# Hybrid cloud faces mounting AI-driven cyberthreats as deep observability emerges as critical defence



Hybrid cloud infrastructure is increasingly strained as artificial intelligence (AI) becomes more pervasive, creating new challenges for organisations trying to secure their environments. According to a recent report by Gigamon, cyberthreats are not only escalating in scale but also in sophistication, leading to a breach rate of 55% over the past year—a significant 17% increase compared to the previous year. This surge has been partly driven by the rise of AI-generated attacks, which have emerged as a critical concern for security professionals.

The economic toll of cybercrime is now estimated to be around $3 trillion globally, a staggering figure highlighted by the World Economic Forum. Against this backdrop, security teams find themselves grappling with outdated tools and fragmented cloud environments that hinder effective threat detection and response. Alarmingly, 46% of security and IT leaders cite managing AI-generated threats as their top security priority. In tandem, network data volumes have skyrocketed, with one-third of organisations reporting more than double the amounts encountered merely two years prior—largely due to the demands of AI workloads. Such an uptick has correlated with a rise in attacks specifically targeting large language models (LLMs), further complicating organisational responses.

In light of these vulnerabilities, many organisations are re-evaluating their cloud strategies. Originally, public cloud environments were viewed as optimally scalable following the disruptions of the COVID-19 pandemic. However, 70% of security and IT leaders now classify these environments as presenting greater risks compared to their private alternatives. Concerns around data security, particularly regarding intellectual property protection, have led to a noteworthy trend where 70% of organisations contemplate repatriating data from public to private clouds. This recalibration also reflects widespread unease surrounding existing security measures, with 55% of surveyed leaders lacking confidence in their tools' capacity to detect breaches effectively.

As organisations pivot towards a more comprehensive security posture, the concept of deep observability has surfaced as a crucial element in hybrid cloud management. With AI driving both traffic volume and complexity, 89% of security and IT leaders affirm the necessity of deep observability in securing hybrid cloud infrastructures. Chaim Mazal, the Chief Security Officer at Gigamon, states, “Deep observability provides that recalibration by combining traditional log data with network-derived telemetry, giving security teams clarity to see through encrypted traffic, detect AI-powered threats, and strengthen defences before the blast radius expands.” This sentiment is echoed across the board, with 88% of leaders acknowledging the importance of this approach for securing AI deployments, aligning with the broader trend of prioritising visibility in cybersecurity management.

Furthermore, the potential for exploits within AI systems is becoming increasingly pronounced, with 47% of organisations reporting targeted attacks against their LLM deployments. In conjunction with rising concerns over accountability and risk management, there is a growing urgency to integrate responsible AI practices. The US Commerce Department is proposing mandatory reporting for developers of advanced AI and cloud computing services to bolster resilience against cyberattacks, aligning with the increasing scrutiny that these technologies face from various stakeholders.

The challenges extend beyond security alone. A survey conducted by Hitachi Vantara reveals that nearly 37% of companies in the US view data quality as a major hurdle in successful AI implementation. With data requirements expected to grow by 122% by 2026, organisations are under pressure not only to manage vast quantities of data but also to ensure its integrity and security. This affirms the critical role of robust data governance as organisations strive to navigate complex cloud environments, optimal AI integrations, and comprehensive security frameworks.

As hybrid cloud strategies evolve, it is evident that organisations must thoughtfully address both security and operational complexities. The urgency for robust tools to achieve complete visibility and effective threat monitoring will dictate the next phase of cloud security, especially as adversaries continue to leverage AI for increasingly sophisticated attacks. As we move forward, deep observability will become foundational for protecting hybrid cloud environments, ensuring that organisations can respond swiftly and effectively to the fast-evolving landscape of cyber threats.

## Reference Map:

* Paragraph 1 – [[1]](https://www.helpnetsecurity.com/2025/05/26/ai-hybrid-cloud-infrastructure-concerns/)
* Paragraph 2 – [[1]](https://www.helpnetsecurity.com/2025/05/26/ai-hybrid-cloud-infrastructure-concerns/), [[2]](https://www.ft.com/content/202c3240-fa20-4081-a2a7-8470b7f12110)
* Paragraph 3 – [[1]](https://www.helpnetsecurity.com/2025/05/26/ai-hybrid-cloud-infrastructure-concerns/), [[4]](https://www.darkreading.com/cloud-security/ai-cloud-adoption-cyber-mistakes)
* Paragraph 4 – [[3]](https://www.reuters.com/technology/us-proposes-requiring-reporting-advanced-ai-cloud-providers-2024-09-09/), [[5]](https://www.prnewswire.com/news-releases/us-data-concerns-soar-as-ai-surges--37-of-it-leaders-identify-data-quality-as-major-barrier-to-ai-success-302326975.html), [[6]](https://www.fierce-network.com/cloud/cloud-migration-struggles-are-big-roadblock-ai-integration)

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.helpnetsecurity.com/2025/05/26/ai-hybrid-cloud-infrastructure-concerns/> - Please view link - unable to able to access data
2. <https://www.ft.com/content/202c3240-fa20-4081-a2a7-8470b7f12110> - This article discusses how AI-capable data centers are becoming strategic resources that governments are eager to control. It highlights the investments by countries like Saudi Arabia, the UAE, Kazakhstan, and Malaysia in AI data center infrastructure to become AI hubs. The piece also touches upon the concerns of U.S. cloud companies regarding partnerships with entities like G42, which have ties to Chinese tech firms, and the potential security risks involved.
3. <https://www.reuters.com/technology/us-proposes-requiring-reporting-advanced-ai-cloud-providers-2024-09-09/> - The U.S. Commerce Department has proposed mandatory reporting for developers of advanced AI and cloud computing providers to ensure safety and resilience against cyberattacks. The proposal includes reporting on development activities of 'frontier' AI models and computing clusters, as well as cybersecurity measures and outcomes from red-teaming efforts. This initiative aims to ensure these technologies meet safety and reliability standards and are protected from misuse by foreign adversaries or non-state actors.
4. <https://www.darkreading.com/cloud-security/ai-cloud-adoption-cyber-mistakes> - This article highlights common cybersecurity mistakes organizations make when adopting AI in the cloud. It discusses issues like granting overly permissive access to AI services, which can lead to security vulnerabilities. The piece emphasizes the importance of maintaining an inventory of cloud resources, monitoring for risky configurations, and promptly remediating them to enhance security in AI cloud environments.
5. <https://www.prnewswire.com/news-releases/us-data-concerns-soar-as-ai-surges--37-of-it-leaders-identify-data-quality-as-major-barrier-to-ai-success-302326975.html> - A survey by Hitachi Vantara reveals that 37% of U.S. companies identify data as their top concern when implementing AI projects. The survey underscores the critical role of data infrastructure and management in AI success and highlights gaps in data governance, security, and sustainability. It also notes that the amount of data required for AI is expected to increase by 122% by 2026, posing challenges for organizations in managing and ensuring data quality.
6. <https://www.fierce-network.com/cloud/cloud-migration-struggles-are-big-roadblock-ai-integration> - This article discusses the challenges enterprises face in cloud migration, which hinder AI integration. It highlights issues like security concerns, high costs, and outdated infrastructure. The piece also points out that incomplete cloud migrations are limiting AI effectiveness and recommends strategies such as direct cloud connections, scalable workflows, and private cloud solutions to enhance data movement and optimize AI performance.
7. <https://taikun.cloud/top-hybrid-cloud-trends-for-2022-2023-and-what-to-do-about-it/> - This article outlines key trends in hybrid cloud for 2022-2023, including operational complexity, cost management, compliance and privacy concerns, disparate cloud operating models, and lack of visibility and control. It emphasizes the need for organizations to address these challenges to effectively implement hybrid cloud strategies and achieve desired business outcomes.