TOP 3 SECURITY CONSIDERATIONS FOR THE CLOUD

How Cloud Security Is Unlike Data Center Security

Data centers are evolving to include a mix of static hardware and cloud computing technologies. This evolution has led to lower CapEx costs, advances in operational efficiencies, and an improvement in data center hardware infrastructure effectiveness. However, with great change comes great challenge. While the threats remain the same, there are differences between how cloud-based computing technologies should be protected and securing traditional hardware-based data centers.

A data center is a fixed environment where applications run on dedicated servers that can only be accessed by authorized users. In contrast, a cloud environment is dynamic and automated, where pools of computing resources are available to support application workloads that can be accessed anywhere, anytime, from any device. For the experienced information security professional, it seems that many of the principles that make cloud computing attractive run counter to network security best practices. What follows are the top three considerations for securing traditional and cloud-based data centers, as well as key requirements for cloud security.

Cloud Computing Does Not Lessen Existing Network Security Risks

The security risks that threaten a data center and network today change once applications move to the cloud, whether in a complete migration or in a hybrid scenario in which some applications move to the cloud while others remain on-premises. In fact, in several ways, the security risks faced when moving to the cloud become more significant.

For example, many data center applications use a wide range of ports, rendering traditional security measures ineffective when those applications are moved to the cloud. Cybercriminals are creating sophisticated port-agnostic attacks that use multiple vectors to compromise their target, hiding in plain sight using common applications to complete their mission.

Security Wants Separation and Segmentation – The Cloud Relies on Shared Resources

For decades, information security best practices dictated that mission-critical applications and data be separated into secure segments on the network. Often, this is referred to as Zero Trust: never trust, always verify.

On a physical network within the enterprise data center, Zero Trust is relatively straightforward to implement through the use of firewalls and VLANs (i.e., virtual LANs), managed by policies based on application and user identity.

In a cloud computing environment, direct communication between virtual machines within a server occurs constantly, in some cases across varied levels of trust. This makes segmentation a difficult task, especially given that cloud applications are based on the notion of shared resources. Mixed levels of trust, when combined with a lack of intra-host traffic visibility by virtualized port-based security offerings, will likely introduce a weakened security posture.

Security Configurations Are Process-Oriented | Cloud Computing Environments Are Dynamic

Virtual workloads can be created or modified in minutes. As such, cloud computing teams operate in a highly dynamic environment, with workloads being added, removed and changed constantly.

By contrast, the security configuration for this workload may take hours, days or weeks. Security delays are not designed to create roadblocks. Rather, they are the result of a process that is designed to maintain a strong security posture. Policy changes need to be approved, the appropriate firewalls need to be identified, and the relevant policy updates determined.

Unless this imbalance is understood and addressed as part of the cloud migration, the result is a discrepancy between security policy and cloud workload deployment. The result is a weakened security posture that can put important data and intellectual property in danger and might also cause violations of compliance and governance policies and regulations.

Key Requirements for Securing the Cloud

- **Consistent security in physical and virtualized form factors.** The same levels of application control, rogue and misconfigured application handling, and threat prevention are needed to protect both the cloud computing environment and the physical network.
- **Segment business applications using Zero Trust principles.** In order to fully maximize the use of computing resources, it is now a relatively common practice to mix application workload trust levels on the same compute resource. The goal is to control traffic between workloads while preventing the lateral movement of threats.
- **Centrally manage security deployments and streamline policy updates.** Physical network security is still deployed in most every organization, so it is critical to have the ability to manage both hardware and virtual form factor deployments from a centralized location using the same management infrastructure and interface. The selected solution must be capable of spanning physical and virtual environments through a consistent policy management and enforcement framework and should include features that automate security policy updates.

To learn more about securing traditional and cloud-based data centers with next-generation firewalls, read the white paper.

paloalto NETWORKS®

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

pan-top-3-security-considerations-wp-061016