# Insights into cloud security challenges and trends for 2025



A recent report titled the “2025 State of Cloud Security Report,” published by Fortinet in association with Cybersecurity Insiders, has revealed notable insights into the current trends and challenges organisations face in the realm of cloud security. The report synthesises data from over 800 cybersecurity professionals and serves as a valuable reference for organisations aiming to enhance their cloud security frameworks while exploring innovations in cloud services.

Despite a burgeoning trend in cloud adoption, the report highlights a substantial decline in confidence regarding the real-time handling of cloud threats. A staggering 95% of respondents expressed moderate to extreme concern over cloud security, while 76% reported experiencing direct impacts of these concerns. The report identifies the prevailing skills shortage as a significant hurdle in addressing these issues. Vincent Hwang, Vice President of cloud security at Fortinet, emphasised that challenges within the sector can be somewhat alleviated through increased automation and the upskilling of existing staff, especially when hiring additional resources may not be feasible.

Among the strategies adopted for cloud deployment, the report indicates a preference for hybrid models, with 54% of organisations selecting this approach. Multi-cloud strategies followed closely at 28%, while only 18% opted for a single-cloud setup. The data shows a marked trend towards multi-cloud utilisation, with 78% of organisations reported using two or more cloud providers. Smaller businesses tend to favour single-cloud solutions, as their flexibility and management cost considerations differ from larger enterprises.

The report elucidates various challenges faced during cloud technology adoption. The most significant concern for 61% of organisations was adhering to security and regulatory requirements, while 54% cited organisational and operational difficulties. Furthermore, 51% of respondents reported facing resource constraints. Notably, protecting data security and privacy emerged as the most critical operational challenge, highlighted by 63% of organisations, and the figure escalated to 58% in the context of multi-cloud environments.

In terms of the essential skills required within the industry, cloud and application security skills topped the list at 65%, followed by identity and access management capabilities at 61%, and advanced technical security skills at 58%. Furthermore, a significant 97% of respondents indicated the value of a unified cloud security platform, with many acknowledging the benefits of a single dashboard for managing security configurations across their entire cloud infrastructure.

Industry experts provided their insights on navigating these challenges. Rom Carmel, CEO of Apono, pointed out the necessity for IT security teams to collaborate closely with engineering teams, stating, “The adoption of the cloud created a situation where engineering and operation teams are the ones creating and maintaining infrastructure...IT security teams must work closely with these engineering teams to build processes to enforce security guardrails constantly as part of managing a dynamic environment.”

Nicole Carignan, Vice President of Strategic Cyber AI at Darktrace, highlighted the importance of visibility in cloud security. “For organisations to effectively manage IAM and compliance, you cannot protect what you cannot see,” she noted, explaining how AI-driven solutions can enhance visibility across multi-cloud environments, facilitating real-time threat detection and response.

Amit Zimerman, Co-Founder and Chief Product Officer at Oasis Security, underscored that cloud security is a “multifaceted challenge that requires both strategic planning and operational excellence.” He advocated for organisations to utilise modern tools that can deliver comprehensive analytics, processing large data volumes to identify and prioritise vulnerabilities effectively.

Overall, the report indicates that while the complexities associated with adopting cloud technologies continue to escalate, the potential benefits are compelling enough to sustain growing interest from organisations. As the landscape of cloud adoption expands, the necessity of addressing emerging security concerns becomes increasingly paramount.

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

## Bibliography

1. <https://cyble.com/knowledge-hub/top-cloud-security-challenges/> - Corroborates the challenges in cloud security, including rapid technological changes, persistent misconfigurations, and the need for AI automation and zero-trust models.
2. <https://cmitsolutions.com/oakpark-il-1005/blog/2025s-biggest-cloud-security-challenges-are-you-ready-to-protect-your-business/> - Supports the top cloud security risks in 2025, such as data breaches, ransomware attacks, and the importance of encryption and zero-trust security frameworks.
3. <https://spacelift.io/blog/cloud-security-statistics> - Provides statistics on cloud security breaches, the prevalence of misconfigurations, and the concerns around multi-cloud environments and resource constraints.
4. <https://cyble.com/knowledge-hub/top-cloud-security-challenges/> - Highlights the significance of addressing misconfigurations and the lack of qualified staff in cloud security management.
5. <https://cmitsolutions.com/oakpark-il-1005/blog/2025s-biggest-cloud-security-challenges-are-you-ready-to-protect-your-business/> - Emphasizes the importance of proactive cybersecurity measures, including real-time logging tools and employee education, to mitigate cloud security risks.
6. <https://spacelift.io/blog/cloud-security-statistics> - Details the operational and security worries related to cloud migration, such as hijacking of accounts and privacy/data access issues.
7. <https://cyble.com/knowledge-hub/top-cloud-security-challenges/> - Discusses the focus on non-human identities (NHIs) and the accelerated adoption of zero-trust models as key trends in cloud security for 2025.
8. <https://cmitsolutions.com/oakpark-il-1005/blog/2025s-biggest-cloud-security-challenges-are-you-ready-to-protect-your-business/> - Explains the financial and reputational impacts of data breaches and the necessity of robust security measures like encryption and zero-trust frameworks.
9. <https://spacelift.io/blog/cloud-security-statistics> - Highlights the challenges in maintaining consistent regulatory standards and ensuring compliance across hybrid or multi-cloud environments.
10. <https://cyble.com/knowledge-hub/top-cloud-security-challenges/> - Mentions the investment in posture management tools and the importance of real-time visibility into cloud configurations for compliance monitoring and automated remediation.
11. <https://cmitsolutions.com/oakpark-il-1005/blog/2025s-biggest-cloud-security-challenges-are-you-ready-to-protect-your-business/> - Discusses how cloud providers are innovating to address cloud security risks, such as AI-driven threat detection and centralized encryption management.
12. <https://informationsecuritybuzz.com/fortinets-state-of-cloud-security-insights/> - Please view link - unable to able to access data