Things to Do Now to Ensure Your Cloud Posture and Preparedness

By Vinay Venkataraghavan, CTO - Technology Partnerships, Palo Alto Networks

Cloud strategy is a top priority for nearly every organization today. The shift to the cloud has created tremendous opportunities, but also introduced new risks that have to be managed. Many leaders who raced to adopt the cloud now want to know what it will take to be as secure in their cloud deployments as they are on-premises.

Much of achieving the goal relies on two industry categories for cloud security technologies. Analyst firm Gartner refers to them as Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platform (CWPP).

CSPM platforms help to define, configure, and monitor the state of cloud workloads and infrastructure deployments. CSPM capabilities are fundamental to be able to manage change and detect abnormal activity across all of an organization's large-scale cloud assets. CWPPs, on the other hand, help protect cloud native workloads, including container- and microservices-based applications.

Ensuring consistent, effective security across the many cloud environments organizations are running on today requires a platform that enables both CWPP and CSPM capabilities. Namely, it requires understanding the baseline of what is deployed and how it should work, and then being able to detect abnormalities while protecting applications and data.

Keys to Elevating Cloud Security Posture

Organizations should examine several vital areas when seeking to improve cloud security posture:

- **File integrity monitoring:** This is a cornerstone capability for application and data workload security: making sure files are not modified in unexpected or unauthorized ways.
- **Microsegmentation:** This is a best practice for cloud environments because in the cloud, the perimeter is not defined by a single ingress point that a single firewall can protect. With cloud native applications that have been decomposed into microservices, there is a need to minimize the attack surface. Microsegmentation accomplishes this by segmenting a virtual cloud network into small, well-defined slices with precise rules and policy for access.
- **DevSecOps:** Shifting security into the earliest stages of development can also help improve cloud security posture. With DevSecOps, security testing and compliance are integrated as code is developed, rather than vulnerability assessments being performed at the end of the application development process.
- **Permissions management:** This is a challenge many organizations face in the cloud. How many times have we all seen public reports of AWS S3 cloud storage buckets left open and exposed to the internet? Often, users will use overly permissive identity and access management (IAM) roles just because it's easier than defining fine-grained access controls and permissions for resources. Tighter permissions are simply required for effective security.

Security Is a Key Component of the Cloud Operating Model

An increasingly common way to manage cloud deployments is with a cloud operating model that defines how services are deployed and managed. The cloud operating model enables organizations to represent all aspects of cloud infrastructure as code (IaC).

Security should not be thought of as an independent layer in a cloud operating model. It has to be integrated at every layer to enable the most secure posture possible.

A common approach for enabling IaC is with a tool such as HashiCorp's Terraform or an AWS CloudFormation template. These resource templates can define how a service should be deployed. It's critical that organizations manage and inspect these templates to make sure the default configuration for a service is secure and has the right network configuration and proper permissions to limit risk. By defining the optimal secure policy and integrating that into a cloud operating model, it's possible to improve cloud security posture.

Be Prepared for the Cloud

Oftentimes, I tell CXOs that their security objectives haven't changed with the cloud. Many of the best practices in the cloud match what has been done on-premises, with fundamental concepts like protecting the perimeter and assigning least-privileged access to resources.

What has changed, however, is the scale and dynamism of the cloud and how that impacts security. Sure, some of the practices are similar, but how we facilitate it is different. We have to react faster, and we need to be more proactive. There is a clear need to have platform capabilities that automate best practices, operate at cloud scale, and are ready to act at cloud speed.

So, ultimately, what I offer to leaders is this: what you need to do for effective security in the cloud hasn't changed, but *how* you do it must.

Learn more about establishing a strong cloud security posture.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

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

www.paloaltonetworks.com