In the shared security model of the public cloud, customers are responsible for the security and compliance implications of resource configurations. This can be especially challenging in a decentralized cloud environment, with users capable of configuring resources rapidly. Based on interviews with security experts on how public cloud transformation has changed their approach to cloud security posture management (CSPM), here are the biggest challenges and questions you should be asking to maintain secure and compliant cloud configurations.

### Your Cloud Security Posture Checklist

**CHALLENGE:**

- Adapting security policies to cover usage across public cloud platforms and environment types.
- Integrating cloud security posture management into day-to-day operations.
- Prioritizing configuration errors based on severity.
- Ensuring teams adhere to standards for secure cloud configurations.

Many organizations find that the biggest obstacle in cloud security is not related to technology, but to people and processes. To address these challenges, many of our customers establish a cross-functional team, often referred to as a Cloud Center of Excellence (CCoE) or Cloud Business Office, tasked with creating standards that balance cloud security posture management with the organization's top priorities. Learn more here.

Many cloud security detection tools provide isolated information, such as the resources that do not comply with certain rules. However, this doesn't provide insight into the level of risk, how the resource is connected to other resources, or recommendations for next steps. Context is key to ensuring teams can focus on the risks with the greatest potential to lead to a data breach.

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. Align with your organization's CCoE to create a cloud governance program to define and socialize best practices, and take action when a policy or standard is violated.

When it comes to enforcement at scale, automation is key. Ensure the right stakeholders are informed of severe violations, and consider auto-remediation to fix some of the more common violations without disrupting workflows or applications.

### Your Cloud Security Posture Management

**CHECKLIST**

**CHALLENGE:**

- Are you able to visualize configurations across all public cloud platforms and environment types?
- How do you know if configurations in your environment affect compliance with the regulatory standards that apply to your organization (e.g. GDPR, PCI, HIPAA)?
- Can you detect configuration errors, compliance violations, or security vulnerabilities in real-time?
- Are you able to understand how individual configuration errors can impact other resources in your public cloud environment?
- Can your teams sort through the scale of your cloud providers’ native monitoring notifications and prioritize configuration errors based on severity?
- Do your teams have the context and information they need to remediate a configuration error, such as who the person or teams to notify, action required, and details to identify similar errors elsewhere in the cloud environment?

### CloudHealth Secure State

For more information about how to apply these best practices, see our complete guide here. Or, get in touch with one of our cloud security experts directly, where we’ll walk you through how you can use CloudHealth Secure State to implement a successful cloud security posture in your organization.

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. Adopt a continuous security model, where the goal is to build security checks right into the continuous integration and delivery (CI/CD) pipeline.