HYBRID CLOUD SECURITY: CHALLENGES AND BEST PRACTICES

Hybrid cloud computing combines the benefits of private and public cloud computing: mission-critical business information can reside in secure private cloud environments on-site while cost-sensitive data and apps can run in multi-tenant cloud data centers off premise. This distribution of IT workloads is based on a tradeoff between cost, performance and dependability of a service. Hybrid cloud computing offers the opportunity to strike an optimal tradeoff—but it also faces significant security challenges.

In this article, let's discuss some key security challenges facing the hybrid cloud as well as industry-proven security best practices to protect your hybrid cloud data centers:

Hybrid cloud data protection

One of the primary concerns that prevent cloud migration is the security of data in the cloud. While private cloud data centers may be physically located on premise, it still follows the model of cloud computing: data stored in private cloud is accessed over the private IT network infrastructure, which is potentially vulnerable to infringements, data leak, eavesdropping and man-in-the-middle attacks.

Hybrid cloud computing allows organizations to take advantage of both public and private cloud models. Benefits include reducing the risk of security threats; however, additional measures are required to manage security as the overall IT architecture becomes a complex mix of public and private cloud deployments. To ensure data security in the private cloud, follow these best practices:

- Encrypt data at rest and in transition.

- Use strong identity and access management (IAM) capabilities.
- Use cryptographic protocols (SSL/TSL) for secure data transmission over the network.
- Use SSH network protocols for data communication between unsecured network connections.
- Communicate the inherent data security risks to your customers and end-users.

Risk assessment and monitoring

Risks facing cloud networks evolve rapidly as cybercriminals find new ways to compromise vulnerable network endpoints and communication channels. To understand cloud network behavior at any given moment, you need an accurate risk profile. This information is critical to proactively perform the necessary risk mitigation activities. It is therefore important to follow these best practices:

- Evaluate and quantify the risk facing private cloud migration initiatives.
- Develop a risk profile and identify the resources required to tackle the security challenges within the available budget.
- Keep all software and network end-points up to date with security patches.
- Monitor network traffic behavior for suspicious activities.
- Use advanced AI-based network monitoring technologies that correlate network behavior with potential risk activities facing the cloud.

Hybrid cloud visibility and control

Cloud computing offers limited visibility and control over the IT infrastructure, as it is managed and operated by a third-party vendor. The case for an on-site private cloud would be different since the infrastructure is dedicated for use by a single customer organization and its authenticated users. The data center is often virtualized or software-defined, and these customers can maximize control over their resources. However, fine-grained visibility and control to combat hybrid cloud security solutions require in-house expertise, advanced technology solutions, and sufficient computing resources to accommodate the growing volumes of security-sensitive information and apps running within private cloud deployments in-house. In this context, the following best practices are useful:

- **Plan for your future data and computing requirements.** A viable cloud migration strategy should account for business growth and private cloud scalability expectations, which are typically more expensive than public cloud alternatives.
- **Watch out for shadow IT practices.** Enterprises have no control and limited visibility over shadow IT solutions that may be accessing sensitive business information across your hybrid

cloud infrastructure.

- **Consider SIEM solutions.** Public cloud solutions and SaaS applications offer limited visibility and control to its users. Advanced Security Information and Event Management (SIEM) solutions may be required to understand how public cloud solutions interact with your sensitive data.
- **Understand compliance**. Additional compliance measures may be required based on the type of data and the cloud deployment model. A hybrid cloud model may introduce additional challenges and opportunities for security compliance that should be identified and addressed.
- **Leverage Service Level Agreements (SLAs) with cloud vendors.** When initiating a cloud service, use SLAs clarify the visibility and control protections allowed to its customers. The clauses should be reviewed with an attorney to ensure that necessary compliance measures are respected as data moves across the hybrid cloud infrastructure.
- **Verify data security and ownership.**
- **Avoid a vendor lock-in.** It may be that the cloud service offers sufficient visibility and control into cloud systems, but the scaling growth may no longer justify the investments. However, it may not be feasible to migrate data and apps to another vendor—vendor lock-in—due to high cost or technology integration issues, thereby locking your data and apps in with the single cloud vendor.

Human error in the cloud

Gartner and WSJ recently reported that human error is responsible for up to 95% of cloud breaches. These errors range from basic configuration issues and unauthorized access all the way to major architectural design flaws.

Though large cloud vendors guarantee certain security protections, they treat cloud security as a shared responsibility. These vendors relieve significant operational burden from their customers by investing in state-of-the-art security technologies. However, the customer is entirely in control of managing configurations, security updates, and the guest OS, data, and apps. It is therefore important to understand the following best practices to eliminate human-related security threats:

- **Understand the shared security responsibility model per vendor.** Know your responsibilities and take proactive measures in performing your part.
- **Encrypt sensitive data.** Encryption should encompass client-side data, server-side file systems, and network traffic.
- **Manage and update regularly.** Manage security configurations and updates of the OS and software running on infrastructure-as-a-service (IaaS) solutions. For abstracted services where you only access and store the data, use appropriate security measures such as encryption, IAM, and data classification.
- **Educate your end users.** Train and make sure your workforce and end users understand how to safety treat data and cloud assets.
- **Limit access.** Use the principle of least privilege when establishing access control for users.
- **Staff right.** Employ in-house experts to manage the varied configuration settings of your hybrid cloud environment.

Additional resources

For more information on cloud computing and security, browse the BMC Multi-Cloud Blog or check out these articles:

- Hybrid Cloud vs. Multi-Cloud: What's the Difference?
- How to Secure Your Public Cloud
- How to Prevent Cloud Configuration Security Vulnerabilities
- Cybersecurity: A Beginner's Guide
- How to Apply Machine Learning to Cybersecurity

Listen to the podcast

Run & Reinvent Podcast · Episode 2: Cloud Security and How Self-Driving Remediation Helps Businesses Reduce Vulnerability