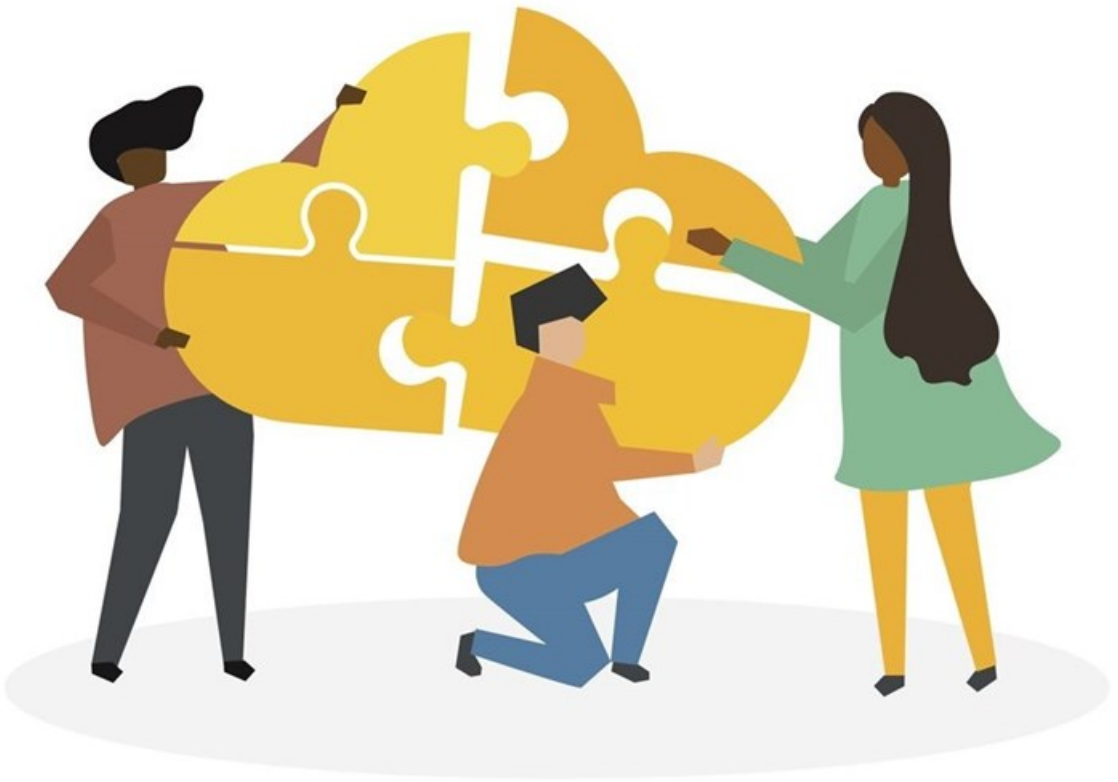
# Moving safely to the cloud

The cloud presents opportunities for companies to improve the availability and accessibility to data resources.



Cloud storage is also more scalable, allowing companies to accommodate ever-growing data volumes easily and cost-effectively. While cloud-based data centres are less risky than on-premise data centres from a security perspective, they are not without risk.

“Cloud-based data centres require a similar approach to security as on-premise data centres, yet companies tend to neglect to secure their cloud-based services. There is a clear segregation of responsibilities for cloud service providers and the companies using those services. Companies cannot rely solely on the service provider to secure their data in the cloud.”

“Similar to on-premise data centres, cloud-based services require configuration and should not be considered a plug-and-play solution. Authenticating the identity of users and managing their access privileges are also important. These aspects are the organisation’s responsibility and not the cloud service provider’s,” says Charl Ueckermann, CEO at AVeS Cyber Security.

Amazon Web Services to open data centres in SA

25 Oct 2018

He continues, “Cloud-based data centres still have a physical base in a physical location somewhere. Companies subscribe to the service providers that own these physical data centres. It is up to the cloud service provider to secure the CIA (Confidentiality, Integrity and Availability) of the physical data centre, wherever it may be. This includes securing the actual hardware such as the servers and routers against threats like theft, natural disasters like fires or floods, power

failures, and unauthorised access.

“In fact, there are various security and privacy standards that cloud providers must comply with in order to provide cloud services to markets across geographies and industries. Some of the more well-known standards include ISO27001, the EU’s GDPR, and the USA’s HIPAA. This serves as the assurance to companies that they have got their security covered.

“It is then up to the subscribing company to ensure that the type of data and services housed in the cloud, as well as who has access to it and what type of access they have, is managed. Simply put, if you are using a cloud-based data centre, you need to have control over what type of data goes to the cloud, what type of services come from the cloud, and who can use it. It is recommended to conduct a comprehensive Hybrid Security Gap Assessment to find the security loopholes between your provider’s security measures and your own. This will help to direct you in addressing any security issues on your side.”

Data Centre Management as a Service is a game changer

Riaan de Leeuw 24 Oct 2018

Other considerations for the effective protection of data in the cloud include defining the types of devices and connections that users can utilise to access cloud-based resources. Accessing the data cloud via an unsecured Wi-Fi connection or using a public computer or one that does not have appropriate endpoint security can put data at risk.

“It all sounds a little overwhelming, but it doesn’t have to be. Protecting data in the cloud is quite similar to securing information in a physical data centre onsite. It just cannot be neglected. And once you are up and running, cloud-based data storage and services offer numerous advantages over on-premise options from accessibility, agility, and performance perspectives, while remaining secure.”