Mitigating Hybrid Cloud Risks

cloud security alliance®

The permanent and official location for the Hybrid Cloud Security Working Group is https://cloudsecurityalliance.org/research/working-groups/hybrid-cloud-security/

Acknowledgments

Initiative Lead:

Zou Feng
Narudom Roongsiriwong

Key Contributors:

David Chong
Chris Hughes
Michael Roza
Demuni Nishanthini Sandamali Silva
Geng Tao
Ashish Vashishtha

Peer Reviewers:

Anand A
Nataraj Bhargava
Diego Diviani
A.M. Garcia
Balaji Karumanchi
Mikko Koivunen
Rajnish Mishra

CSA Global Staff:

Frank Guanco
Hing-Yan Lee
Ekta Mishra
AnnMarie Ulskey (Design)
Haojie Zhuang

Table of Contents

1. Introduction

Hybrid clouds are often the starting point for organizations in their cloud journey. However, any cloud model consists of risks, threats, and vulnerabilities. Earlier this year, the Hybrid Cloud Security Working Group examined hybrid cloud model risks, threats, and vulnerabilities in its Hybrid Clouds and Its Associated Risks white paper.

However, after this review of risks, threats, and vulnerabilities, it's critical to identify adequate mitigation controls. This document will cover countermeasures organizations can implement to improve hybrid cloud risk management and cybersecurity practices.

2. Mitigation Measures for Risks, Threats, and Vulnerabilities

2.1 Mitigation Measures for Risks

2.1.1 Mitigate Distributed Denial-of-Service Attacks (DDoS)

A distributed denial-of-service attack creates disruptions to "internal" communication, and, operationally, it may impact daily activities in a hybrid cloud environment. Therefore, adding control layers to mitigate DDoS attack risk helps the hybrid cloud operation's continuity.

- Evaluate how well a complete hybrid cloud architecture can scale outside of the initial resource allocations. Plan how to increase or decrease resources as needed.
- To defend against DDoS attacks, deploy a powerful anti-DDoS cleaning device or use anti-DDoS services from an internet service provider (ISP) (private cloud) and/or complete solutions provider (CSP) in the access path to continuously process all incoming and outgoing traffic. When a multidirectional attack occurs, these devices must act immediately to implement bandwidth scaling and execution.
- For attacks that exceed their bandwidth reserves and DDoS defense capabilities, provide supplementary mitigation measures utilizing on-premise defense and traffic suppression provided by carriers.

2.1.2 Mitigate Data Leakage

Data leakage is a common risk in hybrid cloud environments because of user endpoints and clouds' connection through open internet. As such, user data is at risk of leakage due to human error or unauthorized access from man-in-the-middle attacks. Control actions (cited below) can mitigate data leakage risks.

- Data classification is the most critical consideration concerning data leakage prevention controls, so developing a defined data classification policy is recommended.

- Establish data security system and process assurance protocols, and specify departments and owners for data security management.
- Classify key data—such as essential sensitive data—in advance and meet data compliance requirements. This data should require extra approvals for access and monitored stringently for data leakage.
- Role-based access control (RBAC), access control list (ACL), whitelist, naming convention, and cloud access security broker (CASB) technologies and management methods can control data access. In contrast, data masking and anonymization protect data privacy.
- Ensure data is generated, transferred, used, saved, deleted, and destroyed throughout the lifecycle, and is auditable. When problems are detected, alarms can be automatically generated. However, in most cases, cloud service providers are not required to provide user data destruction certification unless added as a part of the contract between the cloud service provider and user.
- Cloud applications access user data through secure service interfaces. It is not recommended to access the original dataset directly.
- Data-sharing platforms should implement data sharing, resumable data transfer, data migration, and data encryption between clouds to ensure reliability during transmission.
- Use non-deprecated transport layer security (TLS) (1.2 or higher version) or secure shell (SSH) to encrypt all transmission data to avoid plaintext transmission.
- Use dedicated lines or a virtual private network (VPN) to isolate data transmission.
- Utilize data loss prevention (DLP) to help control the unauthorized exfiltration of sensitive data.
- Use the pseudonymization technique to separate personal identifiable information and other private datasets to reduce data leakage damage.
- Add breach notifications or alerting mechanisms in conjunction with defined timelines to meet regulatory requirements, such as the General Data Protection Regulation (GDPR).

2.1.3 Improve Perimeter Protection

When an organization works with a hybrid cloud environment, perimeter protection may vary compared to other circumstances, including private cloud services utilized by organizations internally or various third party entities. The risk mitigation controls cited below strengthen the perimeter protection to safeguard the organizations' assets in a hybrid cloud environment.

- Utilize whitelisted devices for device-level authentication. Each machine has a certificate.
- Whitelist should manage internet protocol (IP) subnets.
- Consider geofencing if the access is limited to a particular geographic region or country.
- Through in-depth network and security convergence, virtual security protection is implemented through the cloud platform security components at the cloud resource, network, and application program interface (API) boundaries.
- Maintain APIs and add a statement for API security controls such as authentication and authorization through Oauth2.0, OpenID connect, logging, and monitoring.
- Use a cloud management platform for centralized security management and integrated customization of fine-grained security policies between clouds.
- Bind security policies to services to implement synchronous migration and automatic deployment.
- Monitor security events such as management, application, and network in real-time and respond quickly.
- Use strict access control policies to prevent unauthorized access.

- Authenticate third-party applications for accessing cloud service interfaces.
- An authentication credential should be used for validity verification to ensure the interface is not invoked illegally.
- The interface access connection is encrypted based on the secure encryption algorithm.
- The credentials, keys, and tokens used for interface authentication and authorization must be effectively protected.
- All traffic must be scanned. For example, use a web application firewall (WAF) that supports complex ciphers to monitor traffic.
- Verify all parameters inputted through the interface.
- Compile the result code returned by the interface to avoid stack information leakage.
- Set a threshold for the access frequency and access duration of the interface. If the threshold is exceeded, the error code should be returned.

2.1.4 Compliance

In hybrid clouds, achieving and maintaining consistent compliance is a considerable challenge. Maintaining and complying with governance frameworks in a hybrid model can be problematic because data flows between on- and off-premises resources. The considerations cited below will help maintain compliance levels to mitigate risks.

- Organizations should specify which compliance standards apply and ensure compliance status is verifiable in public and private cloud configurations.
- Analyze and specify risks that affect compliance, and establish that the public cloud and private cloud environments meet compliance requirements. Then, substantiate compliance through collaborative work.
- Identify sensitive data involved in services in advance. The public and private cloud environments must comply with industry standards for data security and privacy protection.
- Evaluate information provided by public cloud providers to help customers achieve compliance—including independently validated certifications and attestations and third-party audits.
- Use a cloud security posture management (CSPM) service to report on configuration statuses and risk levels for public and private cloud, and develop mitigation measures for different risk levels.
- Engage in continuous compliance assessment and monitoring through an automated tool—which enhances security posture.

2.1.5 Aligned Service-Level Agreements (SLAs)

Maintaining service-level agreements with multiple cloud environments creates challenges when aligning SLAs of different CSPs—especially if the goal is to deliver an overarching, end-to-end, service-oriented SLA for end users. Therefore, organizations must consider mitigation actions (cited below) to minimize misaligned service-level agreement risks.

- As an overall solution, the SLA must cover services on the private cloud.
- Users should document requirements, thoroughly investigate hybrid cloud providers, and understand the differences between providers.
- User service expectations should be specified and detailed in the SLA to avoid discrepancies.

2.1.6 Alignment of Cloud Skill Sets

Cybersecurity challenges require specialized skill sets—particularly in hybrid cloud environments where public and private cloud environments interconnect and necessitate astute management skills. The alignment of cloud-specific skill sets will increase organizational capacity for effective and efficient hybrid cloud management.

- As a user management, hybrid cloud tool, cloud management platforms must provide unified identity authentication, metering management, virtual design and construction (VDC) management, operation and maintenance, interaction interface, resource management, and monitoring capabilities.
- The cloud management platform must isolate tenant data and enable access control measures.
- The cloud management platform (CMP) must provide a vendor-neutral interface (i.e., portal, command-line interface (CLI), software development kit (SDK), and API).
- The CMP should have a robust Identity aggregation and federation mechanism and attribute/policy-based access control.
- Management planes should integrate with public cloud providers› cost management APIs and allow custom cost metrics definitions to facilitate a unified cost governance structure.
- Management planes should be extensible and allow integration into major service management repositories and tools.
- Upskilling internal staff capability and skill sets is crucial to ensuring sufficient expertise to manage and administer the hybrid cloud securely.
- Augment internal IT team skill gaps by sourcing vendors with the necessary skill sets and experience.
- Cloud-related certifications can independently establish personnel credentials and qualifications.
- Attestations on compliances are generally publicly available for customer reference, which may provide consumer confidence while evaluating services. However, the responsibility matrix must be clearly understood and ensure adherence to security control tasks.
- For any software as a service (SAAS) options, service organization controls (SOC) reports can be obtained to ensure adequate controls.

2.1.7 Overall Considerations for Security Control Maturity

In a hybrid cloud model, public cloud environments require a higher security control maturity level—or a more extensive security control catalog—than typical private clouds. Consider these gaps to improve the adequate maturity level in private clouds as well. Countermeasures (outlined below) will help maintain security control maturity in hybrid cloud environments.

- Understand the security control maturity of different parts of the hybrid cloud (public and private cloud).
- Utilize security gap analysis—a comprehensive assessment of the organizational network security and system—to track weak security areas, set gap measures, and establish policies to protect the organizational network and system.

2.1.8 Comprehensiveness of Security Risk Assessment

Risk assessment can be challenging when evaluating hybrid cloud setups, as it is common for different providers to provide disparate parts of the infrastructure. Countermeasures (listed below) will provide sufficient security risk assessment within the hybrid cloud environment.

- Asset-based risk management ensures that critical systems and data are covered in risk assessments.
- Integrate the hybrid cloud environment as a whole and always strictly implement risk assessment and prevention.
- Conduct a periodic vulnerability assessment to assess the environment threat level.
- Log monitoring must be activated, and software must be updated to the latest version.
- Security data should be viewable and tracked in a unified manner.

2.2 Mitigation Measures for Threats

2.2.1 Mitigate Malicious Insider

The most commonly highlighted cybersecurity threats in a hybrid cloud model involve malicious insiders, such as employees and administrators, who may compromise the public cloud using the private cloud as a conduit. Therefore, organizations should always mitigate these threats with effective countermeasures (cited below).

- Comprehensive monitoring and auditing measures can record and trace all operations on networks and systems, especially key information operations.
- Create an enterprise risk identification and mitigation plan with a clear strategy.
- Stop all unauthorized access attempts.
- Ensure that the least privilege mode is set and applied.
- Delete or disable unnecessary and expired accounts promptly and avoid sharing accounts.
- Establish a strict password control mechanism.
- Strictly restrict access to key assets of the organization.
- Establish internal behavior security monitoring and analysis methods to monitor and report abnormal behaviors.
- Conduct annual incident response drills or tabletop exercises to address common weaknesses found in hybrid cloud environments.
- Develop broad insider threats awareness in security training.

2.3 Mitigation Measures for Vulnerabilities

2.3.1 Encryption

In the hybrid model, ensuring data protection for data at rest and secure communication between private and public clouds during data motion is highly recommended. However, organizations often implement inadequate data encryption mechanisms at the disk level, interconnection interfaces, and pipes (where data is most susceptible to theft or alteration). Therefore, it is recommended to implement adequate encryption mechanisms following suggested guidelines, as stated below.

- Consider the respective characteristics of asymmetric and symmetric encryption. Generally, encryption keys can be combined to transmit data through asymmetric encryption, and symmetric keys can be used for data encryption.
- Protecting data at rest:
  - Employ removable hardware security modules (HSMs) or external devices used in asymmetric encryption to generate encryption keys to encode data and govern data access. These steps will provide assurance that data will not be stolen or altered when transmitted between clouds. Add encryption options (e.g., file-level encryption, transparent data encryption (TDE), column-level encryption, and field-level encryption) to protect data at rest, as per customer feasibility.
  - Utilize trusted platform modules (TPMs), which are chips embedded in motherboards where encryption keys are stored. When enabled, TPMs lock drives until a user authenticates access with login credentials.
  - Use automated encryption, such as network-bound disk encryption (NBDE), which works on physical and virtual machines to encrypt root volumes without entering passwords.
  - For two layers of protection, use NBDE across networked environments while employing TPM, which associates disks with specific systems.
  - Use full disk partition encryption to protect data when computers are off. A standard format to encrypt hard drive partitions in mass is the Linux Unified Key Setup-on-disk-format (LUKS).
  - Maintain encryption keys separately from the cloud environment. If the hybrid cloud is compromised at the disk level, it is onerous to extract data from the disk level due to the key›s unavailability.
- Protecting data in motion:
  - Use internet protocol security (IPsec), a cryptographic extension of the IP, to encrypt network sessions.
  - Encrypt data flows and sessions with strong standards, such as TLS or SSH.
  - Use the Federal Information Processing Standard (FIPS 140-2)—or an equivalent encryption strength that features compliant cryptographic modules—to protect high-risk data.

2.3.2 Seamless Operational Processes

Organizations should review existing processes when adopting a hybrid cloud architecture to evaluate if current operational processes will be applicable, impacted, or disrupted by the transition. This undertaking should occur when dedicated teams—each with differing, required skill sets—are formed to manage each cloud. Suggestions for managing this process are cited below.

- Review security and operational processes to ensure it is seamless in the hybrid cloud.
- Pay particular attention to align the processes, especially those involving multiple teams/service providers. This effort should ensure a proper handoff between the different teams/service providers in a hybrid cloud model.

2.3.3 Network Connection Assurance

Network connectivity between clouds in hybrid cloud architecture is crucial for upholding SLAs, business continuity plans (BCPs), and disaster recovery plans (DRPs). Any slipups in establishing and maintaining this connectivity will drastically increase the risk of service disruption, unavailability, and service quality degradation. The below countermeasures can help mitigate these vulnerabilities within an organization.

- Have a clear network architecture review of the hybrid cloud that considers the capacity, performance requirements, criticality of systems, and dependency/integration between public and private clouds.
- Single points of failures (SPOFs) should be identified and eliminated, and high availability (HA) solutions established where necessary.
- Monitor SLAs for network services and perform regular testing for BCPs/DRPs at the network layer, with full consideration for the different failure scenarios that may occur—including partial failures.

2.3.4 Centralized Identity and Access Lifecycle Management

When public and private clouds are integrated into a hybrid environment, a lack of unified account management may cause account information inconsistencies between clouds—resulting in discontinuous log audits and failures to trace resource misuse. A unified access management process provides a more secure and manageable environment within the hybrid model. Key actions (cited below) will ensure organizations are equipped with appropriate identity management controls.

- Use the unified identity management tool to enable the identity authentication system of public and private clouds—and ensure identity uniqueness and maintain information consistency in real-time.
- Use role-based access for public and private cloud environments. Ensure the least-privilege principle applies, with only the minimum level of access granted to a specific role.
- Use modern authentication protocols and multi-factor authentication for administrative access to public and private clouds.
- Monitor and verify all access rights, including service accounts.
- Decoupling the unified identity management from public and private clouds offers a flexible, scalable, and consistent authentication/authorization solution across the hybrid cloud environment.

2.3.5 Integrated Security Management

The private and public cloud components in a hybrid architecture may have disparate security management policies and processes. Independent deployment of respective clouds' policies may cause inconsistent management, resulting in management confusion and blind spots. Integrated security management provides an adequate and effective security model for hybrid environments. The following countermeasures can ensure the avoidance of integrated security management pitfalls.

- Ensure effective integration of different management teams, clarify management responsibilities, or directly establish a unified operations and maintenance (O&M) management team.
- Take steps to establish an organizational cloud center of excellence (CCoE) where staff with strong cloud competencies can strategize and provide a central point of contact for the broader organization.
- Organizational strategy for cloud adoption should include considerations for technical security controls and a concentrated effort to educate and upskill staff on cloud computing issues.
- Organizational structural changes may be needed to align with the cloud computing paradigm and maximize cloud technology value.
- When managing computing, network, and storage resources in multiple domains, the administrator must ensure that the cross-platform management tools and policies are consistent.
- Define rules for configuration, installation, and access control for sensitive data/applications.
- Strictly define end-to-end access control, user management, and encryption policies to achieve optimal security.
- Use automated configuration management tools to reduce manual configuration errors and automatically generate images.

3. Conclusion

Existing private cloud security, public cloud security, and cross-cloud security environments should determine hybrid cloud security measures. When an organization starts its digital transformation with cloud platforms, most cloud environments begin with hybrid models that provide a smooth transition process with minimum disruption.

Systematic design requires a complete end-to-end security solution. In addition to existing cloud security risks, users and cloud service providers must consider connection and collaboration, management tools and processes, and recognize the importance of governance, risk and compliance management (GRC), vendor management, legal, operations, and architecture security. Finally, the selection of a suitable hybrid cloud solution is an urgent problem for users from a security and compliance perspective.