datacentrix

Avoiding cloud security blind spots in a hybrid IT world

By Kyle Pillay, Security as a Service Centre Manager at Datacentrix

The acceleration of cloud adoption has brought with it new security challenges for organisations to tackle, particularly pertaining to hybrid and multi-cloud environments.

Here, a common security misstep is the persistent confusion around who is responsible for what in the cloud. This oversight can open the door to serious vulnerabilities, especially when it comes to misconfigurations and fragmented security policies.

Kyle Pillay, Security as a Service Centre Manager at Datacentrix

> Many businesses assume that built-in cloud security tools mean they are fully protected. However, without proper firewall configurations, policy enforcement and additional security layers, critical gaps remain.

Mind the gap

One of the most significant blind spots in public cloud environments is the lack of awareness around the shared responsibility model. Many businesses assume that built-in cloud security tools mean they are fully protected. However, without proper firewall configurations, policy enforcement and additional security layers, critical gaps remain.

The type of cloud service used, be it Infrastructure as a Service (IaaS), Platform as a Service (PaaS) or Software as a Service (SaaS), determines how security responsibilities are divided.

For instance, in a PaaS environment, the cloud provider secures the platform, including networking, IP address management and basic firewall protection (typically at Layer 3). However, the business itself is responsible for provisioning

infrastructure, such as storage and compute resources. In addition, applications deployed on PaaS still require additional security measures, such as data encryption and identity management.

For IaaS, the cloud provider secures infrastructure components, including physical servers, and networking, while companies are accountable for everything above the infrastructure level, including operating systems, applications and data security. No built-in security is provided for applications running on IaaS; businesses must implement their own security controls.

SaaS offers the most secure out-of-the-box option, as the provider looks after everything from the application layer down. Thus, the customer only needs to manage data security, such as access control, encryption and data-sharing policies.

The need for unified policies in a multi-cloud reality

Hybrid and multi-cloud deployments are now becoming the norm, but many businesses struggle to implement a unified security strategy across these environments.

Fragmentation is a major concern, and it's not uncommon to find mismatched policies between on-premises environments and cloud deployments, where organisations have failed to extend their existing security policies to the cloud. This creates inconsistencies that threat actors are quick to exploit.

Therefore, to build a consistent security posture, businesses must apply the same principles and policies across all platforms.

Password complexity requirements, access control rules and firewall configurations should be standardised and synchronised. Monitoring tools and alerting systems also need to operate seamlessly across environments to ensure early detection of potential threats.

“

The cloud isn't inherently vulnerable, but assuming that it's secure by default is a risk no organisation can afford to take. Through a proactive, well-informed approach to cloud security, which is grounded in an understanding of service responsibilities and underpinned by consistent policy enforcement, businesses can avoid the blind spots that so often lead to breaches.

Preventing misconfigurations through proactive management

With cloud misconfigurations remaining one of the top threats to enterprise security, largely due to human error and weak oversight, security teams must adopt a rigorous vulnerability management approach to mitigate this risk.

This involves regular internal and external scans, checking for known common vulnerabilities and exposures (CVEs), and conducting exploit testing. Firewall and application-level testing are also essential, particularly for applications developed and deployed in the cloud.

The use of Governance, Risk and Compliance (GRC) tools, in conjunction with vulnerability management platforms, provides visibility and control, helping organisations maintain a robust security posture.

Building a safer cloud strategy

The cloud isn't inherently vulnerable, but assuming that it's secure by default is a risk no organisation can afford to take. Through a proactive, well-informed approach to cloud security, which is grounded in an understanding of service responsibilities and underpinned by consistent policy enforcement, businesses can avoid the blind spots that so often lead to breaches.

For more information contact Elzette du Preez on edupreez@datacentrix.co.za