Downloaded from: justpaste.it/cloud-encryption

What Is Cloud Encryption?

Today’s business models rely heavily on cloud technology in order to collaborate, innovate, and keep pace as business continues to rapidly evolve and advance. This can create vulnerabilities that malicious actors will try to exploit in order to access private information. That is why cloud security has to be at the forefront of any cloud computing strategy. Encryption is one of the fundamental elements of cloud security. It works by scrambling data so that even if a malicious party is able to access your cloud, they won’t be able to view the information. It relies on complex algorithms to encrypt and decrypt information. This guide will cover the basics of encryption for a better understanding of how cloud security works and why it is essential.

Symmetric and Asymmetric Encryption

When it comes to encryption, there are two types:

1. Symmetric is the traditional approach to encryption and it uses a simpler method that relies on one key to both encrypt and decrypt information. While it isn’t as secure as asymmetric

encryption, it can be the better option when it comes to sharing data in bulk. A more complicated encryption process can slow down transmission.

2. Asymmetric is a more advanced type of encryption that uses both a public and a private key. The public key can be used by anyone to send you information while the private key allows you to decrypt and view the data. This approach is used in most types of daily communication and offers better security. However, the two key systems can cause bottlenecks in the pipeline and aren't always the preferred method for handling massive amounts of data.

Encryption at Rest Vs. Encryption in Transit

Cloud security efforts typically focus on protection information as it is transmitted between networks, to or from a cloud storage device, or traveling in general. However, it is important to remember that data is also vulnerable to attack when it is at rest and is stored. Encryption should be used in both cases to help provide a more comprehensive security approach. Implementing encryption practices when data is in transit and rest creates a proactive security system that is preventing attacks instead of reacting once a problem has occurred.

Challenges of Cloud Encryption

While encryption continues to be proven as one of the most effective cloud security tools, it is still underutilized by businesses. One of the main reasons for this is the cost. Encryption does require additional bandwidth, which can increase costs for both cloud storage providers and customers. This can lead to situations where the provider is limiting its encryption efforts. Ultimately, businesses need to weigh the cost of investing in cloud security upfront versus the cost of a data breach or compliance issue that can result in fines and a loss or reputation.

Cloud technology is a powerful tool that is allowing businesses to innovate. However, it can create security concerns that will need to be addressed. Fortunately, there are proven tools that can help maximize security, reduce threats, and allow businesses to recover quickly. Encryption is one of these vital tools and should not be overlooked. In the long run, investing in encryption is well worth the cost. If you would like to learn more about cloud security and encryption, contact the experts at prancer today.