Connecting Across a Hybrid Cloud Securely

Hybrid cloud works as an extension of enterprise processes and systems by combining private cloud infrastructure with one or more public clouds. Even though it offers the benefits of extensibility, agility and cost savings, the security concerns of shifting data beyond their internal control may prevent many organisations from connecting to the cloud. These security challenges, however, can be addressed by leveraging the right transport protocols and strategising the shift from the start.

Enterprises that are usually good at controlling the security of data within their private networks may find things getting complicated when they start venturing into the cloud. While it's true that divesting certain IT infrastructure tasks to a cloud can help to save upon time and efforts in data management, it is important to check how the security of such data gets affected.

As businesses increasingly shift to a hybrid cloud environment, they must take care of certain data security measures. These include:

Data Compliance

Before an organisation starts offloading its files into a cloud, it must ensure that all regulatory compliance laws pertaining to the data are well understood. The laws that originate from the underlying industry vertical must also be taken care of.

A business may be handling credit card details for its customers, or storing the health information of patients in a hospital or working with data shared across multiple branches in different countries. As a cloud services user, it has the responsibility to ensure that all compliance standards are taken care of. In most cases, the cloud service providers inform their client about the compliance standards that they adhere to. If there is anything required over and above these data regulations, the client must inform the service provider.

Cross-Cloud Plan Regulation

An enterprise may have been managing its security policies within its private data centre very well. This, however, does not imply that the same procedures can also be directly transferred to cloud architecture. The principal objective for storage in a hybrid cloud is the ability to organise and sustain a data security policy consistently throughout the network. This involves firewall policies, IPS signatures and authentications with user IDs and passwords.

While dealing with multiple cloud solution providers, this can get complex: since different cloud platforms have different attributes, transmitting security features is usually a manual procedure. This is why IT administrators in a company prefer special platforms to manage content in a multi-cloud environment. They opt for centralised network and security setups.

Data Leaks

Another issue that data security personnel face in securing hybrid clouds is that of data visibility. The decisions on where exactly the data will be stored need comprehensive planning. Even after this, there are chances of losing its visibility. Therefore, whenever sensitive data is moved into a hybrid cloud, businesses must have a monitoring system and ensure that they can easily trace the data storage points as also the traffic flows in both the directions (in and out of the cloud).

Data Encryption

A good way to secure data at rest in any environment is to encrypt it. In a multi-cloud environment, this becomes necessary. Another requirement for businesses is to protect data that's in motion as it transits between the cloud segregation points. Furthermore, they must protect the data that is getting processed and influenced by a cloud app. By taking care of the encryption at these points, businesses can have some security throughout the data life cycle. Hybrid cloud service providers have multiple encryption methods and can help the business to choose the best one for their data type.

Scalability

A final thought that businesses need to ponder upon while drafting their hybrid cloud approach is to ensure that all their security tools and methodologies can be scaled for the growth of data. No organisation will want to face the problem of restricted cloud scalability just because they did not form a security design that grows along with the other infrastructure resources.

The idea, therefore, is to inspect each of the security tools employed in different cloud environments and check how they can be expanded. It is also important to check the potential problems that can surface if there is a massive expansion of cloud resource. Businesses must realise that security solutions are getting more unified now and because individual tools are tied to other resources, any scalability issue in one domain can also affect the whole network.

The common challenge across all these issues is to understand the security requirements as early as possible so that all pieces can be put together before the data is transferred to a cloud environment. The good thing is that all hybrid cloud security issues have a strong solution when you are collaborating with an experienced cloud services provider. With correct protocols applied in transferring data, a business can have a strong hybrid control that is both functional and secure.