waystone | Compliance Solutions

Cloud Migration Security: Best Practices and Pitfalls

John Zuska March 28, 2025

As businesses increasingly shift their operations to the cloud, the promise of scalability, flexibility, and cost efficiency is hard to ignore.

However, cloud migration is not without its challenges, especially when it comes to security. A poorly-executed migration can expose sensitive data, disrupt operations, and leave organizations vulnerable to cyber attacks. In this blog post, we'll explore best practices for securing cloud environments during and after migration, while also highlighting the common pitfalls to avoid.

The cloud offers immense benefits, but it also introduces a shared responsibility model. While cloud providers such as AWS, Azure, and Google Cloud secure their infrastructure, the responsibility for securing data, applications, and configurations falls on the customer. During migration, this responsibility becomes even more critical as systems transition from on-premises environments to the cloud, often exposing temporary vulnerabilities. Post-migration, misconfigurations and overlooked security controls can create long-term risks.

In this blog, we take a look at best practices to ensure a secure cloud migration, followed by the pitfalls that can derail your work.

Best Practices for Securing Cloud Migration

1. Conduct a Pre-Migration Security Assessment

Before moving a single byte of data, assess your current on-premises environment. Identify sensitive data, map dependencies, and evaluate existing security controls. Use tools such as vulnerability scanners or conduct a cyber security assessment. This baseline helps you to prioritize what needs protection in the cloud.

2. Encrypt Data in Transit and at Rest

Data is most vulnerable when it's moving. Use strong encryption protocols (e.g., TLS 1.3) to protect data during the transfer process. Once in the cloud, ensure it remains encrypted at rest, using keys managed either by the cloud provider or your own key management system (KMS). This dual-layer encryption minimizes the risk of interception or unauthorized access.

3. Implement Identity and Access Management (IAM)

Limit who can access your cloud environment with robust IAM policies. Apply the principle of least privilege – only grant permissions necessary for specific roles. Multi-factor authentication (MFA) should be mandatory for all users, especially during migration when administrative access is more frequent.

4. Leverage Automation for Consistency

For firms with software development teams, the use of Infrastructure as Code (IaC) tools such as Terraform or AWS CloudFormation will automate the deployment of secure configurations. Regularly audit these templates to ensure they align with security best practices.

5. Monitor and Log Everything

Visibility is your friend. Set up real-time monitoring and logging (e.g., AWS CloudTrail, Azure Monitor) to track activity during and after migration. This helps to detect anomalies such as unauthorized access attempts and provides an audit trail for post-incident analysis.

6. Test Your Disaster Recovery Plan

Migration is the perfect time to refine your disaster recovery (DR) strategy. Simulate breaches or outages in a staging environment to ensure your backups, failover systems, and recovery processes work seamlessly in the cloud.

7. Post-Migration Hardening

After migration, don't assume the job is done. Conduct a thorough security review of your cloud environment. Update firewalls, patch systems, and remove temporary access permissions granted during the migration. Regularly scan for misconfigurations using tools such as Prisma Cloud or AWS Config.

Common Pitfalls and How to Avoid Them

1. Underestimating Shared Responsibility

Many organizations assume their cloud provider handles all security. Clearly define your responsibilities, secure your data, applications, and configurations while leveraging the provider's built-in security tools.

2. Rushing the Migration

Speed can lead to overlooked vulnerabilities. Build a phased migration plan with security checkpoints at each stage. Test thoroughly before moving critical workloads.

3. Misconfigured Cloud Resources

Publicly accessible S3 buckets or over-permissive IAM roles are common culprits in breaches. Use automated configuration checks and enforce strict access controls from day one.

4. Neglecting Post-Migration Security

Security isn't a one-time effort. Establish a continuous monitoring and compliance program to adapt to evolving threats.

5. Ignoring Compliance Requirements

Our industry has strict and constantly evolving rules when it comes to compliance. Map compliance needs to your cloud setup and validate with regular assessments.

Cloud migration is a transformative step, but security must remain front and center. By planning meticulously, leveraging automation, and staying vigilant post-migration, you can minimize risks and maximize the cloud's potential. The pitfalls are real, but with the right approach, they're avoidable. The cloud landscape will only grow more complex; stay proactive, secure your migration today, to build a resilient tomorrow.

How can Waystone help?

Waystone Compliance Solutions is a leading provider of cyber security consulting and compliance services to the financial services industry. If you would like to find out how Waystone can help you to assess your current cyber security measures, please reach out to your usual Waystone representative, or contact us below.

Contact Us →