BIZCOMMUNITY

# Redefining the cloud and cloud security

By Doros Hadjizenonos

22 May 2019

Migration to cloud-based compute and services platforms have allowed organisations to quickly adapt to the global transition to a digital economy. The ability to quickly spin up resources, adopt new applications, and respond in real-time to end user and consumer demands allows organisations to compete effectively in today's new digital marketplace.

Doros Hadjizenonos, Regional Director – SADC at Fortinet

The result has been astounding. In just a few years, over 80% of enterprises have adopted two or more public cloud infrastructure providers, and nearly two-thirds are using three or more.

## Growing cloud challenges

While the business advantages are significant, this rapid migration is also introducing complexities and risks that few organisations have adequately prepared for - right at a time when the cybersecurity skills gap is dangerously wide, and cybercriminals are more capable of exploiting vulnerabilities than ever before.

Here are a few of the challenges that unchecked cloud adoption has introduced:

- New Cloud services are being adopted and used every day. However, it turns out that it is much easier to deploy a cloud application than to decommission it, so organisations are finding that cloud-based applications and services are piling up, making them increasingly difficult to manage and secure.

- The adoption of cloud-based applications and services is remarkably easy. Literally anyone across the organisation can source a new cloud service. The challenge is that service creation is often not funnelled through the central IT department, resulting in the creation of shadow IT.

  As a result, the organisation has little idea of what services are being used, where corporate information is being stored, who has access to it, or what security strategies are in place to protect it.

- Complicating this further, adoption of these services is heterogeneous. Employees use different cloud services from different providers, and these different providers all offer different security tools, different native security controls, and different levels of security. This can make it extremely difficult to impose any sort of consistency to security policy distribution, orchestration, or enforcement.

What many organisations may not realise when moving to a cloud environment is to what extent they are responsible for securing their own cloud environment.

---

Securing your data across hybrid and multi-cloud environments

Modeen Malick 12 Apr 2019

---

Cloud providers secure the infrastructure, such as storage and compute resources shared by everyone, but securing data, content, and applications are all the responsibility of the cloud customer. And those security controls need to be built separately inside each cloud environment that has been adopted.

If those security solutions aren't fully integrated and interoperable across multiple environments, then the number and variety of security tools that need to be implemented can compound, quickly overwhelming the resources available to manage them.

Part of the challenge is that the cloud has become so large and so complex that the word itself has lost much of its meaning. Even the term multi-cloud isn't much better. So, to build an effective, consistent, and manageable cloud strategy we need to start by clearly defining what we mean when we talk about the cloud.

## Multi-cloud environments introduce new risks

Eventually, all organisations will end up having deployed some combination of the cloud solutions described above. However, adopting multi-cloud environments not only expands the attack surface and complicates the ability to deploy, manage, and orchestrate security with consistent visibility and control, but it also increases other cyber risks, including data breaches and account hijacking.

Addressing these challenges, however, needs to be handled delicately. Performance cannot be sacrificed for security. Instead, organisations need to strike a balance between ubiquitous, on-demand cloud services and establishing consistent controls, policies, and processes. This requires looking for security solutions that help you move from a model where security inhibits business agility, to a model where security can be combined with cloud and automation to help business move faster and more securely.

## ABOUT DOROS HADJIZENONOS


Doros Hadjizenonos is Regional Sales Director Southern Africa at Fortinet

- Local eateries going digital now at risk of cybercrime - 24 Aug 2020
- How to have strong cyber hygiene - 26 May 2020
- How to approach data breaches - 11 May 2020
- Employees must be educated about mobile cyber threats - 13 Feb 2020
- Stay ahead of emerging cyber threats - 8 Jul 2019

View my profile and articles...