4 Key Strategies to Secure Cloud Migration

Comprehensive hybrid cloud security strategy critical to strengthening security posture

Paul Williams, Country Manager SADC at Fortinet, outlines 4 key strategies to help organizations protect their businesses while migrating to private and public clouds:

1. Maintain a Strong Security Posture

Organizations need to maintain a strong security posture in private and public clouds. With the IT efficiencies gained by pooling compute, storage, and network resources through virtualization, SDN, and other technologies, private and public clouds have become increasingly aggregated environments, where not just servers but entire data centres have been consolidated into fewer but more efficient cloud environments.

The mix of data centre traffic has further shifted from north-south, which now only accounts for about 20% of data centre traffic, to east-west, which represents over 70% of traffic, especially as new software-defined environments continue to optimize underlying hardware utilization and efficiency on scale-out architectures. All of this means it is more critical than ever to isolate business units from applications. Organizations must also segment east-west traffic to minimize the impact of a hacker or advanced threat that manages to breach the cloud perimeter via a single weak or vulnerable application.

2. Segregate & Secure Applications in Hybrid Clouds

Many organizations are starting to employ hybrid cloud strategies, where public clouds are used to host more exposed public-facing workloads with less sensitive data. Public clouds with persistent VPN connections should be segmented from private clouds that need to be more secured.

Conversely, some organizations may use the public cloud to host some sensitive data, such as credit card data subject to PCI compliance, in order to alleviate strict industry compliance and regulations on the private cloud. Segmentation between the public and private portions of the hybrid cloud are equally important in this approach.

3. Employ end-to-end segmentation strategy

Organizations need to employ an end-to-end segmentation strategy, starting with micro-segmentation within the software-defined data centre, and complementing that with internal segmentation firewalling within and across the physical network layers of data centres, campuses, and branch offices. Within the private cloud, advances in network virtualization and orchestration mean organizations should consider a fine-grained micro-segmentation strategy that can uniquely firewall and secure workloads irrespective of physical network topology, even down to a single virtual machine or workload.

4. Activate Data Leakage Protection (DLP) and Monitoring

Besides firewalling and intrusion prevention, data leakage protection (DLP) and monitoring are equally important in either or both directions, to ensure that sensitive data does not cross cloud boundaries. This is to limit the damage or loss of a breach in a single-cloud environment.

Having a comprehensive security strategy for the hybrid cloud, including a single pane-of-glass view of security management and policy across both private and public clouds, is essential in establishing a consistent security posture for an organization, regardless of whether a given workload is running in an internal software-defined data centre or on provider-hosted multi-tenant infrastructure.