7 tips for a smart Cloud security strategy

The increased reliability of applications and data in the Cloud, makes a good Cloud security strategy an absolute necessity.

To build a good cloud security strategy, you have to keep these important principles in mind:

1. Easy Access

Easy Access also means High Risk. The public internet is an easy way to connect to the Cloud, but it is also an unsecure connection that hackers like to exploit.

2. Direct Peering

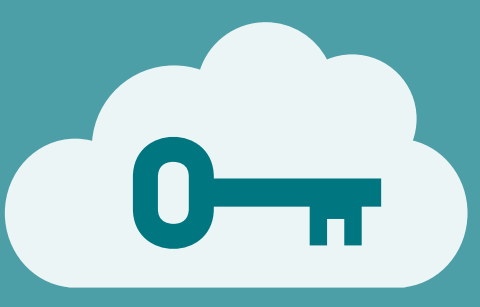
If you're still using Internet connectivity to access major public Cloud platforms, then consider a connection that supports Direct Peering to the Cloud platform.

3. Private connections

If you want a secure connection to the Cloud, you might want to consider a direct network connection to a Cloud platform through private connections (completely separated from the public Internet).

4. Data encryption

Extend the network connection with data encryption at the lowest level if necessary.



5. Redundant

No matter how you connect to Cloud platforms: make sure the connection is actually redundant, with physically separated network connections and data streams.

6. Cloud applications

Structure your data in the Cloud. How many backups should actually be stored? Or what resources can you switch off at night? With a few simple checks, you can manage expenses.

7. Cloud governance

A secure connection starts with the access. It is crucial that security is ensured at this level.
When an organization works in the Cloud, it is essential to know who has which permissions, on what resources. And who is allowed to perform which activities.

More information? Our specialists are ready to assist you

Would you like to know more about how to keep your security future-proof? Contact one of our specialists via info@eurofiber.be or call +32 (2) 307 12 00.

Eurofiber. Lifeline for the digital society