Next-Generation Database Hardening and Threat Visibility Framework for Hybrid AWS-Azure Clouds with Wiz Analytics

Nareddy Abhireddy
Independent Researcher
nareddy.abhireddy.researcher@gmail.com

Abstract

Cloud services allow enterprises to establish hybrid, multi-cloud environments. Such proliferation increases complexity and the attack surface, leading to needed security-, privacy-, and accessibility-compliance controls. Existing tools underutilize cloud providers' compliance tools. Wiz automates asset inventory, vulnerability management, compliance drift detection, risk insights, and identity and access management. Cloud-integrated database hardening uses Wiz insights and guidance to automate hardening and compliance in heterogeneous clouds. Assets—data stores, storage accounts, and databases—proliferate in Azure and AWS, often within a single logical entity. A framework automates security posture, improving cloud-integrated database hardening in hybrid AWS–Azure environments. Data collection and telemetry follow Wiz-driven insights. Controls satisfy technical risks for hybrid asset-sharing scenarios. Attack surfaces and risks in heterogeneous AWS–Azure environments are specified and mitigated. Security controls are mapped to family and subfamily participants. Identity and access management splits responsibilities between Azure and AWS security flaws. Database service encryption meets Azure Secrets store and KMS risk categories.

The threat landscape of hybrid solutions is broader than that of single- or multi-cloud deployments. Data-exfiltration-database-leaking-risk scenarios for Azure are addressed by Wiz identity and access management recommendations and Microsoft and AWS database-service data-in-transit-and-at-rest-encryption controls. These recommendations automate security-compliance attestation. Azure data resource characteristics and Wiz approach are combined with risk categories for remaining clouds. A simple security-architecture pattern for control-expression mapping creates the required hardening.

Keywords : Cloud-integrated database security,Hybrid cloud security architecture,AWS–Azure hybrid environments,Database hardening framework,Cloud security posture management (CSPM),Automated security posture assessment,Wiz security insights,Multi-cloud risk visibility,Cloud-native database protection,Zero trust data security,Security posture automation,Misconfiguration detection in cloud databases,Compliance monitoring in hybrid clouds,Continuous security assurance,Cloud attack surface management,Identity and access management for databases,Infrastructure-as-code security validation,Threat modeling for hybrid databases,Cross-cloud governance and controls,DevSecOps-driven database security.

1. Introduction

Cloud services have grown to play a central role in enterprise and service delivery infrastructure. Hybrid solutions leveraging multiple vendors are increasingly deployed for practical reasons rather than for provisioning resiliency. Azure and AWS provide services that natively interoperate; however, new security considerations arise when data is shared between them.

Recently, few cloud-native approaches have explicitly focused on compliance-driven security management of Azure and AWS hybrid environments. Wiz — a cloud

ISSN: 3050-9696
E-ISSN: 3050-970X
EUROPEAN ADVANCED JOURNAL FOR SCIENCE & ENGINEERING
Volume: 03 Issue: 03
RECEIVED: JULY 22 REVISED: AUGUST 09 ACCEPTED: AUGUST 25 PUBLISHED: SEPTEMBER 07

security posture management solution — integrates cloud graph unification to reveal telecommunications between workloads as well as across different clouds. Its output not only meets security standards but also provides actionable recommendations that align with the MITRE ATT&CK framework. The approach employs the Wiz portal APIs to automate the architecture and continuously safeguard the workloads. The guidance issued by Wiz leads to an overall hardened state of the hybrid workloads.

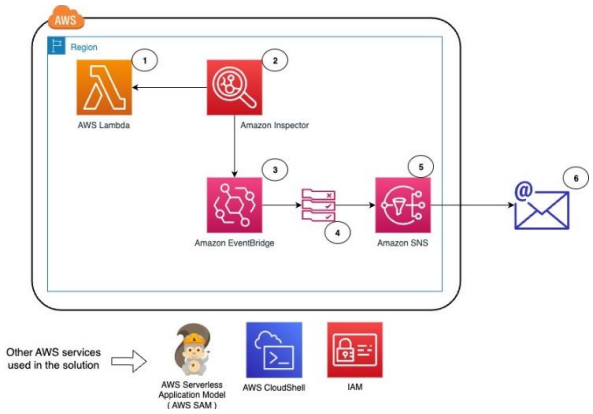
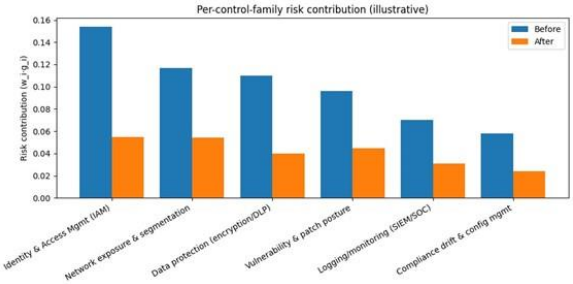


Fig 1: AWS-Azure Environments

2. Background and Problem Statement

Securing database services in public clouds is not a matter of whether but when. Leaked credentials can be especially damaging when attackers gain access to public cloud databases that process sensitive data or contain confidential information. Cloud databases can be made visible to everyone without authentication at their endpoints and can therefore be hacked by script kiddies. A database's security posture represents its current security level in relation to others; it does not guarantee absolute immunity from attacks but can help minimize exposure and greatly reduce the risk of data leakage or compromise. As organizations move their workloads and databases to the cloud and up-to-date tools become available, the security posture of cloud databases should be automated.

Misconfiguration, inadequate access management, data exposure, and inadequate control of cloud resources represent the top cloud security threats. Databases residing in hybrid AWS-Azure environments are particularly vulnerable because they can be configured with higher severity than in mono-cloud environments, increasing the severity of misconfigurations and attack surfaces. Wiz has introduced a unified security platform for cloud environments. Its insights provide a detailed representation of cloud resources and services, revealing misconfigurations. Database hardening strategies in AWS provide the foundation for hardening in Azure, helping determine how to harden databases in hybrid environments. Nevertheless, although recommended hardening strategies have been developed for cloud databases, their implementation often remains a manual activity requiring specialist knowledge.



3. Related Work

As organizations increasingly adopt hybrid cloud infrastructures, security becomes a major concern. Environment complexity and the resulting dependence on third-party managed services and applications underscore the need for improved security. This includes, where possible, the remediation of unsecured service configurations, which cloud providers expose on their dashboards or via audit reports. Such configuration requests can suffer delays and backlogs, as organizations must often work on many such requests simultaneously.

ISSN: 3050-9696 E-ISSN: 3050-970X
EUROPEAN ADVANCED JOURNAL FOR SCIENCE & ENGINEERING
Volume: 03 Issue: 03
RECEIVED: JULY 22 REVISED: AUGUST 09 ACCEPTED: AUGUST 25 PUBLISHED: SEPTEMBER 07

Cloud-agnostic services are one way to tackle this issue. Multiple cloud providers currently offer such solutions or skeleton services. Wiz, a cloud-native security platform that concentrates on resolving security-related issues and configuration errors, is one such system. Wiz's purpose-built organizational portal presents an overview of the entire AWS–Azure security posture, integrates comprehensive sensor-based coverage of cloud assets and services, and generates prioritized risk items based on Microsoft Attack Nader and Cloud Navigators to Cloud Risk Management Frameworks.

Equation 1: Derived equations (step-by-step) aligned to the paper

We can formalize this as a **weighted gap model**:

Step 1 — Define control families
Let there be n control families (examples consistent with the paper):

- IAM
- Network exposure/segmentation
- Data protection (encryption/DLP)
- Vulnerability & patch posture
- Logging/monitoring (SIEM)
- Compliance drift/config mgmt

Step 2 — Define a normalized "gap" per family
For each family i, define a gap score:

$$g_i \in [0,1]$$

- $g_i = 0$: fully hardened (no relevant gap)
- $g_i = 1$: worst gap level

Step 3 — Define importance weights
Assign weights $w_i \geq 0$ such that:

$$\sum_{i=1}^{n} w_i = 1$$

Step 4 — Compute total (weighted) residual risk
Define "residual risk" as the weighted sum of gaps:

$$R = \sum_{i=1}^{n} w_i \, g_i$$

Step 5 — Convert residual risk to a posture score
A simple posture score is the complement:

$$P = 1 - R = 1 - \sum_{i=1}^{n} w_i \, g_i$$

- $P \to 1$ means strong posture (few gaps)
- $P \to 0$ means weak posture

Step 6 — Show improvement via automation
If automation (Wiz insights + scripts) reduces gaps from $g_i^{(before)}$ to $g_i^{(after)}$, then:

$$\begin{aligned} \Delta P &= P_{after} - P_{before} \\ &= \left(1 - \sum w_i g_i^{(after)}\right) \\ &\quad - \left(1 - \sum w_i g_i^{(before)}\right) \\ &= \sum_{i=1}^{n} w_i \left(g_i^{(before)} - g_i^{(after)}\right) \end{aligned}$$

So posture improves exactly in proportion to **weighted gap reduction**, matching the paper's "detect → recommend → remediate" posture automation loop.

4. Architectural Overview

Databases are the cornerstones of online services. High availability, scalability, cost-effectiveness, performance, and responsiveness are primary engineering objectives for designing cloud-based databases. Databases are usually partitioned for low latency by retaining local replicas in hybrid cloud infrastructures. Cloud-integrated security solutions upgrade cloud security levels by deploying hybrid

ISSN: 3050-9696
E-ISSN: 3050-970X
EUROPEAN ADVANCED JOURNAL FOR SCIENCE & ENGINEERING
Volume: 03 Issue: 03
RECEIVED: JULY 22 REVISED: AUGUST 09 ACCEPTED: AUGUST 25 PUBLISHED: SEPTEMBER 07

models based on forensics, sandboxing, and behavior emulation. Wiz provides a cloud-integrated security solution to monitor assets, vulnerabilities, identity and access management-related problems, and recent threats from assets. Popular security postures like Centre for Internet Security Benchmarks should be implemented for these assets. The Wiz service uses a set of deployed modules, a telemetric exposure evaluation module, a query module, a command module, an API module, a GRC module, and a PubSub module with serverless logic, with the central Wiz service at the helm and directly connected via APIs to the core Wiz service. A novel Wiz-driven framework for cloud-assets, especially databases, in hybrid AWS-Azure environments employs the architecture.

Hybrid cloud infrastructures for online services offer cloud databases to users via AWS and Azure. Hybrid partitions of these cloud environments are leveraged to lower latency for users on different continents. Database replicas are maintained as close to users as possible, requiring a hybrid architecture. However, the assets in Azure are usually not provided by native Azure products but through compatible third-party products, introducing risk. Moreover, most of the deployed database services do not comply with database-security-benchmark documents, and the underlying control objectives and securities should be automatically addressed, configured, and secured through the hybrid architecture and the Wiz service. The proposed architecture aims to automatically implement control objectives mapping to a recognized database security-standard document and address the underlying security controls through the Wiz service.

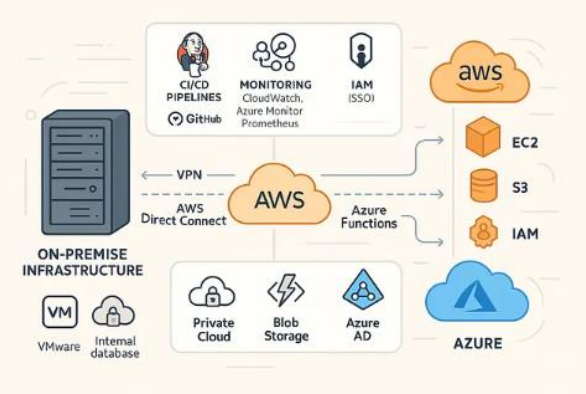


Fig 2: Hybrid Cloud Architecture Explained

4.1. Hybrid Cloud Databases in AWS and Azure

Hybrid database deployments typically employ a combination of managed, semi-managed, and un-managed databases from different service providers. Despite the advantages provided in queried data evaluation, all advantages vanish when it comes to the security of databases due to misconfiguration. Wiz.cloud, a cybersecurity company acquired by Microsoft Azure, provides security posture management for hybrid database deployments. Monitoring the cloud services deployed within the enterprise, it automatically suggests controls for hardening of the cloud. The need for hardening of databases deployed in public cloud services is recognized based on these suggested controls, and a framework is built to automate the hardening process based on the provided suggestions.

Since Wiz.cloud is integrated with Microsoft cloud services, the suggested controls are for hybrid deployment of databases between Amazon Web services and Microsoft Azure. Cloud control mapping is done to ensure that hardening of the databases is done as per the Control Objectives for Information and Related Technology. Misconfigured databases create the largest attack surface for cloud environments and implementing the suggested controls can secure at least 90% of the attack surface. These controls can be mapped against the Security Standards for Not-for-Profit Organizations security Domains

ISSN: 3050-9696
E-ISSN: 3050-970X
EUROPEAN ADVANCED JOURNAL FOR SCIENCE & ENGINEERING
Volume: 03 Issue: 03
RECEIVED: JULY 22 REVISED: AUGUST 09 ACCEPTED: AUGUST 25 PUBLISHED: SEPTEMBER 07

recommended by the Information Systems Audit and Control Association, which is a worldwide professional association.

4.2. Wiz-Driven Insights as a Core Automaton

The necessity of a standalone Wiz control automaton arose to avert a specific outcome of multi-cloud. Policy creation for Azure and AWS workloads in a single delivery in Wiz (for example, GCP information discovery) is still pending. Dissimilar cloud providers grant different visibility and readiness states for deployment/testing. Even the remediations offered tend to differ in framework. It is pointless to (attempt to) build an AWS resource in Azure at the same point in time) for cost/capacity/service differencing.

A multilayer resource readiness workflow was developed between the layers, assuring preparatory workloads for future requests, and superseding "built" workloads upset during the transition to the next layer. It also serviced readiness verification outside the repeat-request loop, clearing retries once readiness was achieved. Associates executing support actions were scheduled in the sustain phase to lower downtime impacts.

5. Security Posture Automation Framework

The transition of enterprise security posture management towards complete automation is underscored by the demand for tools capable of proactively remediating detected vulnerabilities, closing security gaps, and implementing a comprehensive set of security best practices. Aiming to automate the security hardening of hybrid cloud database deployments on Microsoft Azure and Amazon Web Services (AWS), the proposed solution consists of a framework that synthesizes Wiz security insights with Wiz SDK and custom-written scripts to implement corrective actions and achieve auditable policy compliance. Wiz scans cloud infrastructure for misconfigurations, identity, and access management weaknesses, and monitoring and logging gaps. Security best practices are specified using the NIST Cybersecurity Framework and Requirements for Critical Infrastructure in Healthcare. The proposed solution supports patching of nonproduction databases and cluster-wide migration of Azure databases for PostgreSQL Flexible Server and Azure SQL Database resources with service requiring or high-sensitivity classification.

A hybrid cloud-integrated database has become a significantly affordable choice for data export, providing flexibility to use the right service for specific cases and lower costs. However, technical controls are often poorly implemented, and even unofficial classification and policy compliance data are not automatically remediated. Wiz is a cloud security platform capable of automating end-to-end protection across the clouds' cyber environments. Insights can be combined with the Wiz SDK and scripts to perform many of the industry's required technical controls. This work describes a framework capable of supporting the automation of Wiz insights on hybrid cloud-integrated databases hosted on the AWS and Azure platforms, with focus on patch and observability gaps related to databases and on suboptimal configuration or use of managed services requiring high-availability fault-tolerant clusters.

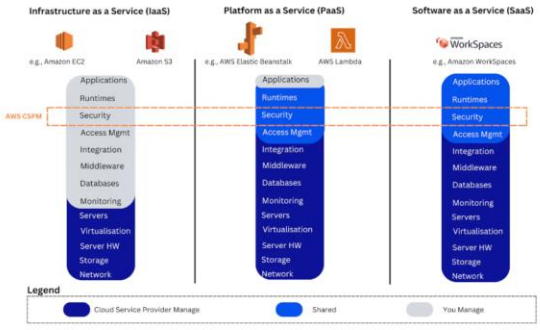


Fig 3: Cloud Security Posture Management (CSPM)

5.1. Data Collection and Telemetry

Database state data on AWS and Azure is drawn together with Wiz for monitoring. Wiz aggregates operational and

ISSN: 3050-9696
E-ISSN: 3050-970X
EUROPEAN ADVANCED JOURNAL FOR SCIENCE & ENGINEERING
Volume: 03 Issue: 03
RECEIVED: JULY 22 REVISED: AUGUST 09 ACCEPTED: AUGUST 25 PUBLISHED: SEPTEMBER 07

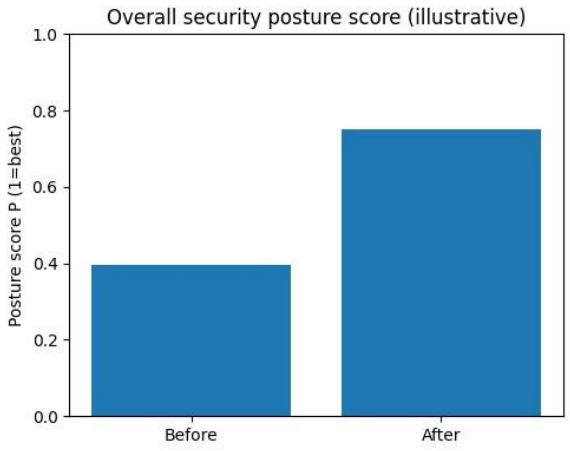
security-related data provided by cloud service providers and compiled with Wiz's own agentless security monitoring for IaaS, PaaS, and SaaS. Wiz covers cloud security and compliance posture management for identity management, network security, data protection, application security, workload protection, infrastructure security, security logging and monitoring, and vulnerability management. Wiz integrates with AWS Security Hub for compliance checking against AWS security best practices. Security Hub uses AWS CloudTrail data to monitor AWS account activity and detect unexpected changes for supporting security investigations. Data stored in the account is destined for a new data warehouse, allowing for targeted analytics and structured visualizations.

Microsoft Azure presents a separate security monitoring and compliance verification environment, Azure Security Center, which adopts a centralized approach to security management and compliance across hybrid cloud environments. Compliance can be verified against on-premises services and databases, with integrated threat detection and other additional services within Microsoft services. Azure Sentinel is a dedicated cloud-native SIEM (Security Information and Event Management) service with associated intelligent security analytics and threat intelligence solutions across enterprise and cloud application ecosystems. Cloud service data and database configuration telemetry are monitored within Wiz for ensuring deployment compliance with tenant-defined security posture requirements.

5.2. Policy Specification and Compliance Mapping

Common cloud policy standards, such as the Cloud Security Alliance Cloud Controls Matrix (CCM) and the Center for Internet Security (CIS) Benchmarks, provide map rate products to security and compliance goals but rely heavily on manual domain expertise rather than automated or tool-based enforcement and verification processes. Wiz Facility, the platform's core automaton for mapping cloud assets against various industry standards and frameworks, can be leveraged to generate those mappings and report which policies are met, partially met, or not met at any point in time.

The Wiz Facility can supply valuable mappings to cloud security policies and controls, allowing domain experts and asset owners to concentrate their efforts solely on the areas identified as needing remediation. These Wiz-driven compliance and security posture insights can subsequently be tied back to corresponding recommendations within the Wiz Product Center, enabling rapid risk mitigation or security hardening of hybrid-cloud assets and reducing reliance on manual commands. Wireless, ad-hoc, one time Wiz queries are ultimately insufficient for continuous security improvement; adopting the Wiz SDK within a dedicated automation repository enables controlled, user-definable executable processes to be created. Wiz Cloud Security and Attack Path Management are used to enhance the security posture.



6. Threat Model and Risk Assessment

The integration of multiple cloud providers augments the attack surfaces of cloud environments. Consequently, strong identification of attack surfaces in hybrid environments is necessary. Based on these identified attack surfaces, a risk scenarios and mitigation strategy table has been formulated.

ISSN: 3050-9696
E-ISSN: 3050-970X
EUROPEAN ADVANCED JOURNAL FOR SCIENCE & ENGINEERING
Volume: 03 Issue: 03
RECEIVED: JULY 22 REVISED: AUGUST 09 ACCEPTED: AUGUST 25 PUBLISHED: SEPTEMBER 07

The attack scenarios are generated by analyzing cloud security documentation—threat assessments, security best practices, and compliance framework mapping—and are adapted to the specific hybrid cloud database architecture. These provide a threat model that, when mapped to a risk assessment in the form of a risk scenarios and mitigation strategy table, improves the process of identifying cloud threats.

When integrating an on-premises environment with a cloud service provider, it is essential to consider the attack surfaces and the corresponding risk scenarios. Cloud providers recommend best practices to enhance the security posture of their cloud service. However, integrating two or more environments increases the attack surfaces. A hybrid cloud database integration across two mainstream cloud service providers—AWS and Azure—has been tested under compliance mapping for security.

6.1. Attack Surfaces in Hybrid Environments

Adopting a hybrid cloud strategy increases the elements to protect and enhances the complexity of the system's attack surface. Multi-service host configurations, high availability stream architectures, multi-cloud APIs, cloud DB with cloud VPN, and verification of integrated DB services in one of the clouds can be AWS attack levels. Attack surfaces are expected to grow further with the popularization of open-source cloud security platforms, such as Wiz. According to the vendor's 2022 Cloud Security Report, lack of protection against lateral cloud movement, assault on debases, and misconfiguration of identity and access management resources are the main attack surfaces found in a survey of cloud protection professionals. This trend also raises the influence of Wiz-driven data insight generations for cloud security posture remediation.

The recent past mapped natural risk scenarios for sweeping enterprise cloud-native DBs misconfigurations by the Wiz security platform. Building on these mapped risk scenarios prohibits seven of the OWASP Top 10 cloud prophecy weaknesses on the DBA. These scouting reports are defined in Templates and the specification details fully comply with the actual control topics' text. Since all-of-the-above approaches are inspired by Wiz's filtered security intelligence, the next (ongoing) stage will instantiate the operator depicted in the overview above. This automaton will take Wiz's cloud geometry-screened alerts as inputs, recycle them with formal Datacom checking processes, and bootstrap the necessary actions on the owning platform."

Equation 2: Risk scoring per scenario (Likelihood × Impact), then mapped to controls

A standard formalization:

Step 1 — For each scenario j define:

- Likelihood $L_j \in [0,1]$
- Impact $I_j \in [0,1]$

Step 2 — Compute scenario risk

$$\text{Risk}_j = L_j \cdot I_j$$

Step 3 — Control coverage reduces likelihood and/or impact

If a control set C is applied with effectiveness $e_j \in [0,1]$, one simple model is:

$$L'_j = (1 - e_j)\, L_j$$

and then:

$$\text{Risk}'_j = L'_j \cdot I_j = (1 - e_j) L_j I_j$$

This fits the paper's idea that posture automation decreases attack paths and misconfig exposure by enforcing controls continuously.

6.2. Risk Scenarios and Mitigation Strategies

The previous sketch of success scenarios illustrates the potential surmountability of some significant risk areas in hybrid multi-cloud environments. However, there are also risk scenarios worthy of attention, one of which describes the continuation of multiple attack paths post-environment segmentation. Ensuring that threat actors cannot gain persistence requires attention to all control families, and default closing of Azure Network Security Groups for

ISSN: 3050-9696
E-ISSN: 3050-970X
EUROPEAN ADVANCED JOURNAL FOR SCIENCE & ENGINEERING
Volume: 03 Issue: 03
RECEIVED: JULY 22 REVISED: AUGUST 09 ACCEPTED: AUGUST 25 PUBLISHED: SEPTEMBER 07

internally accessed services can reduce unprotected paths. Data exposure after network separation is also a concern; sensitive data should thus be stored in Azure for regulatory compliance and access to be carefully monitored. The danger of exposure through shadow accounts is well known, and periodic detection of unused AWS accounts can lessen the risk.

The web application layer represents another key and broad attack surface, and can suffer from weaknesses along all controls. On-idle unattended configurations and weak password practices are common vulnerabilities; the use of Azure DevOps or Cloudflare as an external proxy service can greatly simplify the implementation of security best practices; Azure Security and Azure Key Vault can ensure automated validation and secret management in CI/CD pipelines; and UBA, Azure Sentinel and using SQL as function can alleviate risks related to compromised views and executions.

7. Control Families and Technical Controls

Organizational information, cloud service usage, and setup impact the theoretical exposure and runtime risk of hybrid database environments. While compromise of cloud services is often viewed as a drain on availability and business reputation, the loss of sensitive information by bad actors may additionally yield sales strategies and business plans and provide blueprints for competitive advantages. Utilizing Wiz and established sources of threat modeling and risk management information enables formulation of pragmatic control families, technical controls, and risk-response strategies that reduce risk.

Databases in AWS and Azure are commonly managed by a specific service. The built-in security mechanisms are exposed to the authorized principal identity and associated persistent credentials, enabling performance of actions that may lead to complete and potentially untraceable compromise of the database. Identity and access management controls reduce risk by ensuring that data stored within these services is accessible only by the defined cloud service accounts; these highly privileged accounts should have the least-privileged access for the tasks being executed. The information exposure controls and associated operational security controls limit data availability and risk of sensitive information exposure.

7.1. Identity and Access Management

Many real-world incidents are related to misconfigurations of identity and access management systems. Attackers leverage excess permissions against the least-privileged-identity principle, access keys' lifetime, unused accounts, or even degree of identity federation from environments that undergo continuous monitoring by alert mechanisms (e.g., prevention and detection systems). According to Wiz's insights, insecure storage of cloud provider gathered credentials—often used by third-party services in external environments—exposes additional risks to organizations and must be reviewed soon. Everyone with administrative permissions on resources in external cloud providers must be known and monitored for batch deletion. Recommendations also prioritize the no-allow-everyone-to-do-anything policy, nonroot accounts with access keys, prohibitions to use AWS Root, Azure's global Administrator role key, gcloud's owner, and roll-back policies timeouts for services affecting external operations. New nonno-go productions, if present, may be blackholed, through-line-breaking no-route definitions in cloud providers.

Configuration-based solutions focus more on hardening Identity and Access Management components than on implementation and security provisioning events for production accounts. Guidelines for improving IAM functionalities include metadata usage to enhance deployments; keyless environments for cloud provider services; temporary tokens through Managed Identity Provisioning; federated configuration as code powered by Terrafirma or CloudFormation; appropriate permissions according to the least-privilege access model by Codified policies; and third-party integration executions with security audit.

ISSN: 3050-9696
E-ISSN: 3050-970X
EUROPEAN ADVANCED JOURNAL FOR SCIENCE & ENGINEERING
Volume: 03 Issue: 03
RECEIVED: JULY 22 REVISED: AUGUST 09 ACCEPTED: AUGUST 25 PUBLISHED: SEPTEMBER 07

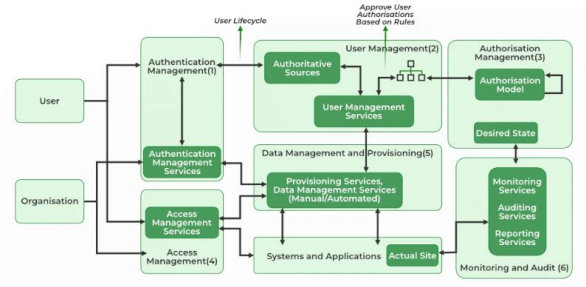


Fig 4: Architecture of Identity Access Management in Cloud Computing

7.2. Data Protection and Encryption

Data protection is vital to regulatory compliance and maintaining the confidentiality and integrity of data processed, stored, and transmitted by cloud providers. The shared responsibility model calls for distinctive application of data protection controls based on data classification. Wiz offers a dashboard view of storage resources used by a customer for sensitive classification or PII data, highlighting those lacking data protection controls or encryption at rest or in transit. The Wiz console also provides a unified position on the protection status of the customer's bucket storage.

To avoid affect and data-exposure risks for customer information stored in the platform, Data Loss Prevention (DLP) solutions should be operated to help discover, protect, and fulfill external obligations for sensitive data spanning multiple datasets, cloud locations, and third-party SaaS applications. Addressing compliance mandates like GDPR, CCPA, HIPAA, and PCI DSS—and client trust—is critical for businesses that handle sensitive data on behalf of customers. DLP solutions help identify sensitive data across multiple cloud storage locations and direct remediation and fulfillment of obligations based on machine learning and classification algorithms. For resources that require data classification scanning, Wiz integrates into a third-party cloud-native image scanning solution and automatically classifies all container images in Azure, GCP, and AWS during CI/CD to verify that all known sensitive data or PII data are handled according to regulation.

Equation 3: Hybrid attack surface index (why hybrid grows exposure)

A compact formalization:

Step 1 — Count exposed elements
Let:

- A = number of cloud assets (DBs, storage accounts, etc.)
- E = number of externally reachable endpoints
- X = number of cross-cloud integrations (replication links, IAM federation links, shared pipelines)

Step 2 — Define a hybrid "attack surface index"

$$ASI = \alpha A + \beta E + \gamma X$$

where α, β, γ scale each contribution.

Step 3 — Show why hybrid often increases X
Even if asset counts are similar, hybrid typically increases cross-cloud links X, raising ASI. That matches the paper's rationale for needing unified visibility and remediation across clouds.

8. Conclusion

Completing the scholarly article, consideration of Wiz capabilities in hybrid cloud database security posture favors formation and fulfillment of a simple data protection hardening operation cycle. Fully integrated cloud environments, however, offer continuously adaptable security postures significantly more advanced than isolated and/or hybrid cloud environments. In particular, security posture adaptation in Azure is a problem yet to be solved. Complementing Wiz with the securing capabilities of Zscaler might enable adaptation of the security posture in Azure. The integration of Wiz and Zscaler in Azure would permit the codification, into a higher level policy definition language, of the possible combined feed-forward fuzzing attacks for hybrid cloud configurations. Detecting potential measures against the fresh security breaches involving

ISSN: 3050-9696
E-ISSN: 3050-970X
EUROPEAN ADVANCED JOURNAL FOR SCIENCE & ENGINEERING
Volume: 03 Issue: 03
RECEIVED: JULY 22 REVISED: AUGUST 09 ACCEPTED: AUGUST 25 PUBLISHED: SEPTEMBER 07

Active Directory databases and secrets would form another area of research. Automated Wiz feeds exploring these attack paths could thus provide concrete information on the recommendations needed for maintaining up-to-date security configurations of cloud-integrated databases.

The drive for cyber-safety will certainly persist, as will research dedicated to attaining matches with all-cloud integrated database security. Data protection will thus ascend ever-deeper into the debate on security of databases running in hybrid environments, until general consensus finally emerges on how best to safeguard against data borrowing, avoiding malicious reputation turmoil.

8.1. Future Trends

The growing adoption of multi-cloud environments for mission-critical databases hosting sensitive information makes mitigating security risks a primary concern for organizations. Wiz addresses this concern by consolidating disparate environment vulnerabilities across Microsoft Azure and Amazon Web Services that enable sophisticated attack paths, thus streamlining security posture management, control family and technical control mapping, and policy compliance. The democratization of such insights opens the possibility of integrating them with other platforms to enrich the audit and security process. Supporting this direction, the proposed security posture management and audit framework automation is based on Wiz-sourced data and implements the Cloud Compliance Automation Framework.

Future trends point to the creation and continuous refinement of a Wiz Integration Library specific to compliance controls, enabling dynamic Wiz API monitoring and control family composition. The library will facilitate automatic mapping of Wiz recommendations to compliance requirements, ultimately resulting in the automated validation of organizations' security posture. The relevance of a hybrid environment-combined perspective relying on data coordination across leading cloud platforms—AWS, Azure, and Oracle OCI—also seems unquestionable. Beyond compliance aspects, the overall security posture of hybrid database environments requires joint consideration and practical mitigation actions across cloud providers to significantly reduce risk.

9. References

[1] Ali, S. (2025). Role of automation in hybrid cloud security configuration management. *ResearchGate Preprint*.

[2] Amazon Web Services. (2025). *Analyze Azure audit logs with CloudTrail Lake* (AWS Blog). Amazon Web Services.

[3] Amazon Web Services. (2025). *Strategy guidance: Creating a single hybrid and multicloud technology and governance strategy* (AWS Prescriptive Guidance). Amazon Web Services.

[4] Amazon Web Services. (2024). *Improving overall security posture with Wiz: Secured AWS landing zone* (AWS Partner Network Blog). Amazon Web Services.

[5] ANSSI. (2025). *Technical position paper on confidential computing (CoCo), v1.0*. Agence nationale de la sécurité des systèmes d'information.

[6] Bertani, A., et al. (2025). Confidential computing: A security overview and future perspectives. *CEUR Workshop Proceedings*.

ISSN: 3050-9696
E-ISSN: 3050-970X
EUROPEAN ADVANCED JOURNAL FOR SCIENCE & ENGINEERING
Volume: 03 Issue: 03
RECEIVED: JULY 22 REVISED: AUGUST 09 ACCEPTED: AUGUST 25 PUBLISHED: SEPTEMBER 07

[7] Center for Internet Security. (2024). *CIS Microsoft Azure Foundations Benchmark (v2.0.0)*. Center for Internet Security.

[8] Center for Internet Security. (2023). *CIS Amazon Web Services Foundations Benchmark (v1.5.0)*. Center for Internet Security.

[9] Center for Internet Security. (2024). *CIS Microsoft Azure Database Services Benchmark (v1.0.0)*. Center for Internet Security.

[10] Center for Internet Security. (2024). *CIS Microsoft Azure Compute Services Benchmark (v2.0.0)*. Center for Internet Security.

[11] Cloud Security Alliance. (2024). *Cloud Controls Matrix (CCM) and CAIQ v4*. Cloud Security Alliance.

[12] Cloud Security Alliance. (2017). *Security guidance for critical areas of focus in cloud computing (v4.0)*. Cloud Security Alliance.

[13] Confidential Computing Consortium. (2023). *A technical analysis of confidential computing (v1.3)*. Confidential Computing Consortium.

[14] Feng, D. (2024). Survey of research on confidential computing. *IET Cyber-Physical Systems: Theory & Applications*.

[15] Force, J. T., et al. (2020). *Security and privacy controls for information systems and organizations (NIST SP 800-53 Rev. 5)*. National Institute of Standards and Technology.

[16] Huang, J., & Yi, J. (2024). The key security management scheme of cloud storage based on blockchain and digital twins. *Journal of Cloud Computing, 13*, Article 15.

[17] International Organization for Standardization. (2022). *ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection—Information security management systems—Requirements*. ISO.

[18] International Organization for Standardization. (2015). *ISO/IEC 27017:2015: Code of practice for information security controls based on ISO/IEC 27002 for cloud services*. ISO.

[19] International Organization for Standardization. (2019). *ISO/IEC 27018:2019: Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*. ISO.

[20] Liu, J., et al. (2024). Key-aggregate based access control encryption for flexible authorization and efficient sharing. *Computer Communications*.

[21] Mani, A. (2024). Cryptography in the cloud: Securing cloud data with encryption. *International Journal of Electronic Security and*

Digital Forensics.

[22] Microsoft. (2025). Cloud infrastructure entitlement management (CIEM) in Defender for Cloud. *Microsoft Learn*.

[23] Microsoft. (2025). Azure security logging and auditing. *Microsoft Learn*.

[24] Microsoft. (2024). CIS Microsoft Azure Foundations Benchmark 2.0.0 mapping (Azure Policy Regulatory Compliance initiative). *Microsoft Learn*.

[25] MITRE. (2024). *MITRE ATTACK Cloud Matrix (Enterprise)*. MITRE.

[26] Mushtaq, S., Mohsin, M., & Mushtaq, M. M. (2025). A systematic literature review on the implementation and challenges of zero trust architecture across domains. *Sensors*, *25*(19), 6118.

[27] National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29)*. NIST.

[28] National Institute of Standards and Technology. (2020). *Zero trust architecture (NIST SP 800-207)*. NIST.

[29] National Institute of Standards and Technology. (2022). *Secure software development framework (SSDF) version 1.1 (NIST SP 800-218)*. NIST.

[30] Pahl, C. (2025). Infrastructure as code: Technology review and research challenges. *Proceedings (SciTePress)*.

[31] Souppaya, M., Scarfone, K., & Dodson, D. (2022). *Secure software development framework (SSDF) version 1.1: Recommendations for mitigating the risk of software vulnerabilities (NIST SP 800-218)*. National Institute of Standards and Technology.

[32] Verdet, A. (2023). *Exploring security practices in infrastructure as code: An empirical study* (Master's thesis). Polytechnique Montréal.


ISSN: 3050-9696
E-ISSN: 3050-970X
EUROPEAN ADVANCED JOURNAL FOR SCIENCE & ENGINEERING
Volume: 03 Issue: 03
RECEIVED: JULY 22
REVISED: AUGUST 09
ACCEPTED: AUGUST 25
PUBLISHED: SEPTEMBER 07