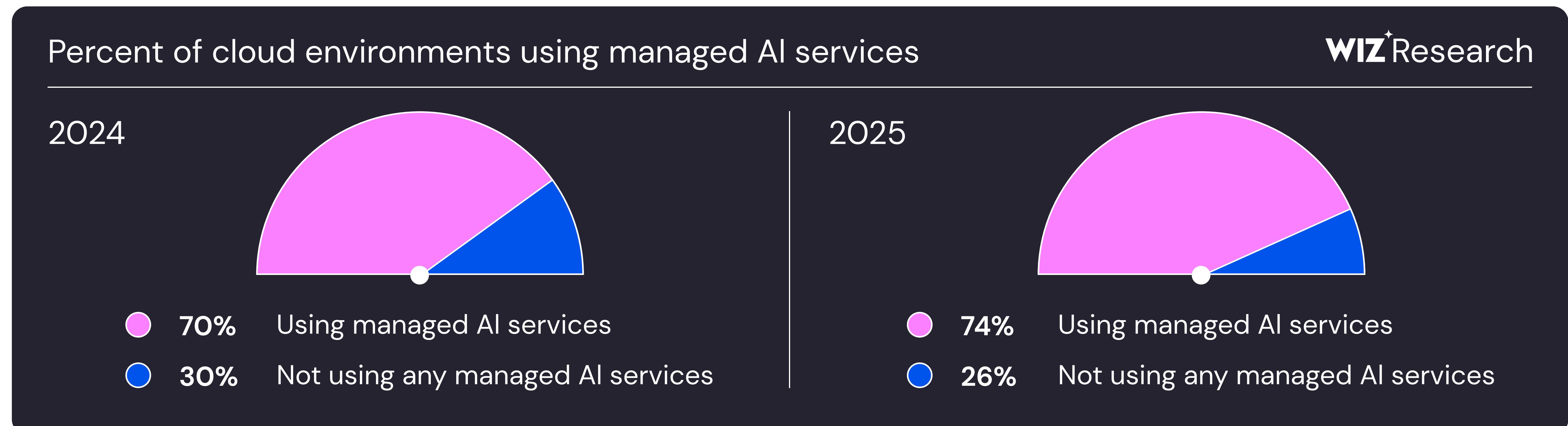


BERT Dominates, Mistral AI Joins the Top 10, Qwen2 Emerges.

- Comparing this year to last, we've seen increased adoption of self-hosted AI models. Among organizations that have chosen to self-host AI models, the most popular identifiable model type remains [BERT](#); it was found in 49% of such environments last year and rose sharply to 74%.

- While the top 10 model families have remained mostly unchanged, Mistral AI has secured a spot in the top 10, bumping Clip to the number 11 spot.
- Qwen2, Alibaba Cloud's LLM, is a new and notable entrant on this year's list.

5 AI managed service adoption stabilizes



The percentage of environments using managed AI services increased by 4 percentage points YoY.

- Over 85% of organizations are currently using either managed or self-hosted AI services or tools. The percentage of organizations deploying managed AI has risen from 70% to 74% over the past year, indicating continued but stable interest in experimentation and development.

Conclusion

AI fosters creativity, competition, speed, and a slew of new opportunities. As adoption accelerates, organizations face familiar challenges around governance, security, and cost management. The rapid introduction of AI tools, often without established standards, raises questions about visibility, risk management, and responsible usage. Security teams and developers will need to work together to address emerging risks, including data exposure and unauthorized AI use within cloud environments.

This report shows a landscape in flux, with DeepSeek poised to trigger a major shakeup. Innovation should not come at the cost of risk, and the major vulnerabilities our research team discovered in DeepSeek and other AI providers underscore the urgent need for stronger AI security. As self-hosted AI adoption accelerates, organizations must prioritize cybersecurity efforts.

Wiz's AI Security Posture Management (AI-SPM) solution helps teams gain full visibility into AI usage, manage risks like Shadow AI, and enable secure innovation. Take a peek behind the curtain to see what insights you'll gain from Wiz's AI-SPM capabilities in this [Sample Assessment Report](#).

The Wiz Threat Research team investigates and analyzes emerging vulnerabilities, exploits, and security trends impacting cloud environments. With a focus on actionable insights, this international team not only provides in-depth research but also creates detections within Wiz to help customers identify and mitigate threats in their environments. Outside of deep-diving into code and threat landscapes, the researchers are dedicated to fostering a safer cloud ecosystem for all.

[Read more](#)

