PROTEGRITY

STRATEGY OVERVIEW

Things to Consider When Migrating to the Cloud

Security is almost always a key concern for organizations moving their sensitive data to the cloud.

Yet, while most companies depend upon a cloud provider to offer robust security features, what cloud providers actually supply is somewhat lacking. The native tools in cloud platforms often do not provide meaningful protection for sensitive data, nor do they address governance concerns over the control of data itself.

Here are some important considerations to review before you start migrating to cloud. How you go about migration will determine how effectively you'll protect your data.

Cloud Vendors Have Access to Your Data

Perhaps the most important point to keep in mind when migrating to the cloud is that regardless of the security schema employed by the vendor, it will always have access to your data in one way or another.

In instances where a vendor is in charge of protecting your data, it will possess the passwords, encryption keys and everything else needed to secure the data. You will rely on the vendor to perform all security functions. This means that someone on the vendor side will have access to your data in the clear. In addition, if a government comes knocking on the cloud service provider's door looking for your data, they do not have to seek your permission to decrypt it.

There are also misconceptions about Bring Your Own Key (BYOK), a process in which users holds the encryption key and believe they have control and can manage data security. But because BYOK offerings upload encryption keys to CSP infrastructure, the user actually doesn't have possession. In that case, the key is actually more exposed than it would be on-site, because of the need to store the key in a separate location, transmit it to the vendor, and only rely on the vendor to delete it after use.

Cloud Users Are Not in Direct Control of Their Own Data

When migrating to the cloud, the customer transfers control to the cloud service provider. In most cases, cloud users are essentially "publishing" data to the cloud, giving permission for the provider to copy or move data without notice to unknown locations–sometimes even unknown to vendors themselves. This can lead to compliance issues, most notably over data residency. Meanwhile, the user can request action on their data, such as protection or deletion, but it is up to the vendor to comply with the request. Data may never actually be removed from all cloud vendor servers, and the user has no way to verify.

In contrast, some situations may actually lead to cloud data loss. According to the report "Security and Privacy Issues in Cloud Computing," by Jaydip Sen of Innovation Labs, "The cloud customers may risk losing data by having them locked into proprietary formats and may lose control over their data since the tools for monitoring who is using them or who can view them are not always provided to the customers. Data loss is, therefore, a potentially real risk in some specific deployments."

Cloud Customers are Not Allowed to Verify Vendor Security

Cloud providers typically don't provide physical infrastructure for audits. Instead, they rely on an honor system, and customers are not allowed to directly verify security. The standard practice of "trust but verify" in vendor data security does not apply to cloud data security.

Not only does this create the potential for holes in security, but it often directly conflicts with internal data security policies and regulatory compliance requirements. According to the Cloud Auditing Project, "Lacking transparency of cloud services (e.g. data access and data lifecycle reports) is an important trust issue that hinders a more wide-spread adoption of cloud computing."

Public Cloud Customers are Responsible for Securing Their Own Data

Despite losing direct control of the data, those who consume cloud services are still the data owners, and usually retain the ultimate responsibility to protect the data, not the cloud vendor. Some enterprises learn this the hard way: after experiencing breaches and loss of data. They only then discover that an agreements with a cloud provider does not hold the provider responsible. This is best illustrated by the shared responsibility model which customers of cloud infrastructure providers agree to as part of their service agreement.

Your brand can suffer from data loss. Providers will pass the buck on responsibility down to the data owners any way they can.

The challenges presented by compliance, data governance, and new technologies can create a conflicting and shifting front, and the security solutions that are built into cloud services may not provide sufficient control, transparency, or security to meet all of your data protection requirements. Best practices for cloud data security are not always a priority of a cloud provider so that is why Protegrity is here to help.

To learn more about Protegrity's Cloud Migration Solution

email info@protegrity.com for more info.