PROTEGRITY

STRATEGIC OVERVIEW

How to Get Control of Your Cloud Data Security

Because cloud platforms don't meaningfully protect their users' data, organizations have to take charge of securing their own digital information. Effective data security means establishing control of the data so that an enterprise can smartly manage how it will approach cloud technologies and effectively secure data in the process.

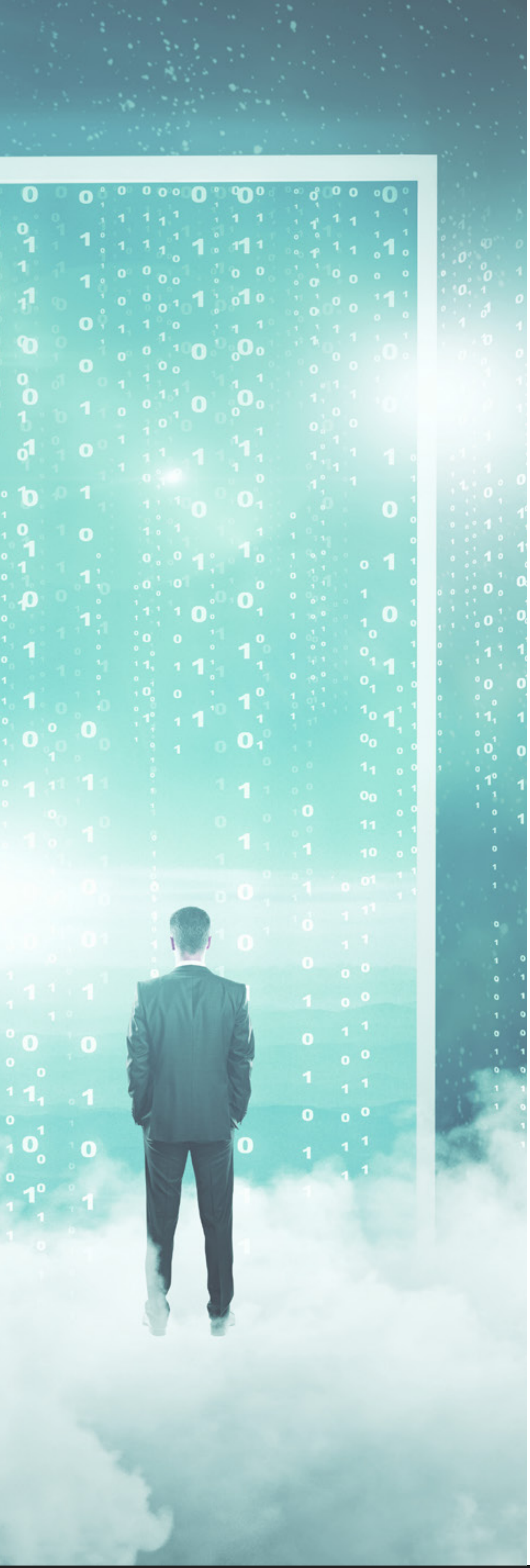
Before shifting workloads and data to the cloud, your organization should match the level of security you expect in internal environments such as databases and file systems. The notion here is that security needs to be systemic. You can avoid data security shortfalls by first selecting technology that can provide the required security services. This also means that in many instances, you don't even allow the cloud provider to control your data. But if you properly leverage technology for a security approach that spans from your enterprise to the cloud, you'll be able to control data security systemically, basically having control of your sensitive information any place that it exists. Here are some ways to get control of and secure cloud-based data.

Remove Cloud Vendor Access to Sensitive Data

You cannot restrict basic data rights (copy, transmit, delete, and others) from cloud vendors, as these are required for elasticity and to keep cloud services running at a high level. This fundamental step leads many to assume that the vendor is the only one that can protect the data. That's incorrect; the user has wide latitude to control and secure data. There are simple governance-related approaches you can take to help protect your sensitive data.

First, you should treat cloud vendors like you would any partner. If you wouldn't trust your partners to possess your sensitive data in the clear, do not give it to them. If you wouldn't trust them to hold an encryption key, do not give it to them.

That basic tenet should solve the issue of trust, but it still doesn't solve the underlying goal: securing sensitive data. If you don't let any data function in the cloud because you don't trust any provider, there's no sense in using the cloud at all. Trying methods such as Bring Your Own Key (BYOK) still doesn't prevent a cloud provider from accessing your encryption keys. You need something else: You need to establish a type of data security that can enable cloud services while also successfully preventing a vendor from accessing your data.



Bring Your Own Security and Gain Control Over Cloud Data

Bring Your Own Security (BYOS) solutions protect data before it ever reaches the cloud, and give you full control of access to sensitive data from inside the enterprise. BYOS solutions use fine-grained, data-centric security, including encryption and tokenization, so that data stays secure wherever it goes and however it is used. Many BYOS solutions use a gateway architecture, having data pass through a protection mechanism inside the enterprise before leaving to the cloud. Similarly, it goes back through the mechanism after leaving the cloud but before reaching the user.

BYOS puts you in charge of the security of your data at rest, in motion and during use. This autonomy allows you to choose which data is protected in the cloud. The cloud provider can't see the data, nor can hackers or government agencies, because you hold all data encryption keys and control over all data security functions.

Some of your customers may be concerned over the use of encrypted data in restricted data fields, but the simple solution is to use tokenization instead of encryption. Tokens replaces random sensitive data with meaningless characters. Tokens strengthen security while preserving data type and length. Also, because there is no mathematical relationship to the data, tokenization can essentially eliminate most data residency issues. Because of its comprehensive approach to data security, many cloud security vendors offer a tokenization solution.

Most data integrity issues can be solved through simple access control rights on protected data, as sensitive data will appear in the clear only for those authorized users who might perform any edits on it.

Verifying Security and Managing Risk in The Cloud

The internal verification of security can be performed through a series of internal audits on role-based data access from your cloud provider, performed through your BYOS solution.

While you may not be able to directly verify security in the cloud, if you control the function and hold all the keys, the security of your data should not change between the application of protection and the transmission and storage of the data in the cloud.

To learn more about Protegrity's Cloud Migration Solution

email info@protegrity.com for more info.

Without using formal audits in the cloud, beyond BYOS there are limited ways to manage risk, but the same principles of enterprise security apply. Basically, you determine the cost of a potential data breach versus the cost of protection. The average total cost of a data breach in 2020 was $3.86 million, according to IBM and Ponemon Institute.

Once you find a cost of risk, you will have a jumping-off point to make the business case for a security solution. In almost all instances, the cost of proper data security is far less than the potential cost of data breach.

Taking Responsibility for Security in The Cloud

Finally, you need to consider operations in your shift to controlling data security. How will all of this technology, including the use of cloud and cloud-based security functions in an ongoing operational state, allow you to meet all service, operational and compliance requirements, regardless of the cloud services provider?

Taking responsibility for your own data in the cloud is a bit more complex than simply signing it over to the provider. As Gartner pointed out, most cloud service provider contracts are inadequate. While cloud services providers have invested extensively on availability and disaster recovery, they often ignore data privacy, integrity and breach remediation in their service level agreements (SLA).

Even if an SLA includes some security commitments, you will still have concerns about data access by privileged insiders, legacy data persisting after a canceled subscription (or a supposed deletion), seized data, and stringent compliance requirements.

It's simply not enough to trust data privacy to your cloud provider. You're in a stronger position maintaining your own data security. BYOS software that includes data encryption and tokenization offers a level of security and control that cloud services providers don't. Read your End User License Agreements. Understanding your rights and data ownership will go a long way to determining how far you need to go to protect your data.

TO SUMMARIZE, HERE ARE A FEW QUESTIONS YOU SHOULD ANSWER BEFORE MOVING CRITICAL DATA TO THE CLOUD:

- ☑ Does the public or private cloud provider sufficiently address your enterprise's security requirements?
- ☑ What happens if there is a data breach?
- ☑ What happens if the government subpoenas your data or data co-located with your data?
- ☑ Who actually owns the content stored in the cloud?
- ☑ If you cancel a cloud subscription, what happens to the data?
- ☑ How do you address data residency requirements while using the cloud?

To learn more about Protegrity's Cloud Migration Solution

email **info@protegrity.com** for more info.