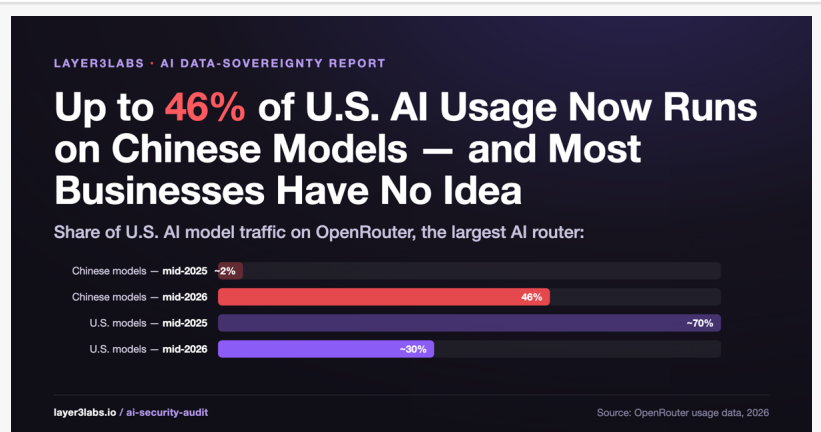


Up to 46% of U.S. AI Usage Now Runs on Chinese Models — And Most Businesses Have No Idea

Chinese models like DeepSeek & Qwen now handle nearly half of U.S. AI traffic on major routers — often reaching businesses via vendors and 'shadow AI.'

MIAMI, FL, UNITED STATES, July 22, 2026 /EINPresswire.com/ -- A fast-growing share of the artificial intelligence powering American businesses is being processed by Chinese-developed models. As much as 46% of token traffic on the largest U.S. based AI model router is funneled to Chinese models. Yet most business owners have no idea which language model is reading their data, according to [Layer3Labs](#), an AI implementation firm that audits companies' AI stacks. A year ago, U.S. models held roughly 70% of that traffic; today it's closer to 30%.



Most business owners think their data stays exclusively on U.S. based servers, but hundreds of gigabytes of their sensitive data are being run through Chinese provided endpoints.

The shift is largely invisible because business owners rarely choose a model directly — they buy “an AI feature,” and the model underneath can be routed, resold, or white-labeled without notice:

“

Most business owners think their data stays exclusively on U.S. based servers, yet hundreds of gigabytes of their sensitive data are being run through Chinese provided endpoints.”

*Jonathan Teplitsky,
Layer3Labs*

Routing defaults: cost-optimizing routers send prompts to the cheapest available provider — increasingly a Chinese endpoint, where inference runs 60–90% cheaper.

Vendor backends: venture firm Andreessen Horowitz estimates 80% of U.S. startups build on Chinese base models; named adopters include Airbnb, Uber, and Cursor.

Shadow AI: research puts 70% of enterprise AI activity outside IT oversight, much of it Chinese models small

enough to run on a laptop, bypassing security review entirely.

The exposure is no longer hypothetical. Any prompt processed by a Chinese-provider endpoint falls under China's National Intelligence Law, which can compel data disclosure to the state. In July 2026, the House Select Committee on the CCP opened a probe into U.S. firms' use of these models, and the NDAA already bars DeepSeek from Defense Department systems. Firms with high "shadow AI" exposure pay an estimated \$670,000 breach premium per incident.³

"Most business owners think their data stays exclusively on U.S based servers," said Jonathan Teplitsky, CEO of Layer3Labs. "Yet hundreds of gigabytes of their sensitive data are being run through Chinese provided endpoints — they just don't know it. Business owners need to ask whose jurisdiction their customer data now lives under."

In its own review of dozens of small- and mid-sized business AI stacks, Layer3Labs found 70% contained at least one Chinese model the company had not knowingly approved.

Layer3Labs is urging businesses — especially those in regulated fields like healthcare, legal, and finance — to run a provenance check on every AI tool touching customer data. The firm is offering a free AI Stack Sovereignty Check that identifies which models are actually processing a company's data and flags data-sovereignty and compliance risk.

"You can't govern what you can't see," said Mark Boyhous. "Step one is simply finding out what's in your stack. Most owners are shocked by the answer."

About Layer3Labs

Layer3Labs is an AI implementation and automation firm that helps small and mid-size businesses deploy AI safely — plugged into the tools they already use, live in 2–4 weeks. Founded in 2019 and based in Miami, the firm specializes in AI strategy, workflow automation, and vendor risk assessment. Learn more at www.layer3labs.io.

Media Contact

[Jonathan Teplitsky] · [Jonathan@Layer3Labs.io] · [954-641-2945] · layer3labs.io

1 — Router usage / cost (the 46% and 70%→30%):

<https://dataconomy.com/2026/02/25/chinese-ai-models-hit-61-market-share-on-openrouter/>
<https://officechai.com/ai/share-of-us-models-being-used-on-openrouter-has-collapsed-from-70-to-30-over-the-past-year/>

2 — a16z 80% + named adopters (Airbnb, Uber, Cursor):

<https://www.cnbc.com/2026/07/07/chinese-ai-models-costs-us-openai-anthropic.html>
<https://qz.com/ai-us-china-open-models-deepseek-qwen>

3 — Shadow AI 70% / \$670K breach premium:

<https://technologyradius.com/statistic/shadow-ai-statistics-2024-2026>

<https://witness.ai/blog/deepseek-security-concerns/>

Jonathan Teplitsky

Layer3Labs

+1 954-641-2945

[email us here](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/928395064>

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.