**Vendor Lock-In Issues:**

The main issues with vendor lock-in, according to the authors, are data migration difficulties, restricted connectivity, and rigidity when utilising several CSPs. These result from customers being unable to quickly transfer providers due to exclusive APIs, tools, and services. Organisations should use open standards to assure data portability, embrace multi-cloud strategies, and refrain from relying too heavily on proprietary services to reduce these. Furthermore, by minimising reliance on a single CSP, hybrid cloud models and third-party management tools can increase flexibility and lower the risk of lock-in.

**Cloud Security Concerns:**

The writers draw attention to issues including unclear shared responsibility, partial erasure of sensitive data, and data breaches. These can be lessened by utilising zero trust models, strong key management systems, encryption—both at rest and in transit—and incident response coordination with CSPs. Furthermore, full coverage may be ensured by integrating on-premises monitoring with cloud-native security solutions like AWS CloudTrail and Macie. Regular security audits and updates also aid in addressing new threats.