Reducing Risks in Your Cloud Migrations

Controlling Privileged Access to Hybrid and Multi-Tenant Environments

Progressively organizations are moving to the cloud that helps businesses to go forward, faster, and achieve competitive advantage. Amazingly, cloud computing transforms the way information technology is managed, consumed, and improved cost efficiencies. According to the Forrester Research report, on average, 58% of companies outsource half or more of their data center operations, network, servers, and storage infrastructure. It demonstrates the shift businesses are making to the cloud environment. But keep in mind that the data transformation does not come without risk or threat. In the world of technology, the cloud is an attractive target to the attacker, and it is highly vulnerable to inside-out threat due to negligence and lack of staff awareness training. Therefore, companies should make sure that the data remain secure wherever the data goes into the cloud environment. Organizations need to implement rigorous cybersecurity practices and protect sensitive data. Organizations strive hard to targeting flexibility and making secure data access strategy for their progressive distributed workforce. For better understanding, let me tell you what Cloud Migration exactly is?

What is Cloud Migration?

Companies increasingly adopt the Cloud system quickly, but the Migration of resources is a significant task. Cloud migration of resources progresses the organization's scalability and flexibility in a fast-growing business environment. Moving resource or data servers to the cloud enhance accessibility for geographically diverse teams and minimize the need for massive server room on-premises. One of the key advantages of cloud migration is it simplifies IT and business management, whether operating in a full cloud, or a hybrid environment. Companies are not always moving all applications and resources on the cloud in a single pass. They do not move completely off-premises to a "pure cloud" environment. Businesses often move some portion of their IT resources or few applications to a "hybrid cloud" infrastructure environment. Cloud migration presents serious security challenges and risks to the organization, even in a portion of a hybrid cloud environment. The Cybersecurity team provides a comprehensive portfolio of Identity and Access Management (IAM) and data protection solutions that ensure only the company authorized user has access and controls keys to the data. Especially across multi-tenant, geographical distributed sites.

Reducing Risks in Your Cloud Migrations

Ironically, most experts identify security is the primary concern that is facing a cloud migration. One of the biggest reasons is many organizations are not even familiar with the cloud shared responsibility model. And they do not even try to figure out who is responsible for securing privileged access to the cloud environment. If your organization IT resources is moving to the cloud, then you need to implement best practice by which you can address these key security concerns. For Reducing Risks in Your Cloud Migrations, you need to;

- Implement Privileged Access Management (PAM), and the responsibility of managing access in cloud environments and workloads fall on your organization.
- Utilize a common security approach for cloud, whether data is on-premises, or moving on hybrid environments.
- Protect themselves from the risk of "identify sprawl" caused by identity silos. More the three-quarters of organizations are using more than one identity directory in their cloud strategy. Force your existing directory to broker authentication to access cloud environments based on a privileged user's identity and assigned roles.
- Adopt a zero-trust approach to PAM that prioritizes "Just enough, Just-in-time" access.
- You have modernized your security approach. Keep in mind what you have done for security may not be the best way to going forward. Turn to cloud-native PAM solution to secure on-premises, hybrid, and multi-cloud environments.

Security Risks in Multi-tenant Environment

In cloud migration, the multi-tenancy is an architecture in which each customer shares software application with a single database, so multiple users from the same company can access the database. It has broadened because of new service models take advantage of virtualization and remote access. Even in multi-tenant, each tenant is inaccessible to other tenants. Multi-tenancy solves major issues of IT departments. A system running in a multi-tenant environment naturally presents an additional vulnerability to all the standard security threats like malware and hacking. Each tenant must face an added layer of threat or risk.

There is a high possibility that an attacker takes benefit of the weak security system to gain unauthorized access to the confidential data. If the multi-tenant environments are not well isolated from one another with enough security, then the hacker penetrates the hypervisor and very easily manipulates or steals an organization's assets and confidential data. They are also able to disrupt an organization's operations by turning off the whole system and damage brand reputation. There are some solutions to prevent attacks in a multi-tenant environment. For instance, the two-tier security model of the public cloud helps you to shield yourself from co-tenanted environments risk at the application and storage layers.

Solutions to Multi-tenant Environment in the Cloud Migration

Migration to the cloud requires a Cloud Service Provider (CSP) that hosts data for hundreds of clients. The data potentially run on the same cloud resource, and knowing who has privileged identification to access the cloud infrastructure is always a challenge. Division among tenants and locks to each unit must be strong enough that can deal with attacks that security breaches. The CSP is a security measure that has clients assessing their server who may not have rigorous standards. Each tenant can strengthen their property with security measures for their peace of mind. The client of CSP who is operating resources with mufti-tenancy and migrating the business to the cloud, they need to add layers of access control to prevent attacks and alter before breaches occur.

Privileged Access Management (PAM) & secure Cloud Environment

Implementing a Privileged Access Management (PAM) system organizations can secure their assets, resources, or data, whether it is on-premises or on the cloud. It streamlined way to authorize and monitor all privileged users for all relevant systems to prevent the attacks. As we know, data integrity is lifeblood to any organization. To avoid penalties due to data breaches, organizations must need to take proactive actions and actively manage user access to information. Appropriate PAM system keeps an organization safe from both accidental and voluntarily misuse privileged administrator access to critical resources. It provides a countermeasure to secure multi-tenant, hybrid, and pure cloud environment. Keep in mind, the security of an organization's assets depends on the integrity of the privileged accounts that manage IT systems. Hackers or Cyber-attackers actively target privileged access to infrastructure systems to gain access to an organization's confidential data. Therefore, it is essential to protect privileged access, whether the environment is on-premises, cloud, or hybrid on-premises. The privileged administrative accounts must effectively control the security perimeter. Protecting administrative access from attackers requires effective methods of isolating an organization's systems. Securing privileged access requires changes to an organization's processes, administrative practice, knowledge management, and technical components.

1 Centralized Access Management (CAM)

A PAM system offers central management that enables streamlined management of all users across multiple systems, especially hybrid cloud environments. The access management system allows the IT security team to grant and revoke access privileges.

Many organizations frequently change personnel and roles. The single console for access management allows a secure system and robust password control even in a multi-tenant or hybrid environment. Centralized Access management improves the security system and increases IT productivity. The fantastic thing about the CAM is high authority administrators grant access to the users on systems. They are authorized to access data when it is required for defined periods. The access revokes automatically when the need expires. This process helps to ensure the security of critical organization's resources and prevent hacker attacks.

2 Robust Password Management

Having access to IT resource for each privileged user indicate that there are a higher number of chances bad actors breach the security and steal the data. A robust password Management is another solution to prevent the treats in your IT system. It keeps hacker threats away and strictly protects administrator passwords. This tool imposes strict, complicated requirements for password security and frequently rotate them for more system security. It reduces the number of entries points and makes access simplified for an authorized user. It changes the roles and entry points for those who leave the organization. Whenever companies migrate resources, assets, or applications into the cloud, there is a high need to pass data carefully and securely among cloud applications. Keep in mind, without a PAM solution, DevOps often set in passwords in their scripts. By this job running unattended, it can be a huge security risk that the organization often faces. Two components include a secure password vault, and another one is Application-to-Application Password Manager (AAPM) to deal with this issue. AAPM unlocks the secure vault to recover the correct password, which is made to the script for the duration of the process. By delivering access through AAPM, you isolate the identification from the script that makes it harder to gain access for an unauthorized user.

3 Audit & Oversight

A PAM can generate a permanent audit trail for Privileged operations. So, the IT security team can easily track, monitor, and take actions for any privileged user. By doing this, administrators can see what actions any user has taken in the cloud or on-premises system and automatically dismiss unauthorized operations or hacker attacks. This action protects your cloud infrastructure, whether it is on-premises, hybrid, or multi-tenant. As we know that regulatory compliance is essential for any organization, and cloud or hybrid systems make complying with cybersecurity standards harder to achieve. PAM system makes compliance easy and provides proof of compliance for audit purposes.

Whenever organizations are looking for a PAM solution to protect their IT system, they need to choose the best single solution that includes all critical components of PAM.

Conclusion:

Organizations should consider a PAM solution, whether they are running on-premise, in the cloud, or hybrid cloud environment. Organizations that are migrating their resources or applications to the cloud, PAM is an essential tool that prevents the hacker attacks and protects their resources. It is essential to understand how to choose the right PAM solution to solve many cloud security and Access Management challenging issues. PAM components are designed to improve IT productivity and protect the organization's resources.

Contact the Author

To find out how you can effectively protect your production workloads in the cloud, contact the author directly at dan.jatau@bitsecure.co or call 07540 460322.