Essential cloud security concepts

By Doros Hadjizenonos

20 Jun 2019

Possibly the most important attribute of the cloud is that critical business applications, can be deployed, managed, and distributed faster and easier than by any other method, giving employees and customers real-time access to critical information - wherever they are located and on whatever device they are using.

Doros Hadjizenonos, Regional Director – SADC at Fortinet

That requires nimble resources that can scale and move, and applications that are simple and intuitive to use, have access to real-time data, and can be quickly updated to meet constantly evolving trends.

Security is just as critical a component of any cloud environment - especially as cybercriminals look to exploit the rapidly expanding attack surface. But to be effective, it needs to be as agile and dynamic as the cloud infrastructure being protected.

Effective security not only needs to protect connections between data and users but also secure literally every connection to every physical or virtual device across the distributed infrastructure.

In such an environment, complexities arise from the use of different security solutions, as deploying security solutions that are only available on a single cloud platform may not be available on others, and may have functional limitations. Such

deployments have actually imposed limits on the true potential of the cloud.

To address these challenges, organisations need to incorporate the following four security concepts into their cloud development strategies:

1. Security-led cloud development

Security breaches tend to be the result of a determined cybercriminal exploiting the weakest link in an organisation's attack surface. And for many organisations, the adoption of the cloud has expanded their attack surface exponentially.

Eliminating those weak links requires security to be enforced consistently everywhere, even when the infrastructure is in a state of constant flux. Because infrastructures are expanding and changing so rapidly, it is essential that an overall security plan become the foundational requirement for any network changes.

Mandating that proper security tools, policies, and procedures are in place before any new resources are spun up allows security to adapt in sync with infrastructure and application changes. This requires selecting security tools that understand the infrastructure in which they have been placed, and that can also operate consistently across all environments - including multi-cloud - to enforce policies and ensure visibility that enables secure applications and connectivity from data centre to cloud.

2. Cloud-native security

Since data and workflows will need to move throughout the infrastructure and to the cloud, security needs to function consistently. Selecting a cloud firewall from the same vendor that is protecting the organisations physical assets will not necessarily solve that problem. There is a need for these solutions to interact seamlessly with cloud services and subscribe themselves to these services as well as identify cloud-based resources in the same logical way that they identify other resources.

That said, the underlying technology used for protecting networks is very different from the tech used for protecting cloud-based resources, but the practice of managing security needs to remain similar. That is why native integration into the cloud infrastructure is critical.

3. Multiple form factors

Consistent security enforcement depends on the same security solutions being deployed across as many platforms and in as many different form factors as possible. Applications, for example, should be able to make calls to a cloud-based security solution to identify and protect specific data and transactions.

Container-based applications should have access to containerised security tools in order to easily integrate security functionality into the application chain. And ideally, these tools should be operated in the exact same way as solutions deployed everywhere across your distributed infrastructure, including at branch offices and edge devices.

However, don't fall into the trap of thinking that a virtual version of your network firewall will be adequate for your cloud or container deployment.

4. Central management

One of the biggest complaints from network administrators is that they cannot see and manage their entire network through a single console that extends visibility across physical and virtual networks. A management solution that can see and close the gates against an attack in one area of the network but not in another is likely lead to a compromised

infrastructure.

To eliminate gaps in security enforcement, organisations need a single pane of glass to gain visibility and define consistent security policies throughout the entire infrastructure to effectively manage risk. Security solutions need to share and correlate threat intelligence, receive and implement centrally orchestrated policy and configuration changes, and coordinate all resources to respond to detected threats.

Rethink your security

Traditional security models where devices are placed at a network gateway to monitor predictable traffic and devices are obsolete. Today, security needs to span your distributed infrastructure, dynamically scale when application resources grow, and automatically adapt as the infrastructure continuously adjusts to changing demands. And just as important, it also needs to ensure consistent functionality and policy enforcement regardless of its form factor or where it is deployed. Achieving that may require you to rethink your current security infrastructure.

If the cloud is going to play a significant role in the future of your organisation, you may be better off finding a single vendor that supports your overall application lifecycle and infrastructure roadmaps and expansion plans - especially a solution that provides consistent protection and functionality across multiple public and private cloud domains, even if that means replacing the traditional security hardware you have deployed on-premise.

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...