EBOOK

7 Best Practices for Cloud Security Posture Management

CloudHealth by vmware

Introduction

Public clouds have fundamentally changed the way organizations build, operate, and manage applications. Developers now have easy access to a variety of cloud services and tremendous flexibility in how each service can be configured in order to build complex, modern applications. However, this freedom to innovate also comes with its own set of security risks.

The rising number of cloud data breaches due to simple service misconfigurations is forcing public cloud security owners to rethink classic security concepts and adopt approaches that better address the needs of developers building the dynamic, distributed cloud infrastructure. This includes rethinking how security teams engage with developers and IT, identifying new security and compliance controls, and designing automated processes that help scale security best practices without slowing down innovation.

As a result, teams tasked with securing their organizations' cloud environments have focused on what is known as cloud security posture management, or CSPM, which is **defined** as "a continuous process of cloud security improvement and adaptation to reduce the likelihood of a successful attack."

We interviewed several security experts and asked them how public cloud transformation has changed their approach to cloud security posture management. In this eBook, we'll share seven best practices we discovered during our research.

01

Establish a Cloud Center of Excellence

When it comes to driving success in the public cloud, many organizations find that the biggest hurdle they must overcome is not related to technology, but to people and processes. Leading organizations are establishing a formalized Cloud Center of Excellence (CCoE)—also known as a Cloud Business Office, Cloud Strategy Office, or Cloud Program Office—which is a cross-functional team tasked with supporting and governing the execution of the organization's cloud strategy.

Security and compliance is one of the three key areas of excellence within a CCoE (in addition to cloud financial management and operations). **The CCoE is responsible for:**

- Ensuring continuous compliance with relevant standards
- Staying up-to-date with the changing threat and compliance landscape
- Translating business requirements into cloud security standards

If your organization does not currently have a CCoE in place, this should be your first step towards building an effective cloud security posture.

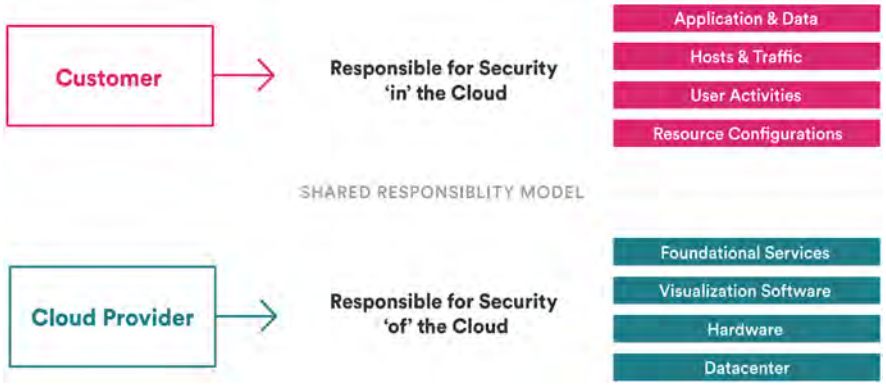
02

Distribute Cloud Security Responsibilities

Once you've established a Cloud Center of Excellence, you can effectively distribute cloud security responsibilities across your organization. There is often confusion over the division of security responsibilities in the cloud. Not knowing who owns tasks for ensuring security and compliance in a dynamic cloud environment can lead to blind spots in your cloud security posture.

There is a shared security responsibility between the cloud provider and the customer. Shared responsibility can vary depending on the cloud provider and service, but in general, the cloud provider is responsible for the security of the cloud, and the customer is responsible for security in the cloud.

For example, the cloud provider assumes responsibility for the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The customer assumes responsibility for the guest operating system, applications and workloads, identity and access management, and the configuration of cloud services.



In addition to security responsibilities between the cloud provider and customer, it's also important to identify responsibilities internally. Cloud security is no longer a function of just one team—it's a shared responsibility throughout the organization, with each department understanding the security risks and policies of the cloud services they're using.

The CCoE should define the lines of security responsibility amongst individuals and teams within their organization, and then prevent silos by enabling efficient information-sharing and implementing a regular cadence of communication. With this, stakeholders from across functional teams can understand the cloud security implications of decisions before implementing them, along with the actions expected of them to maintain a strong cloud security posture.

03

Gain Visibility Into Your Entire Cloud Environment

As the saying goes, “you can’t protect what you can’t see,” it’s critical to have visibility across your entire cloud environment for a successful cloud security posture. Cloud service providers offer native monitoring tools that can be helpful to an extent, but have limitations, especially when it comes to getting detailed context and visibility across hybrid cloud or multi-cloud environments.

Leading third-party **cloud security and compliance solutions** can provide a complete picture of your cloud environment, across hybrid, multi-cloud, and containers.

When evaluating the cloud security solution for your business, there are a few questions to keep in mind in terms of visibility:

- Does it provide granular visibility across different asset types (accounts, owners, IaaS, PaaS, serverless)?
- Can it show relationships and dependencies between cloud services (not just in isolation)?
- How often is data updated? Weekly, daily, or near real-time?
- Can I visualize information by category (projects, cloud providers, teams, etc.)?

In addition to having the right tools for visibility into your infrastructure, it’s important to have a coordinated approach to collecting, organizing, and analyzing your data. As a best practice, implement consistent tagging policies by application, owner, resource, department, etc. to break down reliable information by the categories most important to you.

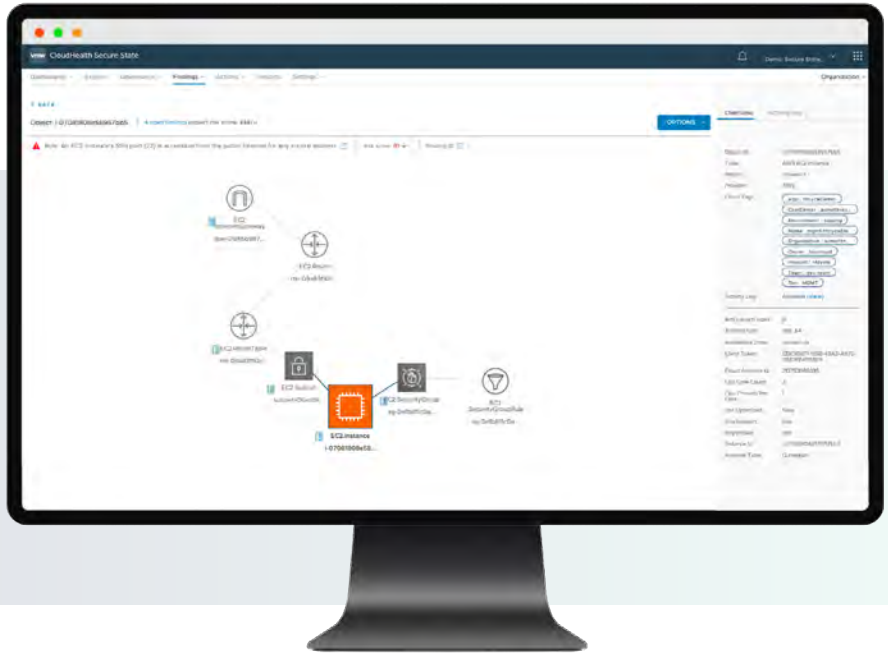
04

Detect Security Risks and Misconfigurations in Context

After attaining complete visibility of your cloud environment, then you can effectively detect risks and misconfiguration vulnerabilities. Many cloud security detection tools will provide isolated information. It can show that within a security group, a resource type is not compliant with a certain rule, but this doesn't provide insight into the level of risk, how it's connected to other resources, or recommendations for next steps.

For example, an EC2 instance with SSH port (22) accessible from any source address is a medium risk security violation.

SSH port is commonly used for administrative access and is an attractive target for attackers. However, the relationship diagram below also shows that the same EC2 instance is connected to an internet gateway. This relationship makes this SSH port publicly accessible, thus elevating the overall risk of the security violation.



To better prioritize security issues and make your job easier, look to leading cloud security solutions that can visualize cloud resource relationships and misconfigurations in context, detect security risks in real-time across cloud platforms, and track progress for detections and remediations.

05

Remediate Issues with Automation

With the rate at which workloads are deployed in the cloud and the number of people that can deploy at the same time, speed is key when it comes to cloud security. Bad actors today rely extensively on automation and can target new cloud misconfiguration vulnerabilities quickly, sometimes in just under a minute. While the attacks are getting more frequent and sophisticated, cloud security teams must rely on automated remediation in order to scale.

Initially, most security teams resist auto-remediation. They worry that without reviewing, automated actions could break production or cause other problems. The key to automation for cloud security teams is to segment security actions into ones that can be fully automated and those that need human intervention.

As a best practice, fully automated actions or guardrails are cloud security policies and configuration standards that apply universally across cloud teams or resources. Examples include policies that deny accidental changes to baseline security monitoring controls or those that require boundary permissions for all IAM users and roles.

The policies you choose to automate, and at which level, depends on the organization. The CCoE is responsible for defining where to automate policies and where manual actions may be needed, which brings us to our next best practice.

06

Define Standards and Controls With a Cloud Governance Program

Cloud security teams need to strike a balance between giving cloud users what they need when they need it, and also putting rules in place to ensure security. To do this, align with your organization's CCoE to create a cloud governance program where you define best practices, socialize them, and take action when a policy or standard is violated. **When defining policies, consider your controls, target environments, and exceptions:**

CONTROLS

The Center for Internet Security (CIS) provides a list of cloud security controls that are a good place to start, but especially if you're in a highly regulated environment such as Healthcare or Government, ensure your controls cover all the guidelines you require (e.g. HIPAA, GDPR, NIST).

TARGET ENVIRONMENTS

Once you've defined your controls, specify which environments they do or do not apply to. Should the control be applied business-wide? For internal or external environments? For development, testing, and production environments?

EXCEPTIONS

They're going to happen, so plan out the workflow and documentation around exceptions—what are the exceptions specifically? How long is the exception in place? For which users does the exception apply?

To see how a control might look like in your organization, here's a practical example:

Control: EC2 instance is Publicly Accessible and has elevated privileges for S3 Buckets (CIS AWS, NIST 800-171, EU-GDPR)

Target environment: All Production SaaS Accounts

Exception: Whitelist/suppress accepted EC2 instances with Tag App1

PRO TIP

To help increase cloud security policy adoption, ensure policies are clearly defined and something a developer could actually put into code. For example, if you have a policy that passwords must be complex, it would be better to have a policy that passwords must be greater than 12 characters because a developer can implement this function into their code.

07

Shift Left Security Testing

Our final best practice is to “shift left” security testing by integrating security checks proactively into the application deployment processes. Why is this so important?

It’s critical to detect security violations as early as possible, otherwise you risk notifying a developer of an issue after they’ve already moved on to something new. Switching context to analyze violations in a piece of code that was deployed a few weeks back can be extremely time-consuming. In many cases, remediation might require disruptive changes, resulting in ugly workarounds and accumulation of technical debt.

To counter these issues, organizations adopt a continuous security model, where the goal is to build security checks right into the continuous integration and delivery (CI/CD) pipeline.

Besides the static code analysis, this involves continuous monitoring for risks such as host vulnerabilities or misconfigurations at the time of resource deployment. In case a violation is detected, a remediation workflow automatically kicks in to remediate the violation or trigger a notification to the developer, requesting them to fix the issue or provide justification for an exception. This ensures that the violation is resolved before the application hits production, resulting in a delivery model that’s secure by design. This approach also establishes a continuous feedback loop for security teams to refine their policies over time and for developers to adopt best practices.

Besides continuous verification, many teams also leverage resource templates that are already solidified and certified by security teams. These templates should be defined as code, as it makes it easier for developers to start with a baseline and then modify design and resource configurations based on application needs. Starting with standardized templates improves productivity and reduces the probability of developers making a security mistake. Once the application is deployed in production, the environment should be continuously monitored for configuration drift.

A continuous security approach improves developer productivity and helps companies and their customers build confidence in the security of new releases.

Conclusion

Reducing misconfigurations, monitoring malicious activity, and preventing unauthorized access are foundational activities necessary to ensure security and compliance of applications and data in the cloud. As criminals become more sophisticated in their abilities to exploit cloud misconfiguration vulnerabilities, security teams need a smarter approach to prevent security breaches.

CloudHealth Secure State is an intelligent cloud security and compliance platform that helps organizations reduce risk and protect millions of cloud resources by remediating security violations and scaling best practices at cloud speed.

To learn more about CloudHealth Secure State, **visit us online to schedule a demo**, where we'll walk you through our rich feature set and how you can improve your cloud security posture with simple steps and industry best practices.

Learn more about how CloudHealth Secure State can help you improve your cloud security posture **here.**