Cyscale

The Buyer's Guide:

Cloud Security Solutions for Startups

Where do I even start when it comes to cloud security?

Cloud security is a critical consideration, there's no denying that. From your intellectual property and software services you sell, to sensitive data on customers and users, any threat can put your reputation on the line.

While public cloud resources are key enablers of business, they come with the adoption of a shared responsibility model that makes it difficult to define your security perimeter. This makes securing your apps and data in the cloud a complex and confusing process. But it doesn't have to be. Good cloud security is achievable for any business, regardless of size, and it shouldn't take all your time and resources to get it right.

Context is king

How many cloud resources or assets am I running? What even is a cloud resource? My engineers are creating new assets every week, how am I going to keep track of them all? Where does the responsibility of AWS end and mine begin? These are the kind of questions you are going to be faced with, whether cloud security is your full-time job or just part of your responsibility for the overall tech stack.

Finding answers to these questions and more, will take time and effort because there are no standard responses. Everyone's cloud infrastructure is different and brings with it unique risks.

This is why context is so important. Cybersecurity tools are notorious for creating alert fatigue – an overwhelming number of alerts for every vulnerability, misconfiguration, and new threat out there. Following up on all these alerts as and when they come in, can easily start out as a fool's errand and frequently become humanly impossible.

For example: An unsecured Virtual Machine in isolation may pose no risk but will still trigger an alert. An unsecured VM that has access to a bucket used to store sensitive client data poses a much bigger risk that your company, your customers, and your lawyers will care about.

Identify

Being able to identify the risks is only one part of the challenge.

Prioritize

Understanding the context of the risk to prioritize it is an essential second stage in the process.

Fix

The steps needed to remediate the risk are the third stage in the solution.

Because there is no one-size-fits-all solution to cloud infrastructure security, any attempt to follow this path will eventually result in frustration due to not feeling in control, and a lack of understanding of the impact of a security issue, which can lead to bigger threats.

My cloud provider has its own security tools, can't I just use them?

All the big cloud providers, such as AWS, Azure, and Google Cloud, offer a suite of security tools specific to their products and these are a common choice for cloud native organizations as they can be added on when buying cloud services and are built by the same provider.

But these solutions have evolved in line with the sprawling menu of cloud services on offer, and the application of these tools has become granular to the level where some security components and their corresponding configuration are attached to specific products and services, and then again to specific regions and resources.

The cloud providers charge for security services in much the same way they do for cloud resources. Not only does this frequently trigger the 'bill shock' associated with cloud consumption, because activating a native security solution for a service introduces unpredictability into the pricing, it makes management of your cloud security posture very complex and time consuming.

This approach has significant implications for context as well – because information is scattered within the toolset, you are required to make the relevant correlations yourself, resulting in poor overall visibility and blind spots.

Furthermore, this is just for a single cloud environment. If your organization needs to secure apps or data across multiple clouds, you need to learn a whole other set of security services and tools specific to the cloud environment.

So, if you use the AWS supplied toolset, you must go to 1,000 different places to understand all your security settings, let alone how all the security settings relate and connect to one another. And when you go to Azure, it's another 1,000 places that you go to check.

Of course, some companies will become proficient in using the cloud provider's own security tools, but there is still the associated cost in deployment and the investment into a non-transferrable skill. This can result in cloud security know-how being concentrated within certain people and makes it difficult to understand your broader posture from both a cloud security and compliance perspective.

What about the big-name cloud security solutions I read about in a Gartner report?

There are well-established vendors, like Check Point, that have developed their portfolios over time, and there are relative newcomers to cloud security, like Orca and Wiz, that have picked up big name customers and you would be wise to assess these offerings.

However, most of these solutions are targeted at enterprise customers with big teams and big budgets, and even the analysts note that some of the most comprehensive security solutions are not suitable for smaller organizations due to the investment required in skills, deployment, and management, not to mention the overall cost.

For even the most experienced of users, heavyweight solutions can become overwhelming, resulting in a counter-effective approach as users lose control of their security posture.

But there are free tools I can use

The cloud security landscape is very competitive and there are a range of tools available that claim to be completely free. But anyone making security tools for cloud infrastructure knows that cybersecurity is not something you can cut costs on, so these tools will not remain free, except perhaps for the smallest organizations.

Most of the free tools are limited in scope or capability requiring a paid 'upgrade' to unlock. Others are designed to be self-installed at the free level – a challenge in itself – while the as-a-service version comes with a price tag.

In short, you get what you pay for, and solutions that have no investment in their development are unlikely to offer the level of service and support you get from a paid solution. These tools will quickly become frustrating due to a shortfall in features and an overreliance on multiple offerings to achieve an inferior result.

Cyscale itself offers a free trial of the full product with no limitations, as well as onboarding support to ensure you will get the most value out of our solution before you buy.

How do I address cloud infrastructure compliance?

Enabled by the agility of cloud computing, many companies launch SaaS products into the market without fully understanding the regulatory climate, then realize they need to show compliance.

With an infrastructure that changes on a weekly or even daily basis as engineers spin up new VMs and resources, preparing for an audit can be stressful, especially in regulated environments where you have to check your security posture against frameworks such as CIS Cloud Benchmarks, ISO 27001, SOC 2, GDPR (General Data Protection Regulation), HIPAA, PCI DSS (Payment Card Industry Data Security Standard), NIST, or many others.

Further challenges can arise in organizations where engineers have adopted a cloud provider's own security tools, as these products are notoriously difficult to get visibility into whether established policies are being followed in implementations, leaving you blind to security drifts.

At the end of the day, compliance should be delivered as a byproduct of good security, and your Cloud Security Posture Management (CSPM) approach should ensure you are able to see compliance with regulatory frameworks and policies without the need to manually correlate reports from multiple applications.

Identity, Access, and Entitlements

One of the biggest challenges when building applications in the cloud is identity, access, and entitlements, sometimes referred to as Identity and Access Management (IAM). This refers to all the best practices and rules that must be followed when establishing authentication and authorization for a user to an organization's systems and applications, because while keeping track of who has access to what sounds simple, it's something that is really difficult to do in the cloud.

Moreover, access is not restricted to human users; applications and other types of identities also require access to different types of resources.

Of course, the big cloud providers each have their own unique approach to access management, and this means learning approaches specific to each cloud environment. Some cloud security solutions integrate with AWS, Azure, Google Cloud and other vendors to check for vulnerabilities and help you manage identities and access form a central location, improving your organization's cloud security posture.

Understanding the cloud infrastructure security landscape

Glossary

CSPM

Cloud Security Posture Management (CSPM) solutions are designed specifically for cloud environments, using the Application Programming Interfaces (APIs) offered by public cloud providers to gather rich data on cloud configuration and workloads. Cloud security platforms use their own sophisticated technologies to process and analyze this data to identify misconfigurations, vulnerabilities, and risks, with some adding additional context and identifying potential threats, as well as suggesting remedial measures before any actual breach occurs.

Misconfiguration

An incorrect configuration of a cloud system that may lead to vulnerabilities. Possible misconfigurations are too many to list but may include making sensitive databases publicly accessible, creating identities with access rights more elevated than required, enabling write access on a resource that should be read only.

Vulnerability

A vulnerability is an inherent weakness in a cloud system that means a resource is unable to resist the actions of a threat agent. A vulnerability could be created through a misconfiguration, or series of misconfigurations, but it could also be a newly discovered flaw in a piece of code or software that a resource is dependent on.

Threat

A cloud threat is a type of attack or adversary looking to exploit vulnerabilities and misconfigurations, resulting in data breaches, data loss, system hijacking, and a myriad of other internal and external threats.

Resource

A cloud resource, also known as an asset, refers to any one of a number of entities including but not limited to, a virtual machine, a database, or storage bucket. An asset could also refer to VPC, subnet, policy, security key, or IP address.

CNAPP

A CNAPP (Cloud-Native Application Protection Platform) is a security solution designed to protect cloud-native apps. A cloud-native application is an application that is designed for, run and hosted in the cloud.

CIEM

CIEM (Cloud Infrastructure Entitlements Management) tools manage identities and access privileges to cloud infrastructure and services. It is often deployed as an umbrella solution that includes Identity and Access Management (IAM).

Further reading

Visit Cyscale.com for more resources like this!