Nasdaq

DeepSeek and Beyond
Monthly Cybersecurity Update

January 2025

Ilaria Sangalli, Index Research Lead, Nasdaq

DeepSeek: the Chinese AI startup that challenged Silicon Valley

The entire technology sector was shaken when DeepSeek released V3, a large language model (LLM) allegedly trained on 2,048 Nvidia H800 chips, a less powerful version specifically designed by Nvidia for the Chinese market, following the US exports ban. DeepSeek disclosed that training the model required approximately over two months for a total of 2.788 million GPU hours[1]. At an estimated cost of $2 per GPU hour, the total training cost amounted to around $6 million, well below the $100 million required to train GPT-4.[2] If those claims were true, V3 would match the performance of top US models at a fraction of the cost.[3]

It will take time to shed light on the genesis of DeepSeek. However, the unexpected rise of the Chinese AI startup has already sparked debates on whether AI models can be trained more efficiently, achieving impressive results with fewer resources and less sophisticated chips. After some initial turbulence during the last week of January, markets have welcomed the disruptive challenge that DeepSeek represents, boosting returns of companies that rely on AI technologies. Besides the enthusiasm ignited by the perspective of a more cost-efficient AI, concerns related to cybersecurity could not be delayed, either.

DeepSeek's vulnerabilities strengthen demand for advanced cybersecurity solutions

DeepSeek itself experienced a large-scale cyberattack on the same day its app achieved the top position on the US App Store. The attack, uncovered by Wiz Research, has illicitly accessed DeepSeek's internal database, ClickHouse, which contains sensitive information, such as user chat histories, API keys[4], and log entries[5]. Registrations of new users were also disrupted.

Potential vulnerabilities of DeepSeek have been questioned by threat intelligence experts, that showcased some jailbreaks methods used to target popular AI models. Jailbreaks can challenge the security of AI models and are used to bypass safety mechanisms, which prevent the LLM from generating harmful or

[1] GPU hours refer to the total amount of computational time required to train a model on a GPU. It corresponds to the total number of hours spent by all GPUs used for training. This metric is helpful to estimate the cost and efficiency of training models. Total GPU hours = Number of GPUs x Hours used
[2] https://www.bbc.com/future/article/20250131-what-does-deepseeks-new-app-mean-for-the-future-of-ai
[3] DeepSeek used MoE (Mixture of Experts) technique, that helped the startup reduce computational costs. MoE is a technique where only parts of the model (experts) are activated at a time, instead of using the entire model for every task. This can make the model faster (not all parameters are used at once), more efficient (less computing power) and scalable (handling bigger models without massive costs)
[4] API Keys are authentication tokens used to access DeepSeek's services
[5] https://cybersecuritynews.com/deepseek-database-leaked/

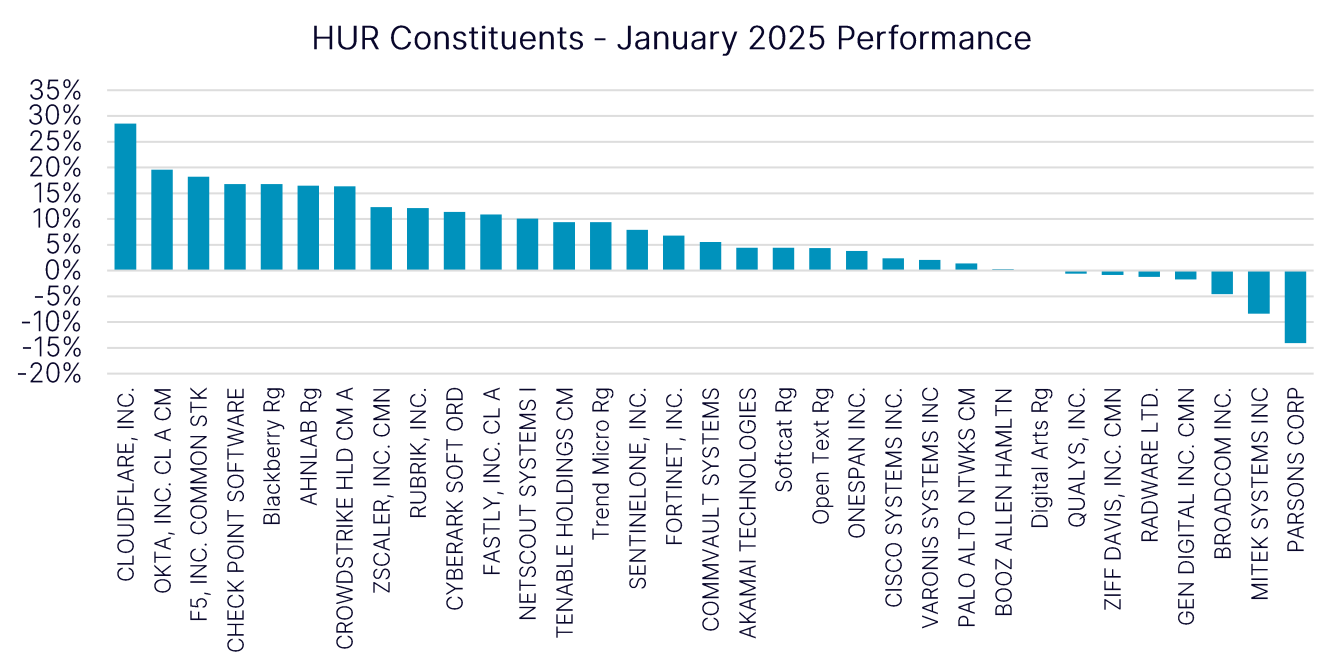
prohibited content. The cyber security intelligence company Kela highlighted that DeepSeek could be vulnerable to some jailbreaks against which ChatGPT is, instead, protected.[6,7] This pointed out some relevant security vulnerabilities within DeepSeek's infrastructure, reinforcing the major concern that cybercriminals could exploit AI systems for malicious activities.

There is no doubt that democratizing AI would improve efficiency and cost-effective solutions, but collateral impacts should not be ignored. The more AI technologies become widely used across several entities (consumers, enterprises, government functions), the higher the risk of new cyber-related threats. Demand for increasingly advanced cybersecurity solutions is on track for considerable growth in the near future.

A deeper (DeepSeek?) look at the ISE Cyber Security UCITS™ Index (HUR™)

In January 2025 the ISE Cyber Security UCITS™ Index (HUR™) registered 7.60% gains, overperforming the Nasdaq-100® (NDX®, up 2.22%) and S&P 500 (SPX, up 2.70%).

The index performance is a tangible consequence that, although reduced costs for AI technologies can negatively impact companies directly related to semiconductors and chips production, they are highly beneficial for the broader spectrum of the technology applications industry, including cybersecurity. AI has already been recognized as a pivotal technological trend which will transform how threats are detected and mitigated. As AI technologies become more affordable, their adoption in cybersecurity will become more widespread, leading to the proliferation of innovative and more effective security solutions. According to IBM, organizations using security AI and automation are saving on average $2.2 million on data breach costs.[8]



Price returns as of January 31, 2025, in USD

[6] https://www.securityweek.com/ai-jailbreaks-target-chatgpt-deepseek-alibaba-qwen/
[7] According to Kela, although many jailbreaks in ChatGPT have been patched over the years, researchers keep finding new bypasses
[8] https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec

Among the major AI players, only Broadcom resides in the index and was materially impacted by the DeepSeek news, dragging down the index performance by 0.18% for the month, while most other constituents, including Cloudflare, Okta, CrowdStrike, Fortinet and SentinelOne continued to perform well.

Cloudflare (index weight 6.13% as of January 31, 2025) increased by 28.53% over the month of January. Cloudflare has introduced an AI assistant within its Security Analytics dashboard to help users identify anomalies and cyberattacks more efficiently.[9]

Okta (index weight 0.58% as of January 31, 2025) jumped 19.57% during January. The market has responded positively to the company's strategy to integrate AI into its products. "Auth for GenAI" is an authentication platform for AI agents which automates the authentication process for these agents and provides a secure protocol to build bots around.[10] This will help address security challenges posed by the proliferation of AI-powered bots and agents.

CrowdStrike (index weight of 5.55% as of January 31, 2025) gained 16.34% last month. Its cybersecurity platform, Falcon, uses AI-threat intelligence to detect malware and sophisticated cyber-attacks.

SentinelOne (index weight of 5.02% as of January 31, 2025) delivered 7.88% performance in January. The company has been leveraging AI on its Singularity XDR platform, which is designed to protect computers, cloud environments and servers from cyberthreats. The platform also used behavioral AI to detect fileless malware.[11,12]

Fortinet (index weight of 5.10%, as of January 31, 2025) has posted gains of 6.77%. Fortinet's AI-powered security assistant, FortiAI, uses GenAI to help security teams make more informed decisions and quickly address threats.

Sources: Nasdaq Index Research, FactSet.

[9] https://blog.cloudflare.com/security-analytics-ai-assistant/
[10] https://investor.okta.com/static-files/0de0b68b-4284-48f3-bde0-c474882503df
[11] https://www.sentinelone.com/blog/behavioral-ai-an-unbounded-approach-to-protecting-the-enterprise/
[12] Traditional antivirus detects threats by matching them to a database of known malware. New attacks like fileless malware (which does not rely on traditional files or downloads to infect a system) can evade this method. Behavioural AI analyses activity patterns instead of relying on specific file signatures. It learns what "normal" behaviour looks like and can identify potential anomalies that indicate potential attacks.

Disclaimer: