COMMON CLOUD SECURITY MYTHS

As Public Cloud technology becomes more popular, some businesses are still unsure of making the move because of security concerns. Here are our top 5 security myths debunked for you.

1 THE PUBLIC CLOUD IS NOT SECURE

Public Cloud providers invest millions in security. They use shared threat-intelligence, artificial intelligence, have dedicated Security Operations Centres and more. Your data is stored encrypted by default. The problem for most businesses is they don't understand the cloud shared responsibility model and are afraid of losing control. Understanding this model is key to understanding what type of security is available and where your responsibilities lie.

2 EVERYTHING IS EXPOSED ON THE INTERNET

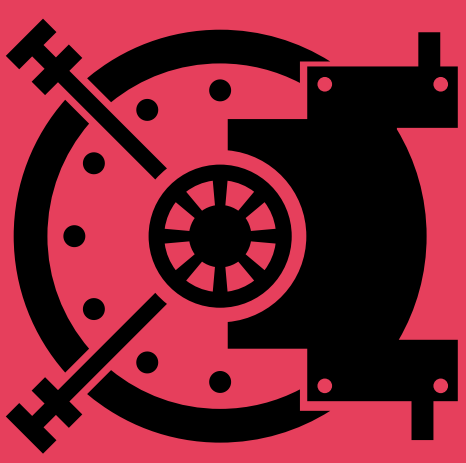
In reality, you are always in full control and it's a matter of understanding the shared responsibility model and how your cloud infrastructure and applications are configured, and also monitored & reviewed to account for any misconfiguration.

3 SECURITY IS ALWAYS THE JOB OF A VENDOR

Again, this relates to understanding the cloud shared responsibility model. The vendor will ensure their datacentres are secure, the physical equipment is kept up to date and their software routinely tested and updated. The security of your own cloud applications, identity & access management (IAM) and virtual infrastructure still needs to be considered and accounted for within your business.

4 ON-PREMISES SYSTEMS ARE ALWAYS MUCH SAFER

Most breaches involving public cloud-based solutions are down to misconfiguration of the cloud service by the end-user. Cloud providers invest significantly in security, realising that their business would be at risk without doing so. Again, it's important to understand where the responsibilities lie and to take time to understand how the public cloud vendors secure their infrastructure, details of which are freely available on their websites.



5 THE PUBLIC CLOUD IS MORE VULNERABLE TO ATTACK

There is a misconception that data stored on-premises is always more secure than in the cloud. It may seem that having your data physically close to you on your own infrastructure is more protected, but the location of where your data resides doesn't determine how secure it is. It is important to note that data security is robust in the cloud, offering a multi-layer approach to security. The key to protecting your data in the cloud is to focus on a well-defined security strategy that meets your businesses specific security and governance requirements.