BIZCOMMUNITY

Moving to cloud? Take note of common security needs

By Anton Jacobsz

4 Sep 2018

The claim that cloud computing is radically transforming the way organisations (both big and small) do business, for better, agile and faster results, has become fact. However, there are still numerous scares denting the confidence of decision makers to shift workloads to the cloud, and security in the cloud continues to have an impact on the "shall we stay on premise or go hybrid or settle in the cloud" conundrum.

Anton Jacobsz, managing director at Networks Unlimited Africa.

Since the dawn of cloud computing, securing workloads in the cloud has been top of mind for business and technology developers. Data – no matter where it is stored – needs to be guarded for obvious reasons.

At the present moment though, I believe that it’s more of a risk not moving into the cloud as, quite simply, the cloud is an integral part of digitisation. The move can no longer be an ‘if’ choice for organisations, but rather a boardroom conversation that starts with ‘when’.

Networks Unlimited Africa anticipated the rapid rise of cloud when it made the decision to offer its customers throughout Africa solutions from RSA, a global cybersecurity leader who offers business-driven security solutions that uniquely link business context with security incidents.

Don't let your guard down...

In a high-risk world, organisations cannot afford to let their guard down. We are positive that making RSA solutions available to our customers on the continent will aid their transition not only to the cloud but also into the macro digital marketplace.”

RSA holds the accolade of being named a “leader” in four Magic Quadrants by Gartner: 2017 Magic Quadrant for Business Continuity Management Program Solutions, Worldwide; 2017 Magic Quadrant for IT Vendor Risk Management; 2017 Magic Quadrant for IT Risk Management Solutions; and 2016 Magic Quadrant for Operational Risk Management Solutions.

The company also protects millions of users around the world, and helps 90% of the Fortune 500 companies thrive in an uncertain, high-risk world.

Data security in the cloud - whose responsibility is it really?

29 Aug 2018

At Networks Unlimited Africa, we are especially pleased RSA enables customers’ cloud adoption plans through its strategy to ensure that its security technology operates is built to scale in the cloud environments that customers deem important.

The realities surrounding security in the cloud have been documented in the white paper titled, *'RSA & The Cloud: Opportunities, capabilities & challenges when considering security & the cloud'*.

The paper highlights the three common requirements of businesses moving into the cloud and states

> “As enterprises move applications and data to the cloud, every CISO (chief information security officer) is concerned about how their workloads will be secured, the same as if they operated on-premises. They know they don’t get a free pass from hackers just because the data is in the cloud. Threat actors view this as another potential attack vector to be exploited in this new, expanding and highly porous attack surface area of the modern enterprise. The bottom line is that enterprises have the same needs to provide (1) threat detection and response, (2) identity and access management, and (3) enterprise risk management for their assets in the cloud.”

The RSA paper expands on these issues and explains:

“Detecting threats in the cloud: When it comes to security monitoring, customers can’t ignore the cloud as a potential threat attack vector. While it certainly differs from on-premises deployment of security capabilities, the assets still need to be secured. Therefore, enterprises need to have endpoint-to-cloud visibility of all enterprise threats.

Suffer a data breach and lose up to one third of your customers

30 Aug 2018

“Ensuring people are who they claim to be in the cloud: With so much critical data moving to IaaS and SaaS applications, the CISO needs to have a high degree of assurance that users are who they claim to be when accessing cloud resources.

“Providing insight into ‘who has access to what’ in the cloud: With so many applications, the enterprise needs to ensure that users have the right entitlements to both cloud and on-premises apps, based upon their role. Why is too much access a problem? As identity is such a consequential attack vector, limiting what data and apps a threat actor can gain access to using stolen credentials reduces an organisation’s risk and exposure.

“Understanding risk and compliance of the cloud: A major challenge to any organisation’s cloud strategy comes with tracking how the business is utilising cloud services and its relationships with external providers.”

The paper makes for a thought-provoking read. What stands out, in particular, is the sentence: ‘Security software that can’t operate from the cloud will be left behind’. And being left behind in the digital marketplace...well, that just spells disaster.

ABOUT THE AUTHOR

Anton Jacobsz, managing director at Networks Unlimited Africa.