VISION by protiviti®

In Focus

February 18,
2025

Does DeepSeek disrupt your AI strategy? It should.

By Christine Livingston

Managing Director, Protiviti

Late last month, DeepSeek, the China-based AI startup, sent shockwaves worldwide when it released its latest model, DeepSeek R1, which it says rivals ChatGPT's capabilities. OpenAI's o1 model was released on Sept. 12, 2024, roughly four months ahead of DeepSeek's R1 model release in January.

Like OpenAI's reasoning models, DeepSeek uses a large language model that responds incrementally, simulating how a human would reason through a problem. But unlike OpenAI, DeepSeek has open-sourced their model (code and weights) — meaning anyone can copy, download and build upon it. The result could be a more democratized AI, allowing smaller players to catch up quickly. But perhaps even more concerning for U.S. AI companies was the reported $6 million price tag DeepSeek claimed — compared to an estimated $100 million for OpenAI. If that's true, DeepSeek radically impacts the AI race and likely should change your enterprise AI strategy.

Why it matters

DeepSeek's disruption to the AI industry is substantial; it has already overtaken ChatGPT as the most downloaded free app in the Apple App Store in the U.S. DeepSeek has also disrupted the psyche of the U.S. tech establishment, casting doubt as to whether American firms would dominate the exploding AI market. Before DeepSeek's arrival, most tech experts assumed that would be the case. But China may have been much further along than most thought, prompting U.S. President Donald Trump to call DeepSeek "a wake-up call" for America's tech companies.

DeepSeek's R1 open-source model comes with inherent security risks. For instance, when using open-source models there is no third party to hold liable; the responsibility is on the enterprise to perform robust safety and security testing to ensure there are no embedded vulnerabilities. Other challenges include:

- **Security:** DeepSeek and other open-source AI models contain source code that is accessible, resulting in possible vulnerabilities in the architecture being open for exploitation.

- **Credibility:** There is some skepticism about the accuracy of some of DeepSeek's claims, as well as accusations of AI plagiarism.

- **Skill Sets:** Typically, open-source models lack readily available support, meaning that AI-ML skill sets may be needed to modify the model.

- **Compliance and Regulatory:** The implications of DeepSeek on compliance and regulatory requirements are still unclear. In the U.S., New York, Texas and Virginia have statewide bans on the app; Oregon and North Carolina have banned DeepSeek on state devices. Globally, South Korea has banned the DeepSeek app, and Australia has banned the app on government devices.

Conversely, open-source AI models afford benefits such as:

- **Transparency:** By virtue of open-sourcing the model and providing full access to the code base, DeepSeek and other open-source models provide transparency into algorithms and data sources not possible in closed models, which may be required for regulatory compliance in some use cases.

- **Customizability:** Open-source models such as DeepSeek allow users to adapt models for tailored solutions and specific needs and more seamlessly integrate future model versions while preserving those customizations, compared to fine-tuning a closed-source model.

- **Barrier to entry:** Open-source models leverage open-source licences, which are either free or far less expensive than closed/commercial licences.

What they say

Dario Amodei, CEO of Anthropic, a public benefit corporation dedicated to building safe AI systems

“DeepSeek produced a model close to the performance of U.S. models 7 to 10 months older, for a good deal less cost. All of this is to say that DeepSeek is not a unique breakthrough or something that fundamentally changes the economics of large language models; it’s an expected point on an ongoing cost reduction curve. What’s different this time is that the company that was first to demonstrate the expected cost reductions was Chinese. This has never happened before and is geopolitically significant.”

What we say

Enterprise leaders should view DeepSeek as a critical point of reflection. A robust enterprise AI strategy should incorporate a blend of both open-source and closed-source AI models, avoid reliance on a single provider, and afford flexibility to interchange models seamlessly. With the regulatory environment around AI evolving quickly, many AI applications will necessitate high degrees of transparency. Achieving this level of transparency is challenging, if not impossible, with many closed-source models.

The bottom line

Both the U.S. and China have powerful AI models, but DeepSeek shows China is closing the capability gap with the U.S. in the AI race. The U.S. should take note. Open-source models such as Meta's Llama, Google's Gemma, and DeepSeek's R1 will play a critical role in the enterprise as organizations look to differentiate themselves with unique applications of AI applied to their enterprise data. Open-source models may offer more flexibility for customization and extension but will require emerging capabilities and new talent to configure and deploy, test comprehensively, identify vulnerabilities, and mitigate security risks. Expect AI red teaming to become more ubiquitous in the future as organizations continue to integrate both open- and closed-source AI into their enterprise architecture and business processes.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach, and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, digital, legal, HR, governance, risk, and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2024 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with smaller, growing companies, including those looking to go public, and with government agencies. Protiviti is a CMMCAB RPO organization and has been supporting companies with CMMC services for seven years. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

About VISION by Protiviti

VISION by Protiviti is a global content resource exploring big, transformational topics that will alter business in the future. Written for the C-suite and boardroom executives worldwide, *VISION by Protiviti* examines the impacts of disruptive forces shaping the world today and in the future. Through a variety of voices and a diversity of thought, *VISION by Protiviti* provides perspectives on what business will look like in a decade and beyond.

© 2025 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans.
Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.

protiviti®