GlobalDots

Blog

Is Data Safe in the Cloud?

Admin Globaldots 28.06.2018 7 Min read

Background

Cloud storage is one of the most ***cost-effective, secure and scalable*** ways for companies to store their data in third-party datacenters through a cloud service provider. Thanks to rapid development of processing and storage technologies, many organizations are rapidly shifting more core business to cloud platforms. However, many organizations still struggle with a concern: is data safe in the cloud?

The obstacles concerning cloud security are somewhat complex, but they can be divided into two broad categories:

1. Security concerns faced by cloud providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud)
2. Security concerns faced by their customers (companies or organizations who host applications or store data on the cloud)

Why are people concerned with cloud security?

GlobalDots

proving to be a significant barrier to adoption. To a certain extent, this paranoia is understandable. The idea of storing your sensitive business data on servers and systems that you don't have control over is intimidating. Understanding all these concerns, cloud companies are continuously working to create a range of security options that make sure that the data is encrypted and safely stored.

With cloud computing gaining strong ground, the concerns related to cloud security have become more relevant. The problems have become more complex as no two clouds are the same or serve the same purpose. Depending on their need, enterprises can choose from different types of cloud computing services like IaaS, PaaS and SaaS. Every type of cloud computing platform presents its unique set of challenges and security concerns.

Cloud storage providers and enterprises share a collective responsibility to ensure that your data is encrypted and safely stored. Implementation of baseline protection of the platform begins at the end of cloud storage providers. It further includes ensuring protection to the data they process, by methods such as authentication, access control, and encryption. To ensure further protection, many enterprises strengthen these protections with additional security measures. These security measures help in strengthening cloud data protection and in ensuring the right access to sensitive information in the cloud.

Cloud storage risks

Cloud security is tight, but it's not infallible. By using automation and brute force attacks, hackers can get access to the files stored in the cloud. That said, one of the biggest risks with respect to storing data in the cloud is privacy. Even if this data is not stolen, it still can be viewed or accessed. Law enforcement agencies or government departments can request for access to information stored in the cloud. Depending on the nature of the request, cloud service providers can provide or deny access. As data revealed by large companies like Google and Microsoft show, every year, there are a huge number of requests from governments for providing access to information.

Cloud security controls

Cloud security controls are created to protect the systems against any weaknesses, and minimize the possibility of an attack. Cloud security controls can be classified into the following categories:

GlobalDots

As the word implies, deterrent controls are created to minimize the possibility of attacks on a cloud-based system. Similar to a stop sign on a road or a warning sign placed on a property, a deterrent control minimizes the threat level by warning potential hackers that there will be legal consequences if they proceed to carry out any illegal action.

Preventive controls

Preventive controls are meant to add one more layer of security and prevent attacks from taking place. Multi-factor authentication, for example, makes a cloud-based system more secure, and prevents access to data from unauthorized users.

Detective controls

Detective controls are meant to take action based on any incidents or events that take place. For example, in the case of an attack, a detective control will alert the security team or a system on the likelihood of an intrusion, and the steps that must be immediately taken. Intrusion detection systems and network monitoring tools are actively used by enterprises to identify and recognize that take place on cloud-based systems.

Corrective controls

Corrective controls are intended to minimize the impact of an attack. Restoring backups automatically or isolating a compromised system are examples of corrective controls.

How cloud enterprises protect my data?

To ensure safety of data in the cloud, there are several methods and techniques. Some of these methods are described below:

Cloud data encryption

To keep data safe and secure, the first line of defense for a cloud-based platform is encryption. By default, encryption techniques use a mix of complex algorithms to protect information stored in the cloud. To view encrypted files, the attackers will need access to an encryption key. While encrypted information can also be viewed, the process to decrypt requires not only a huge amount of time, but also significant computing resources.

GlobalDots

offer encryption related services. This includes an encrypted connection to prevent man-in-the-middle type of attacks and encryption of data before it is transmitted to a cloud-system. Public cloud service providers also provide encryption keys to decrypt the information or data. This has proven to be one of the most effective ways to protect data.

Data encryption is regarded as one of the most effective approaches to data security, scrambling the content of any system, database, or file in such a way that it's impossible to decipher without a decryption key. Encryption ensures that only users who are authorized by the company can access data. Hence, if the data is lost or stolen, it is of no significance to the hacker, as he or she does not have access to the encryption key that is required to decrypt the data.

AI tools and auto-patching

AI can be a great asset for ensuring the enterprise security posture of a company. AI can be used to analyze huge volumes of network traffic and identify malicious activity with great speed and accuracy. AI can also be used for understanding attack patterns and prevent future attacks from happening. Auto-patching enables enterprises to completely automate their patch management process. This includes scanning all virtual machines to detect and fix the missing patches and ensure compliance to security.

Built-in firewalls

A firewall is a security product whose function is to stop malicious traffic. In the context of the cloud, a cloud firewall is a firewall that is hosted in the cloud and provides a virtual barrier and protection around cloud-based assets.

Third-party security testing

While finalizing a cloud provider ensure that they have in place third-party security companies to test and certify their servers and software. The outside monitoring decreases the chances of attack by hackers and cybercriminals. Third-party security testing also allows cloud service providers to address possible vulnerabilities before any hackers get an opportunity to exploit them.

What are the steps that I can take to keep my cloud data safe?

GlobalDots

incorporate all necessary steps to keep your cloud data safe. Here are some of the key steps you can take to tackle the issue of data theft:

Organization-wide security policies

Organizations using the cloud should adopt security policies related to data security (actually, all organizations should adopt them, but with the cloud it's even more important to do so). This is mostly related to passwords and general security practices. The best cloud protection in the world won't help you if you use simple-to-guess passwords, or if someone from your organizations reveals passwords and other sensitive data to bad actors. It is hence critical that organizations have clearly defined and documented security processes and policies to prevent such situations or scenarios.

Always backup your data

Cloud storage is by design built to protect enterprises from different attacks and natural disasters.

Cloud-based storage is also an extremely effective way to backup or restore your data. It is recommended to backup your critical company-related information on in-house company maintained servers. This will ensure that you still have access to your critical information in case of an outage at the cloud service provider.

Consistent security updates

Your system frequently alerts you for and reminds you about various updates. All these updates come with tools to make your network more secure and provide protection against threats. Cloud service providers, server providers and organizations must consistently update their security measures.

Regulatory compliance

When you select a cloud computing service provider, ensure that the service provider follows the laws as enforced by the respective governing authorities in specific regions. You can also check the credentials of the service provider with respect to industry-specific regulatory compliance such as HIPAA (For the Healthcare industry) or PCI Security Council Standards (For any merchant accepting credit cards). Regulatory

GlobalDots

cloud.

Trust, but verify

You have to validate the faith you put in your cloud computing service provider. Trust is absolutely vital because everyone must have access to your cloud-based infrastructure. But it's essential that you also monitor and audit continuously so you can verify business-critical activity and manage risk effectively.

Final thoughts

No system is 100% safe, but cloud infrastructure almost reaches this goal. Data is safe in the cloud, but some precautions have to be in place to ensure everything works smoothly. It is also equally important to adhere to regulatory and compliance requirements as mandated by the law.

If you have any questions about how to effectively adopt the cloud for your business, or how to optimize your cloud performance and reduce costs, contact GlobalDots today to help you out with your performance and security needs.

Table of Contents

GlobalDots

Comments

0 comments

Name*

Email*

Write your comment..

Save my name, email, and website in this browser for the next time I comment. For further information please see our Privacy Notice.

Send

There's more to see

GlobalDots

GlobalDots

Back to Blog

GlobalDots

Subscribe

Solutions by industries

Website Performance

Website Security

Cloud Security

DevOps & Cloud Management

Cloud Hosting, Hardware & Networking

Legal

Privacy Notice

Privacy Settings

Support

English

GlobalDots

Developed by E&R