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. 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.

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.

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.

Your Cloud Security Posture Management

CHECKLIST

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.

You can read the complete guide here. You can also see our complete guide here. For more information about how to apply these best practices, see our complete guide here.