Keys to Building a Successful Cloud Security Strategy

Securing workloads in the cloud is not the same as securing workloads on-premises

By Matt Chiodi, Chief Security Officer, Public Cloud, Palo Alto Networks

One of the most common misconceptions among organizations entering a cloud transformation journey is the belief that securing workloads in the cloud is the same as securing workloads on-premises. In reality, that's just not the case.

One of the first keys to building a successful cloud security strategy involves the realization that the cloud requires a fundamentally different approach from on-premises security. Organizations cannot, and should not, be securing cloud workloads the same way they were secured on-premises.

On-premises security is typically reactive and largely driven by manual processes. In the cloud, with the speed of DevOps and cloud native development, it isn't possible to do things manually—or leave security as a last step—and be secure. Additionally, some executives assume that moving to the cloud equates to automatically gaining automation. Unfortunately, that is not true either. You need to build in automation yourself, especially from a security perspective. An important part of any successful strategy is overcoming these common myths.

Identity Security in the Cloud

The recently released Cloud Threat Report, 2H 2020 from Unit 42, the threat research division at Palo Alto Networks, outlined a number of different risks and common security issues for cloud workloads.

Among the high-level findings in the report is that cloud identity flaws are both difficult to detect and highly impactful. Identity is all about verifying who a given user is and providing the appropriate level of authorized access—but what happens when an attacker is able to abuse an identity due to a misconfiguration?

Unit 42 carried out a Red Team exercise on behalf of a customer and, in less than a week, was able to completely compromise the customer's entire cloud environment. The team did this by exploiting a misconfigured identity and access management (IAM) trust policy.

With a misconfigured IAM policy, an attacker could get access to the proverbial keys to the kingdom for an organization's cloud assets. The attacker could then do any number of things against the organization, including stealing sensitive data or even wiping out the cloud infrastructure.

The Big Cloud 5 Holistic Cloud Security Strategy

Certainly, automation is a key part of building a successful cloud strategy, as is the need to manage IAM policies. Looking beyond just these two tactical elements, organizations should consider what we call the Big Cloud 5, which outline the elements that enable a holistic cloud strategy.

1. **Visibility**: Getting and maintaining deep visibility into what is actually running is a critical foundational step.
2. **Guardrails**: Leveraging guardrails to enforce best practices for configuration, it's possible to help eliminate many types of misconfigurations, such as misconfigured IAM policies that could be exposing the organization to risk.
3. **Standardization**: When everything is done with an ad hoc approach, it's not possible to automate—and automation is key. Adhering to known standards and best practices is also central to enabling compliance. Standardizing as much as possible in a cloud deployment will make it easier to enable repeatable and automated processes.
4. **Human skills**: It's critical to hire and train security engineers who know how to code. As DevOps pipelines increasingly dominate cloud deployments, having staff with the right skills is of paramount importance.
5. **Shifting left**: Bolting on security at the end of the process doesn't work. What's needed is to "shift left"—that is, to embed security in the development process earlier to help limit the risk of vulnerabilities making it into production workloads.

Taking a "Default: Aggressive" Posture in Cloud Security

Being secure in the cloud is not about taking a passive stance. After all, security for your workloads is up to you, not the cloud provider.

A principle known as Default: Aggressive was defined by former US Navy SEAL officers Jocko Willink and Leif Babin. The Default: Aggressive approach is all about taking a confident, independent, and proactive default approach to real-time challenges.

I see the Default: Aggressive mentality as very similar to the mindset of Assume Breach, where security professionals assume that their environment has already been exploited.

Don't take the stance that, just because your team has ticked the boxes on a few cloud service provider-delivered security capabilities, all cloud workloads are OK. Rather, assume and take a Default: Aggressive stance to begin with.

Part of a Default: Aggressive stance is having a holistic strategy as well as making sure you have automated as much of your security tooling and response as possible.

Measuring Success with Shared Metrics

Having the right metrics to help benchmark and gauge cloud workload deployment security is another key to success.

What's critical, though, is bringing DevOps and security teams together to come up with shared metrics for cloud workloads. Typically, DevOps teams have one set of metrics that may well be more focused on availability and resilience, whereas security teams tend to look at vulnerability-related issues.

For an organization to really develop a DevSecOps culture that enables a successful cloud security strategy, it is important to have shared metrics that measure developer, operations, and security key performance indicators.

Building a Strong Foundation for the Future

The reality today is that the cloud is more important than ever—which is why it's paramount to have the right foundation in place for cloud security success.

The 2020 State of Cloud Native Security report by Palo Alto Networks surveyed about 3,000 practitioners worldwide. We found that, in 2020, 46% of organizational workloads were already in the cloud. Over the next two years, we expect that to rise to 64%. With the ongoing pandemic, we expect the adoption figure to actually be even higher in our 2021 study. In a tight business environment, the cloud gives organizations the ability to be agile and to respond more quickly to competitive threats.

As organizations accelerate their migration to the cloud, they need to remember that the cloud is not the same as on-premises and that, to enable cloud security success, there is a clear need to embrace and implement automation as part of a holistic strategy.

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