My Employees Are Using DeepSeek. Should I Be Concerned?

Opinions expressed by Entrepreneur contributors are their own.

DeepSeek, the AI chatbot currently topping app store charts, has rapidly gained popularity for its affordability and functionality, positioning itself as a competitor to OpenAI's ChatGPT. However, recent reports suggest that DeepSeek may come with serious security concerns that business leaders cannot afford to ignore.

Here's a breakdown of its pros, cons and alternatives, so you can make the best AI optimization decisions for your business:

What is DeepSeek?

DeepSeek has positioned itself as a powerful AI tool capable of advanced natural language processing and content generation. Developed by China-based High-Flyer, DeepSeek has gained traction due to its ability to deliver AI-driven insights at a fraction of the cost of American alternatives (OpenAI's Pro Plan has already jumped up to $200/month). However, cybersecurity experts have raised alarm bells over its embedded code, which allegedly allows for the direct transfer of user data to the Chinese government.

Investigative reporting from ABC News revealed that DeepSeek's code includes links to China Mobile's CMPassport.com, a registry controlled by the Chinese government. This raises significant concerns about potential data surveillance, particularly for U.S.-based businesses handling sensitive

intellectual property, customer data, or confidential internal communications.

Related: Google’s CEO Praised AI Rival DeepSeek This Week for Its ‘Very Good Work.’ Here’s Why.

Echoes of TikTok’s privacy battle with China

DeepSeek’s security concerns follow a familiar pattern. TikTok, which faced a federal ban earlier this year, was caught in a legal and political tug-of-war due to concerns over its Chinese ownership and potential data security risks. Initially banned on January 19, TikTok was temporarily reinstated following President Trump’s intervention, with discussions on a forced sale to American investors still ongoing.

Despite ByteDance’s reassurances that U.S. user data is protected, national security experts have continued to raise concerns about potential Chinese government access to private information. TikTok’s brief ban underscored the heightened scrutiny surrounding foreign-owned digital platforms, particularly those linked to adversarial governments. Now, DeepSeek is facing similar questions — only this time, security experts claim to have found direct backdoor access embedded in its code.

Unlike TikTok, which denied direct government ties, DeepSeek’s alleged backdoor to China Mobile adds a new layer of risk. According to cybersecurity expert Ivan Tsarynny, DeepSeek’s digital fingerprinting capabilities extend beyond its platform, potentially tracking users’ web activity even after they’ve closed the app.

This means that companies using DeepSeek may be exposing not just individual employee data but also proprietary business

strategies, financial records and client interactions to unauthorized surveillance.

Related: Avoid AI Disasters With These 8 Strategies for Ethical AI

Should business leaders ban DeepSeek?

A knee-jerk reaction might be to ban DeepSeek outright, but that may not be the most practical solution. AI tools like DeepSeek offer significant efficiency gains, and the reality is that employees are often quick to adopt new technologies before leadership has time to assess the risks. Instead of an outright ban, leaders should take a strategic approach to AI integration.

Here are some best practices for AI optimization in your organization:

1. I**mplement AI Governance Policies:** Establish clear policies for AI adoption within your company. Define which tools are approved for business use, specify data security measures and educate employees on safe AI usage. AI governance should be part of your overall cybersecurity strategy.
2. **Segregate AI for Sensitive Data:** If employees are using AI tools like DeepSeek, restrict their use to non-sensitive tasks such as content brainstorming, general research, or customer service automation. Never allow AI tools with questionable security practices to access confidential financial records, proprietary data, or internal communications.
3. **Use Enterprise-Level AI Alternatives:** Encourage the use of vetted enterprise AI solutions with strict data security measures. Platforms like OpenAI’s ChatGPT Enterprise, Microsoft Copilot and Claude AI offer more

transparent privacy policies and allow companies to maintain greater control over their data.

4. **Monitor for Unauthorized AI Use:** Conduct regular audits of software usage across company devices. The recent viral “wiretap android test” demonstrated how easily apps can access user data without explicit permission. IT teams should proactively monitor for AI applications that may pose security risks and implement access restrictions when necessary.
5. **Educate Employees on AI Risks:** Employees should understand the potential risks associated with using foreign AI platforms. Awareness training on cybersecurity threats, data privacy laws and corporate policies will help ensure that AI usage aligns with the company’s risk tolerance.
6. **Stay Informed on AI Policy Changes:** The regulatory landscape for AI and data privacy is evolving. Governments worldwide are scrutinizing AI platforms, and companies should stay informed about potential bans, restrictions, or security advisories related to AI tools in their tech stack.

AI-powered platforms like DeepSeek offer compelling advantages, but they also introduce serious security risks that business leaders must consider. Entrepreneurs, CMOs, CEOs and CTOs should balance innovation with vigilance, ensuring that AI tools enhance productivity without compromising data security.

https://www.entrepreneur.com/science-technology/my-employees-are-using-deepseek-should-i-be-worried/487308