European Science Review 2026,
No 1–2
ISSN 2310-5577

PREMIER Publishing
ppublishing.org

Section 9. Applied Research: Information Technology

DOI:10.29013/ESR-26-1.2-78-84

NAVIGATING THE THREAT LANDSCAPE: A COMPREHENSIVE ANALYSIS OF SECURITY CHALLENGES IN MULTI-CLOUD ENVIRONMENTS

Agbanwu Joshua Ojomiache [1], ***Agbanwu Jedidiah Alefia*** [1]

[1] Undergraduate student, Federal University of Technology Minna, Nigeria

Cite: *Agbanwu Joshua Ojomiache, Agbanwu Jedidiah Alefia (2026). Navigating the Threat Landscape: A Comprehensive Analysis of Security Challenges in Multi-Cloud Environments. European Science Review 2026, No 1–2.* https://doi.org/10.29013/ESR-26-1.2-78-84

Abstract

The rapid adoption of multi-cloud architectures introduces unprecedented security challenges stemming from architectural complexity, fragmented data governance, inconsistent identity management, and heightened compliance burdens. This paper provides a systematic analysis of the unique vulnerabilities inherent in multi-cloud environments, drawing on recent industry reports, case studies, and empirical research. Key findings reveal a 332% increase in policy violations, a 71% higher frequency of security incidents, and significant risks in data privacy, Identity and Access Management (IAM) fragmentation, and compliance drift. The study concludes with a call for integrated, adaptive security frameworks to mitigate these evolving threats.

Keywords: *Multi-Cloud Environments, Cloud Security, Security Challenges, Threat Landscape, Architectural Complexity, Expanded Attack Surface, Data Fragmentation, Data Privacy, Encryption Gaps, Identity and Access Management (IAM), IAM Fragmentation, Compliance Fragmentation, Visibility Gaps, Monitoring, API Vulnerabilities, Misconfigurations, Zero Trust, STRIDE, DREAD*

1. Introduction & Background

Cloud computing has evolved decisively from single-provider models to sophisticated multi-cloud strategies, driven by vendor diversification, regulatory requirements, and service optimization. While offering enhanced flexibility and scalability, multi-cloud environments introduce a fragmented security landscape characterized by inconsistent policies, expanded attack surfaces, and profound operational complexity. Recent data indicates that 91% of organizations now use multiple cloud service providers, facing a 71% higher frequency of security incidents compared

to single-cloud deployments (Palo Alto Networks, 2023; Khan, 2025). This paper critically examines the unique security challenges posed by multi-cloud architectures, providing a foundation for developing resilient security postures.

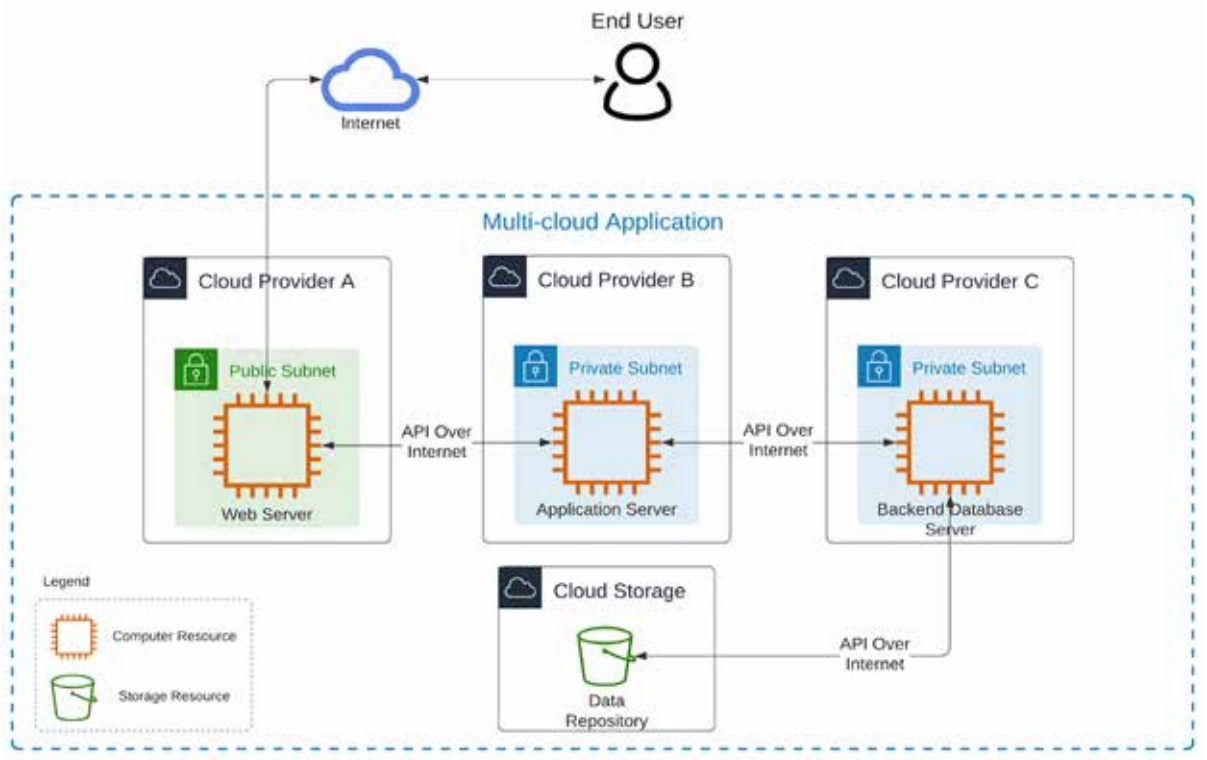
2. Architectural Complexity & Expanded Attack Surface

The fundamental architecture of multi-cloud environments inherently increases security complexity through several key architectural mechanisms that collectively expand the attack surface. Heterogeneous security models create translation gaps between different cloud providers' security frameworks and policy languages. Fragmented data pathways introduce encryption discontinuities and visibility gaps during inter-cloud data transit. Inconsistent identity systems across platforms require complex federation that expands credential-based attack vectors. Combinatorial configuration states grow exponentially with each added provider, creating a vast and continuously evolving attack surface.

Unlike single-cloud deployments, multi-cloud architectures create emergent vulnerabilities at the intersections of disparate cloud ecosystems that are not merely additive but multiplicative in nature. This multiplicative risk occurs because each additional cloud provider introduces not only its own attack surface, but also unique interoperability requirements, policy translation challenges, and monitoring gaps that collectively amplify security complexity beyond simple accumulation.

With 87% of organizations distributing workloads across at least three cloud service providers, the attack surface expands dramatically (Shackleford, 2024). Identity-centric security is paramount, as emphasized by the Identity Defined Security Alliance, which roots Zero Trust in identity with data access as the ultimate objective (Joshi, 2025). Risk analysis using STRIDE and DREAD frameworks confirms that authentication and architectural integrity are the highest-risk areas in multi-cloud setups (Reece et al., 2023).

Figure 1. *Three-Tier Web Application Architecture in Multi-Cloud (Reece et al., 2023)*



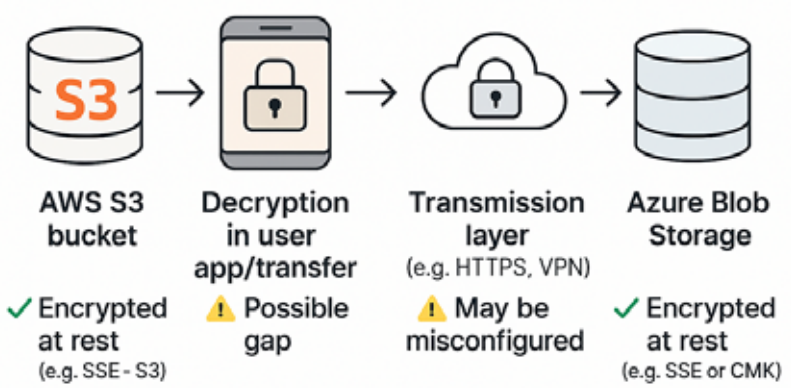
This diagram illustrates a typical multi-cloud deployment with web, application, and database servers distributed across different cloud providers. It visually represents how architectural complexity expands the attack surface.

Attackers exploit this expansion: IBM's X-Force report notes a 69% year-over-year increase in API-based attacks targeting multi-cloud environments (IBM, 2024). Additionally, 82% of organizations report that securing applications across multiple clouds is their primary technical challenge (Fortinet, 2024.

3. Data Fragmentation and Privacy Risks

Data distributed across multiple clouds suffers from encryption gaps during inter-cloud transit, increasing the risk of unauthorized access. A 2023 Cloud Security Alliance report found that 68% of enterprises experienced encryption misconfigurations. Data sovereignty and fragmentation are critical, with Thales reporting that 51% of organizations experienced at least one cloud data breach in the past year, and multi-cloud users face 2.3 times higher rates of data exposure (Thales, 2023). A primary issue is lack of visibility: 42% of organizations cannot fully track where their sensitive data resides across providers (Thales, 2023). Figure 2 illustrates the encryption gap risk during inter-cloud transit.

Figure 2. *Encryption Gaps During Inter-Cloud Transit*



The diagram illustrates vulnerability when moving data between AWS S3 and Azure Blob Storage, where data encrypted at rest may be decrypted during transit if misconfigured.

Recent studies highlight that 40% of organizations in Singapore experienced a cloud security breach in the last 12 months, with 82% storing sensitive data in the cloud but only 41% encrypting it (Thales, 2024).

4. IAM Complexity Across Clouds

Each cloud provider enforces distinct Identity and Access Management (IAM) policies, making unified access control a fundamental challenge. Mismanaged roles and over-privileged accounts contribute to approximately 42% of cloud-related breaches (IBM, 2023). Compromised credentials are involved in 68% of cloud security breaches, with multi-cloud organizations particularly vulnerable due to fragmented systems (IBM, 2024). Organizations maintain an average of 45 distinct access policies per application, and 79% of security leaders cite inconsistent identity controls as their primary challenge (StrongDM, 2024). This results in significant overprivilege: 32% of cloud identity permissions are unused yet active, contributing to 76% of cloud security incidents (StrongDM, 2024). See Table 1: IAM Frameworks Comparison (AWS IAM vs. Azure AD vs. GCP IAM)

Table 1. *IAM Frameworks Comparison (AWS IAM vs. Azure AD vs. GCP IAM)*

Feature / Aspect	AWS IAM	Azure AD (Active Directory)	GCP IAM	Policy Inconsistencies & Notes
Core Identity Service	AWS Identity and Access Management (IAM)	Azure Active Directory (Azure AD)	Google Cloud IAM	Different naming, scope, and integration.

Feature / Aspect	AWS IAM	Azure AD (Active Directory)	GCP IAM	Policy Inconsistencies & Notes
Policy Language	JSON-based	JSON + Azure RBAC	IAM Policy (YAML/JSON)	AWS: Action-Resource-Effect; GCP: Role-Binding; Azure blends both.
Granularity of Control	Fine-grained (per API call)	Role-based (RBAC), less granular	Fine-grained with custom roles	Azure is less granular unless using PIM or Conditional Access.
Resource Hierarchy	Account → Resource	Tenant → Subscription → Resource Group → Resource	Organization → Folder → Project → Resource	GCP/Azure offer better logical grouping for large orgs.
Temporary Credentials	STS Tokens, IAM Roles	Azure AD Conditional Access + PIM	Service Account Impersonation	Inconsistent implementation and terminology.
Policy Evaluation Order	Deny > Allow	Deny > Allow (via Conditional Access)	Allow if any binding grants access	AWS/Azure prioritize «Deny»; GCP assumes allow if a role grants it.
Logging and Audit	AWS CloudTrail	Azure Monitor / Azure AD Logs	Cloud Audit Logs	All support audit trails, but log structure and access vary widely.

Highlights disparities in policy language, granularity, resource hierarchy, and evaluation logic.

Recent data shows that 88% of organizations struggle with over-privileged identities across multi-cloud infrastructure, and 95% have identities with enabled but unused permissions (Microsoft, 2023).

5. Compliance Fragmentation

Maintaining continuous compliance across heterogeneous clouds is notoriously resource-intensive. Organizations navigate an average of 13.4 distinct compliance frameworks simultaneously, consuming 33% of security team resources (Orca Security, 2024). Regulatory frameworks like GDPR, HIPAA, and PCI-DSS require uniform implementation, yet native tooling and standards vary by provider. For example, a PCI-DSS encryption standard may be native in AWS but require third-party tooling in Azure, creating policy blind spots. Only 29% of firms achieve comprehensive, real-time compliance monitoring across multi-cloud setups (Palo Alto Networks, 2023).

The global GRC market is projected to grow from USD41.74 billion in 2023 to USD101.89 billion by 2033, driven by multi-cloud adoption (Business Research Insights, 2024). Organizations in Asia Pacific cite regulatory compliance as a major concern, with 45% struggling to manage compliance across multiple clouds (Thales, 2024).

Visibility, Monitoring Gaps, and Expanded Attack Surface

6. Visibility, Monitoring Gaps, and Expanded Attack Surface

The distributed nature of multi-cloud environments creates significant visibility challenges. Sysdig's 2023 report indicates that multi-cloud environments experience 332% more security policy violations than single-cloud deployments, with nearly 1,900 critical misconfigurations daily (Isbitski, 2023). A comprehensive analysis reveals that 61% of enterprises lack centralized log consolidation capabilities from AWS, Azure, and GCP, delaying incident response (Potla, 2025). Security teams face an average of 2,846 security alerts daily 47% more than single-cloud deployments with sophisticated attackers explicitly targeting these gaps (Microsoft, 2024).

Table 2: Multi-Cloud Security Incident Analysis by Region (2023–2024)

Region	Security Incidents	Avg Response Time (hrs)	Data Breaches	Financial Impact (USD M)
APAC	1,247	18.5	342	4.8
North America	2,183	12.3	486	6.2
Europe	1,856	14.7	397	5.5

Shows variation in incidents, response times, and financial impacts across regions.

Organizations without unified monitoring experience a median dwell time of 204 days for attackers moving laterally, compared to 38 days for those with cross-cloud visibility (Microsoft, 2024).

7. Specific Attack Vectors in the Expanded Surface

- API Vulnerabilities: APIs facilitating inter-cloud communication are high-value targets if not secured with strong authentication, rate limiting, and auditing. The 2022 Oracle API breach exposed over 10 million records due to weak authentication (Krebs, 2022).
- Container Orchestration Misconfigurations: Vulnerabilities in Kubernetes clusters (e.g., exposed dashboards) can lead to widespread compromise.
- Serverless Function Exploitation: Insecure deployment of functions (AWS Lambda, Azure Functions) can expose backend resources.
- Misconfigured Storage Services: Publicly accessible cloud storage buckets remain a rampant source of leaks, with 78% of cloud data breaches involving improperly controlled storage resources (Thales, 2024).
- Cloud Supply Chain Compromises: As seen in the SolarWinds incident, dependencies on shared services or third-party code libraries can introduce systemic vulnerabilities that propagate across environments.

Table 3. *STRIDE/DREAD Risk Analysis of Multi-Cloud Attack Vectors*

Threat Vector	DREAD Score	Risk Level	Primary Mitigation
Architecture: DoS Attacks	42.67	Critical	WAF with DoS mitigation
Authentication: Man-in-the-Middle	32.67	High	DNSSEC, static network config
API: Privilege Elevation	28.00	High	PAM, least privilege
Compliance: Data Privacy Laws	22.00	Medium	Regulatory compliance automation

Quantifies risks associated with architectural, API, authentication, automation, and compliance attack vectors.

8. Conclusion

The multi-cloud paradigm, while offering significant business advantages, introduces a complex and expanded threat landscape characterized by architectural fragmentation, data privacy risks, IAM inconsistencies, compliance burdens, and visibility gaps. The statistics presented—332% more policy violations, 71% higher incident frequency, and significant dwell time disparities—underscore the urgent need for integrated security approaches. Future efforts must prioritize unified visibility, automated compliance, and identity-centric security models to mitigate these evolving risks. This paper lays the groundwork for subsequent research into adaptive security frameworks capable of safeguarding distributed cloud ecosystems.

References

Burgess, M. (2023, July 11). A Microsoft Azure bug exposed customer data for years. WIRED. https://www.wired.com/story/microsoft-azure-bug-exposed-customer-data/

Business Research Insights. (2024). Governance Risk Management and Compliance (GRC) market size, share, growth, and industry analysis, by type, by application, regional forecast by 2033. https://www.businessresearchinsights.com/market-reports/governance-risk-management-and-compliance-grc-market-102540

Cloud Security Alliance. (2023). State of cloud security concerns: Challenges and misconfigurations. https://cloudsecurityalliance.org/research/state-of-cloud-security-concerns/

CrowdStrike. (2024). 2024 Global Threat Report. CrowdStrike Intelligence. https://www.crowdstrike.com/global-threat-report/

Cybersecurity Asia. (2024). 2024 Thales Cloud Security Study: Cloud resources now Singapore's biggest targets for cyberattacks. https://cybersecurityasia.net/2024-thales-cloud-security-study-released/

Fortinet. (2024). Key findings from the 2024 Cloud Security Report. https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2024-cloud-security.pdf

IBM Security. (2023). Cost of a data breach report 2023. IBM Corporation. https://www.ibm.com/reports/data-breach

IBM Security. (2024). IBM X-Force Threat Intelligence Index 2024. IBM Security Research. https://www.ibm.com/reports/threat-intelligence

Isbitski, M. (2023). Sysdig 2023 cloud-native security and usage report. Sysdig Research. https://sysdig.com/blog/2023-cloud-native-security-usage-report/

Jada, I., & Mayayise, T. O. (2024). *T*he impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. *Data and Information Management, 8(2), 100063*. https://doi.org/10.1016/j.dim.2024.100063

Joshi, H. (2025). Emerging technologies driving Zero Trust maturity across industries. *IEEE Open Journal of the Computer Society, 6, 25–34*. https://doi.org/10.1109/OJCS.2024.3503056

Khan, R. S. (2025). Security challenges and mitigation strategies in multi-cloud environments: A comprehensive analysis. *World Journal of Advanced Research and Reviews, 26(01), 3725–3731*. https://doi.org/10.30574/wjarr.2025.26.1.1502

Krebs, B. (2022, June 10). Oracle bug allowed anyone to hijack any AWS account. Krebs on Security. https://krebsonsecurity.com/2022/06/oracle-bug-allowed-anyone-to-hijack-any-aws-account/

Markets and Markets. (2024).Cloud Security Posture Management Market by Component (Solutions and Services), Cloud Model (IaaS, PaaS, and SaaS), Vertical (BFSI, Healthcare, Retail & eCommerce, IT & ITeS, Government, and Education) and Region Global Forecast to 2027. https://www.marketsandmarkets.com/Market-Reports/cloud-security-posture-management-market-71228949.html

Microsoft. (2023). 2023 State of Cloud Permissions Risks report. Microsoft Entra. https://www.microsoft.com/entra/cloud-permissions-risk-report

Microsoft. (2024). Microsoft Digital Defense Report 2024. Microsoft Security Insider. https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024

Orca Security. (2024). What is multi-cloud compliance? Orca Security Research. https://orca.security/resources/blog/what-is-multi-cloud-compliance/

Palo Alto Networks Unit 42. (2023). Cloud Threat Report, Vol. 7. Palo Alto Networks, Inc. https://www.paloaltonetworks.com/unit42/cloud-threat-report-vol-7

Potla, S. (2025). Securing multi-cloud environments: Challenges and solutions. *Journal of Computer Science and Technology Studies, 7(4), 780–785*. https://doi.org/10.32996/jcsts.2025.7.4.90

Reece, M., Lander Jr., T. E., Mittal, S., Rastogi, N., Dykstra, J., & Sampson, A. (2023). Systemic risk and vulnerability analysis of multi-cloud environments. arXiv preprint arXiv:2306.01862.

Shackleford, D. (2024). Multi-cloud security challenges and best practices. TechTarget SearchSecurity. https://www.techtarget.com/searchsecurity/tip/Multi-cloud-security-challenges-and-best-practices

StrongDM. (2024). The State of Zero Trust Security in the Cloud Report. StrongDM Research. https://www.strongdm.com/blog/state-of-zero-trust-security-cloud

Thales Group. (2023). Data Threat Report 2023 – Pathways to Sovereignty. Thales Cloud Security Research. https://cpl.thalesgroup.com/2023/data-threat-report

Thales Group. (2024). 2024 Cloud Security Study. Thales Group. https://cpl.thalesgroup.com/cloud-security-research

Wiz. (2024). Cloud Security Report 2024. https://www.wiz.io/cloud-security-report-2024

submitted 02.02.2026;
accepted for publication 16.02.2026;
published 28.02.2026

Contact: joshuaagbanwu@gmail.com, agbanwujedidiah@gmail.com