BIZCOMMUNITY

Tackling fears and misconceptions about cloud security and compliance

By Christian Hagner

26 Apr 2018

We speak to many CIOs and CTOs about the cloud, and I often walk into a room where I see folded arms as I start talking about cloud benefits. I realise that the only reason I'm in the room is because the audience has a KPI set by their CEO/CFO who are motivated by the business and cost benefits of this new technology.

Christian Hagner

There are two main reasons that hold back CIOs and CTOs from moving to the cloud, namely data security and compliance concerns for cloud-based workloads.

But the writing is on the wall: public and private cloud deployments will overtake those of traditional infrastructure very rapidly, according to the latest IDC ITC Infrastructure Tracker. As we move into 2018, this article addresses key fears and misconceptions to help address your cloud concerns.

Deeper pockets means better security

We have designed, built, and worked on multiple cloud environments over the years: as soon as you setup a new public-facing project, it is inevitably probed and scanned for vulnerabilities. Bear in mind that there is no way you or your local provider are spending as much as the hyperscale cloud providers are to ensure perimeter security and system integrity.

Gartner expects worldwide information security spending to reach $93bn in 2018, up from $86.4bn in 2017.

Take Microsoft for example: it has budgeted $1bn annually on security. Google has seven products with one billion users each that it protects on a 24x7x365 basis. Meanwhile AWS, the largest retailer on the planet with the biggest IaaS and PaaS footprint all of these cloud providers invest in the best technology, systems, and people available.

Your guide to the top three cloud computing trends of 2018

Brett St Clair 8 Feb 2018

This brings us to the related topic of expert skill-sets: hyperscale cloud providers leverage thousands of security professionals, data scientists, engineers, and developers on an ongoing basis to ensure a secure environment. These experts have developed sophisticated algorithms for monitoring environments, aided with the use of analytics and machine learning to identify out-of-the-ordinary behaviour.

Can your business sit back and relax then? Unfortunately not.

It's like getting into a car with top-notch airbags and not wearing your seatbelt: the safety features need to work in combination to be effective.

Having the world's best technology and skills taking care of cloud environments (for example, Microsoft, Google, or AWS) does not mean that you can just ignore it. There are several tools and strategies for cloud-based workloads recommended by cloud providers or application vendors that you need to adopt to ensure your workloads are protected.

The next key concern

The next key concern that South African companies raise is around compliance. Is the cloud PoPI (Protection of Personal Information act) compliant?

Most South African companies want to know if the large cloud providers are in line - as if they just want to tick that box and move on. But it's not that simple and usually they don't really understand what PoPI means.

Compliance requires an evolved availability approach

Claude Schuck 16 Apr 2018

From the cloud provider's point of view, they are defined as the operators. This means that their responsibilities are limited to issues of confidentiality and notification in the event of a system or data breaches (which they do!).

The main aim of PoPI is to ensure the protection of personal information and thus, the onus of ensuring this, lies with your business - not the cloud provider's, regardless of whether your data is internal, hosted locally, or hosted international. What this ultimately means is that asking whether the cloud service provider is compliant with PoPI or not does not actually assist you.

Where can your business get more info on cloud compliance standards?

All the hyperscale cloud providers provide long lists of independent certifications of security and compliance, it's just a matter of Googling it. This information is more than sufficient for the needs of a bank, a government institutions and yes, your needs too.

Can I get your attention!

Jared Molko 25 Apr 2018

A few years ago, many businesses were opposed to adopting virtualisation because the associated questions were just too many to comprehend.

There’s a similar pattern today with opposition to the cloud: security and compliance are the key issues that senior decision makers invoke to apparently avoid moving with the times. It’s important for your business to address any misconceptions as soon as possible if you want to unlock your business potential in 2018.

The benefits of the cloud - massive cost-saving, scalability, security and machine learning amongst others - are too great to ignore.

ABOUT THE AUTHOR

Christian Hagner has been in IT for over 20 years and has assisted some of the largest local and global companies with their IT strategy. He now heads up the cloud team at Siatik and focuses on helping customers assess, plan and implement cloud solutions. He can be contacted at [[christian@siatik.com]].