**CLOUD SECURITY BEST PRACTICES**



What is cloud security management?

Imagine storing your company's important data and programs online, like in a giant digital warehouse. Cloud security management is like having security guards, alarms, and firewalls for this warehouse. It's all about keeping everything safe from threats like hackers or data leaks. This involves constantly checking for weaknesses, fixing any problems, and making sure only authorized people can access your stuff.

Why cloud security management is required?



* **Data Protection:** Keeping your sensitive information safe from prying eyes in the cloud.
* **Cyber Threats:** Protecting your cloud environment from hackers and other malicious actors.
* **Compliance Requirements:** Making sure your cloud setup follows the rules.
* **Shared Responsibility Model:** Understanding who's responsible for security in the cloud (it's both you and the provider).
* **Risk Management:** Identifying and addressing potential security issues in the cloud.
* **Business Continuity:** Keeping your cloud operations running smoothly even when things go wrong.
* **Trust and Assurance:** Showing everyone you take cloud security seriously.

**Cloud security goals:**

Ensure the confidentiality of data during transmission across networks.

Address the distinct cyber security challenges faced by enterprises utilizing multiple cloud service providers.

Manage and regulate user, device, and software access.

| Service Model | Responsibilities of Cloud Service Provider | Customer Responsibilities |
| --- | --- | --- |
| Infrastructure as a Service (IaaS) | Provisioning computing, network, and storage resources on demand. Securing core computing services. | Securing everything above the operating system layer, including applications, data, runtimes, middleware, and the operating system itself. |
| Platform as a Service (PaaS) | Offering a complete development and deployment environment. Protecting the runtime, middleware, and operating system, in addition to core computing services. | Safeguarding applications, data, user access, end-user devices, and end-user networks. |
| Software as a Service (SaaS) | Providing access to software on a pay-as-you-go basis. | Ensuring security for their data, users, and devices. |

How to secure cloud?

* **Lock down access:** This means using strong passwords, multi-factor authentication (MFA), and giving users the least access possible to do their jobs (principle of least privilege).
* **Encrypt everything:** Encrypt your data both at rest (stored) and in transit (moving around). This makes it much harder for hackers to steal even if they can access it.
* **Plan for the worst:** Have a disaster recovery plan in place in case of outages or attacks. This includes having backups of your data and a way to quickly restore your systems.
* **Stay up-to-date:** Keep your cloud software and security tools updated with the latest patches to fix vulnerabilities. New threats are always emerging, so staying current is crucial.
* **Regular Penetration testing:** Simulate cyber attacks on your cloud environment to identify vulnerabilities before malicious actors can exploit them. Penetration testing helps you stay ahead of the curve.

**Some of the security practices that can be adopted by every organization are:**

* Remove un-used permissions in IAM identities and provide least privilege
* Rotate IAM access keys every 90 days
* Enforce Tagging on AWS resources
* EBS volume should be encrypted
* Function App should only be accessible over HTTPS
* Storage account blob public access should be disallowed
* FTPS is required on App Services

CSR Certificate to get a custom-made key for your secure cloud storage unit. It is used for,

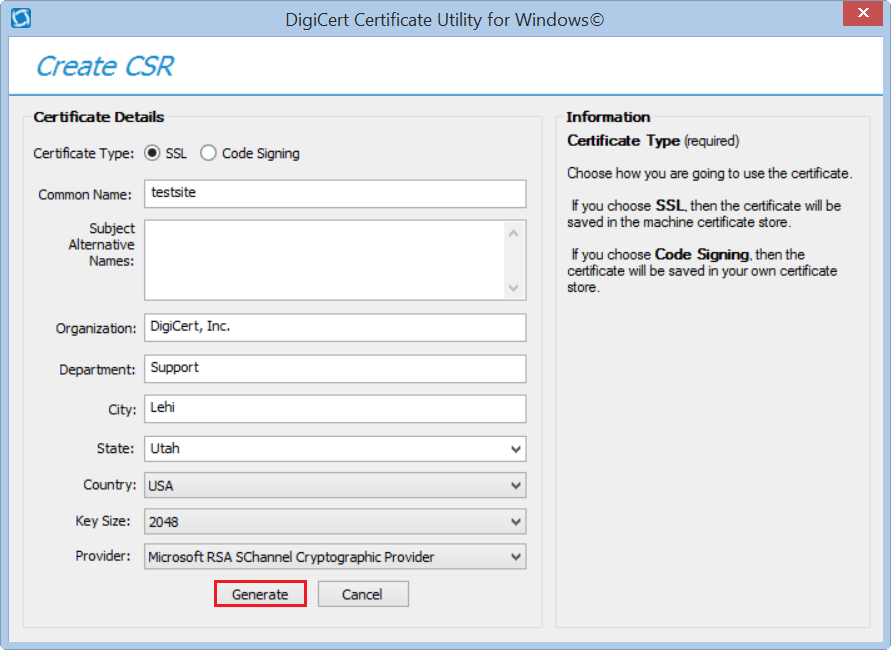
1. Identity Verification
2. Secure Communication

Here’s how to generate CSR Certificate:

1. Download and install DigiCert.



1. Open and generate CSR with details.
2. Once details are filled, click on generate CSR.



1. Get the certificate from Security team.
2. open digicert, import the security key certificate(named PKCS certificate) into it, click on next and finish.
3. Further WinSCP can be used to convert the pfx file to desired format.

Image result for WinSCP Logo.png

Please refer the below links,

Below link can help you to create CSR file with SAN from Windows Server OS:  
  
<https://www.entrust.com/knowledgebase/ssl/how-to-generate-certificate-signing-request-using-microsoft-management-console-mmc-on-windows-2012>

If you are using DigiCert Utility tool below steps to follow:  
  
<https://knowledge.digicert.com/tutorials/csr-creation-instructions-for-microsoft-servers>