**What Do You Need to Know Before Deploying an Enterprise Cloud Security System**

Cloud security is to safeguard your cloud computing environment with a security platform that covers all perceivable threats. The important thing is to thwart unauthorized access, attacks, hacking, and malware.

Public cloud services are provided by third party providers, which are easily accessible via web browsers, making authentication, identity management, and access control critical. On the other hand, a private cloud is a dedicated service devoted to a single enterprise, making it less vulnerable. A hybrid cloud is a combo of private and public clouds, allowing enterprises to better control their data and applications. You can get to know more about cloud security platforms and the 360° protection they offer through reputable service providers like [**https://sonraisecurity.com/solutions/cloud-security-platform/**](https://sonraisecurity.com/solutions/cloud-security-platform/). Here’s a look at the security challenges you need to be aware of:

**Management and Security Challenges Caused by Incompatibilities**

If your setup is designed for an on-premise environment, it is often incompatible with a cloud environment. Serious visibility and control gaps occur due to this incompatibility, causing misconfiguration, data leakage, and other vulnerabilities that affect your security platform. Even granting too much-privileged access and compliance issues are security threats to your enterprise.

As not all cloud environments have the same building blocks comprising storage, Oss, or hypervisors, it makes a particular security process or technology of any cloud environment unsuitable for any other multi-cloud environment.

**Simple Errors Lead to Severe Damage**

One significant benefit you enjoy from cloud computing is the ability to scale rapidly. However, such rapid scalability comes with certain drawbacks like security issues, vulnerabilities, and misconfiguration that increase suddenly and cripple operations. Under such circumstances, you cannot rule out massive service outages or security breaches. One good example is cloud administrator consoles providing high-level user capabilities that allow users to manage, configure, or delete servers on a massive scale. However, the flip side is that onboarding and managing such privileged accounts is often a daunting task.

**DevOps and Cloud Security**

The rise of the DevOps movement comes with a plethora of security considerations as it relies a lot on cloud deployments and automation. DevOps teams experiment on untested open source tools while managing countless security groups and server instances. Under such circumstances, a slight error or misconfiguration and lapse in security while sharing credentials or SSH keys can often lead to security and compliance issues.

**Risks Covered by a Fortified Security Platform**

**Better Control:** While using a public cloud service, you are practically renting IT assets. You have hardly any ownership over your hardware or applications and software that run on these cloud services because you are just leasing IT services. A comprehensive cloud security approach allows you to have the proper steps in place to counter your cloud vendor’s approach to your assets.

**Access Control:** You should allow access to your cloud environment only to authorized users. With a strong identity management and authentication process, you’ll be able to maintain a high level of security to protect your data and applications. Also, allowing limited access (to fulfill a role) to data and applications enhances security.

**Malware:** Although most cloud environments have inbuilt anti-malware protection, it may not be sufficient to cover the security risks. Hence, you need to be vigilant and find and plug gaps so that all cybersecurity solutions are perfectly in place.

**External Threats:** Threats from hackers can never be ruled out. You must be vigilant and have an early detection mechanism in place along with a multi-layered perspective that includes vulnerability management, data encryption, firewalls, etc., which will ensure that hackers are kept at bay.

**Internal Threats:** You should not be complacent while handling internal threats, which can be due to negligence (sharing credentials), which are difficult to detect immediately. Such risks can cause immense damage, and the best way to counter that is to have the proper privilege management tools that help limit the damage.

You need to fine-tune user activity management to keep track of the users accessing your cloud environment. Password control should be high on your priorities list for privileged and non-privileged passwords by banning shared passwords. This ensures that your security platform is safe from threats.

**Disaster Recovery:** Keep yourself updated on your cloud vendor policies relating to data backup, recovery, and retention; make sure such policies align with your internal standards. Also, ensure that a proper security monitoring system is in place across your cloud environment.

**Summing it Up**

When you have a well-thought-out security strategy in place, you can expect the best from your employees, boosting productivity. Also, you will be able to ensure that your data and applications are safe and secure. As of October 2018, a survey conducted by IBM Institute for [Business](https://en.wikipedia.org/wiki/Business#:~:text=Business%20is%20the%20activity%20of,enterprise%20entered%20into%20for%20profit.) Value indicated that over 85 percent of enterprises had already switched to a multi-cloud environment, with many more intending to opt for multi-cloud solutions by 2021.