SaaS adoption: Why organisations shouldn't neglect data protection, security aspects

By Simon Williams

22 Dec 2020

With the acceleration of digital transformation due to the Covid-19 pandemic, organisations have had to turn to technologies such as cloud computing to ensure business continuity and enable employees to work remotely.
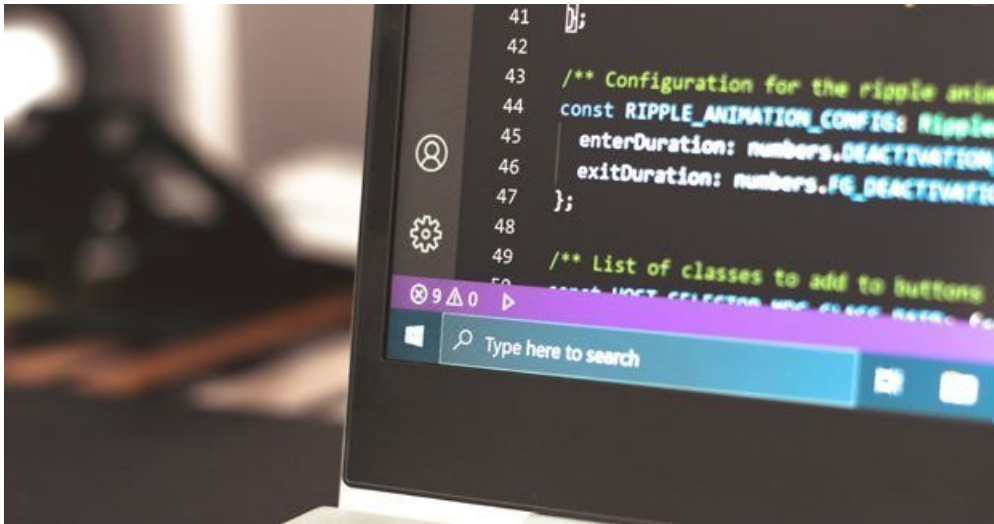

Photo by Heliberto Arias on Unsplash

While this trend has highlighted the significant benefits of digitisation for businesses, it has also effectively underscored the importance of Software-as-a-Service (SaaS). It has accelerated its uptake as a mechanism for organisations to procure technology through operating expense (Opex) as opposed to capital expense (Capex).

Essentially, SaaS has taken what traditionally software vendors would sell as an on-premise solution and coupled it with hardware infrastructure, be it compute, processing, networking, or infrastructure storage, and moved it into some form of the cloud environment.

At the same time, it's important to note that this is a massive transition for organisations that are considering adopting SaaS. It may not be every organisation's preferred choice, largely due to data sovereignty concerns that could lead to resistance to moving sensitive information into a public cloud.

For those who are able to shift their data and application off-premise, cloud adoption has become a common strategy that forms part of a larger strategic imperative. This is to gain speed of deployment, ease of use and limited the amount of IT resources needed to run their environments.

Who's responsible for data protection?

However, organisations often neglect to consider that while cloud vendors provide offsite infrastructure, they rarely take responsibility for protecting a company's data. We often see companies taking their data off-premise, where it was once backed up, to then move it to the cloud and trust the cloud vendors to provide that service 99.9% high availability is all too often confused with data durability.

Therefore, organisations must ensure they partner with a technology provider that has the expertise and experience to implement a data backup and protection offering that fits the needs of the business and protects their data beyond the firewall.

Hence, it is crucially important for businesses to look at what the levels of data protection and backup offered by the cloud vendor are. This ensures that they can determine whether they need third party tools to guarantee that their data is adequately secured and backed up.

Why is SaaS so valuable in a post-Covid-19 business environment?
Johan Scheepers 19 Nov 2020

The best way for organisations to certify that their SaaS data is properly protected and secured would be to team up with a data management partner that has in-depth experience. The partner must have the need to be knowledgeable in the areas of security, data sovereignty, compliance and governance that companies are expected to adhere to.

The right technology partner should be able to provide proof of past capability, showing that they have provided these services sufficiently for organisations in the past. If you put your eggs in the wrong basket, they will break, so companies need to look for a reputable vendor that has data protection, sovereignty and compliance at the heart of their organisations.

SaaS impacts the cost of ownership

Importantly, adopting a SaaS approach also impacts the issue of the cost of ownership at a time when companies seek predictability of cost. While there are organisations for which SaaS would be a good fit, they actually need to spend their money. From time to time, we see companies avoid SaaS, but only because Capex is a preferred financial trading model.

However, for others, adopting SaaS will generally result in a greater return on investment (ROI) over the medium to long term. This is due to the fact that the unpredictable cost mechanism of Capex for on-premise software solutions over this period is exponentially more expensive than SaaS.

The importance of SaaS adoption is especially relevant now as companies need a balanced service at a time when they need to rethink how they model their business because their workforce is now more mobile than ever before.

It is up to data management providers to capture customers who are on this journey and provide a simple, cost-effective, mobile and nimble solution. A solution that provides data security, data durability, compliance and governance needed for enterprises to connect with their remote staff.

ABOUT THE AUTHOR

Simon Williams is Metallic sales specialist UKI and Nordics at Commvault.