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.

**Challenge:** Adapting security policies to cover usage across public cloud platforms and environment types

- Are you able to visualize configurations across all public cloud platforms and environment types?
- How do you know if configurations are 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?

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.

**Challenge:** Integrating cloud security posture management into day-to-day operations

- Are your IT/security teams working in alignment with your organization’s top priorities?
- Are you able to automatically alert the relevant stakeholders when a policy or standard is violated?
- Can you prioritize configuration errors based on severity?
- Can your teams sort through the noise of your environment to 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.

**Challenge:** Detecting configuration errors in a distributed and complex cloud environment

- Are you able to visualize configurations across all public cloud platforms and environment types?
- How do you know if configurations are 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?
- Can your teams sort through the noise of your environment to 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.

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.