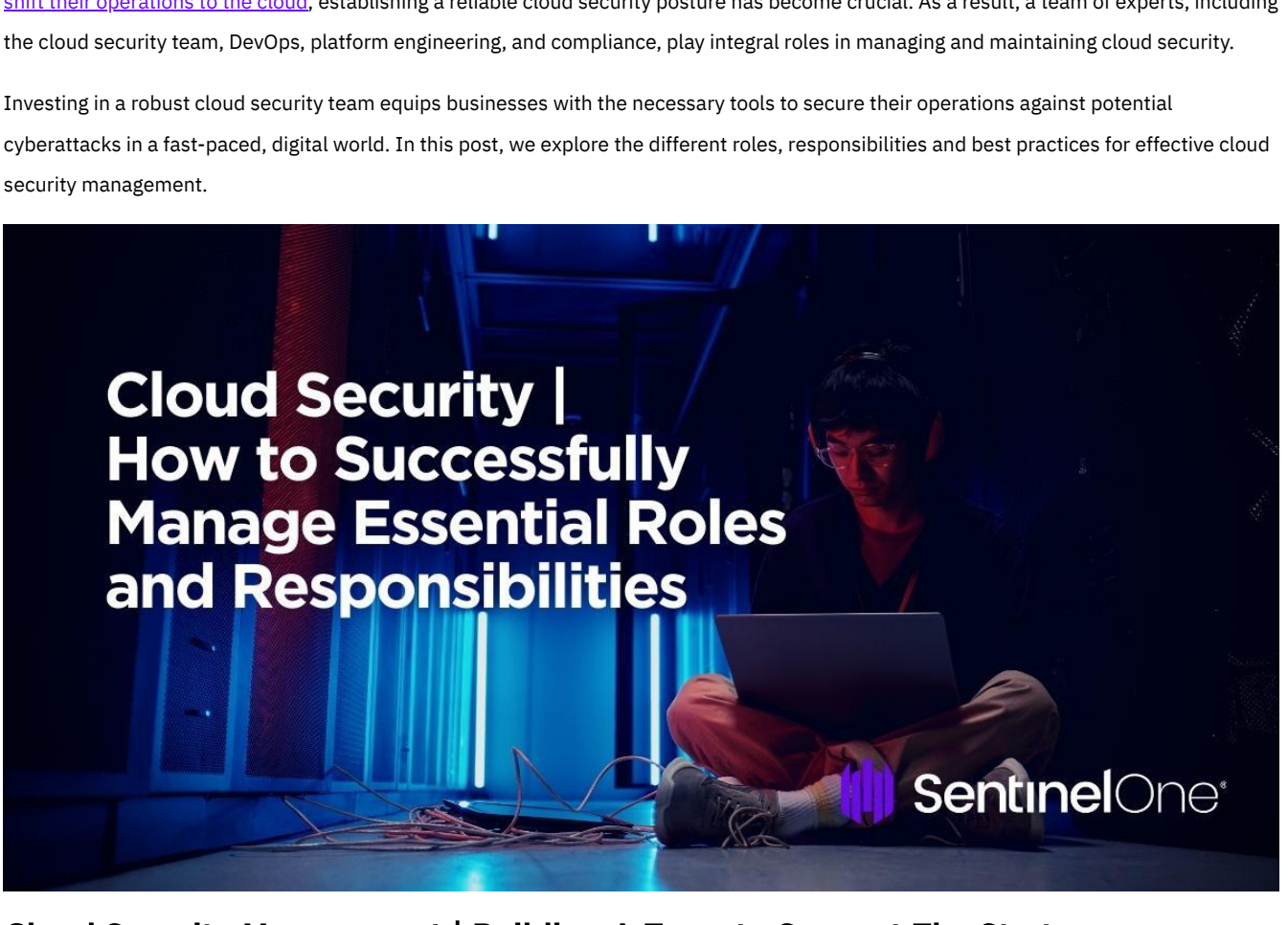
Cloud Security | How to Successfully Manage Essential Roles and Responsibilities

March 21, 2023
by SentinelOne

Protecting company data from cyber threats is an essential and ongoing responsibility for enterprises of all sizes. As more organizations shift their operations to the cloud, establishing a reliable cloud security posture has become crucial. As a result, a team of experts, including the cloud security team, DevOps, platform engineering, and compliance, play integral roles in managing and maintaining cloud security.

Investing in a robust cloud security team equips businesses with the necessary tools to secure their operations against potential cyberattacks in a fast-paced, digital world. In this post, we explore the different roles, responsibilities and best practices for effective cloud security management.



Cloud Security Management | Building A Team to Support The Strategy

Cloud security strategies take time to develop and implement. Having the right team dedicated to cloud security ensures that any cloud-related strategies, decisions, and workflows align with the needs of the business and follow industry best practices.

Depending on their size and security maturity, organizations may choose to manage their cloud security through a Cloud Center of Excellence (CCOE) or, alternatively, build an in-house cloud security team as an extension of the larger security team.

Establishing Oversight | Cloud Centers of Excellence (CCOE)

A Cloud Center of Excellence (CCOE) is an organizational entity that has become a popular choice for many businesses to help accelerate cloud adoption. A CCOE is dedicated to the organization's strategy for cloud, including its implementation, management, upkeep, and security.

With a CCOE in place, organizations can make business decisions with security at the forefront, rather than as an afterthought. They are also a key component in maintaining effective security for an organization's entire cloud operations and portfolio as it continues to scale.

CCOEs operate through three main pillars to deliver a best practice approach to driving cloud-enabled security strategies. As a centralized function, CCOEs hold the following responsibilities:

- Establish Governance – Through the CCOE, cloud security policies are created in collaboration with cross-functional champions and in alignment with the overarching cloud strategy and any cloud management tools used.
- Provide Brokerage – CCOEs assist senior leadership and technical teams with selecting cloud security providers and architect the cloud solution in a way that meets the unique needs of the business and any regulatory controls.
- Build Community – Cultivate a culture of knowledge-sharing regarding cloud best practices and developing technologies. A CCOE is responsible for sharing this knowledge though easily accessible knowledge base and source code repositories as well as training opportunities.

Utilizing In-House Resources | Cloud Security Teams

An in-house cloud security team is responsible for managing the security of an organization's cloud infrastructure, working closely with other teams in the organization to ensure that cloud security is integrated into every aspect of business operations.

This dedicated team sets up and manages security policies and access to cloud resources, then implements security controls to protect the overall cloud infrastructure. They also monitor the cloud infrastructure for security breaches and respond to incidents as they occur.

Cloud security teams hold the following responsibilities:

- Regularly reviewing and updating security policies to reflect changes in the organization's operations and the latest security threats.
- Implementing multi-factor authentication (MFA) to protect against unauthorized access to cloud resources.
- Using managed key services for key rotation and ensuring they are safely stored in a segmented area. Encryption is used to protect sensitive data while in transit and at rest.
- Conducting regular security audits and vulnerability assessments to identify and address potential security risks.
- Establishing incident response procedures and regularly testing them to ensure they are effective.

Organizations that opt to build cloud security teams in-house will typically appoint set cloud-based roles and responsibilities for existing C-level executives as well technical leads from IT, DevOps, and Engineering teams. These roles all satisfy particular functions of the cloud security strategy and can be broken down into a structure such as the following:

- Cloud Security Executive – This role is usually assigned to an organization's Chief Information Security Officer (CISO). This is the team's C-level liaison responsible for analyzing current security demands of the business and forecasting future cloud security trends. This executive role designs the company's security roadmap, embedding any cloud-based security requirements needed. In this role, the CISO will be accountable for overseeing the rest of the cloud security team and enforcing changes to policy and processes across the organization.
- Cloud Security Architect – This role acts as the lead for the cloud security team and is responsible for creating and implementing new cloud security workflows and cloud-based incident response use cases. The Cloud Security Architect must have a deep understanding of their organization's strategy and processes and ensure that any cloud security policies and processes are aligned with the rest of the business.
- Cloud Security Engineer – Those assigned to this role are responsible for overseeing the day-to-day security operations of the cloud infrastructure. This includes monitoring for cloud-based threats and checking the performance of the IT framework.
- Cloud Security Auditor/Tester – A significant role in the cloud security team, auditors are responsible for performing regular penetration tests on the organization's cloud infrastructure and bypassing its defenses. This role is critical to the ongoing improvement cycle and supports the upgrade of security processes by detecting possible exploits, areas of weaknesses, and any inefficiencies.

Understanding the Role of DevOps in Cloud Security

DevOps is a software development and deployment approach emphasizing communication and collaboration between development and operations teams. In terms of cloud security, DevOps teams are responsible for developing, testing, and deploying software applications in the cloud.

DevOps teams play a critical role in the cloud security strategy by ensuring that security is integrated into the software development process. This includes identifying and addressing potential security risks during the development phase and implementing security controls to protect software applications in the cloud.

Oftentimes, the cloud security team will route their findings to the DevOps engineering team to be fixed within pre-set service level agreements (SLA). Based on the severity level of the findings, cloud security teams may run campaigns to monitor and investigate findings that exist outside of the SLAs to ensure DevOps teams are not overrun.

A best practice for the central cloud security team is to ensure that each cloud account has an accurate and updated list of contacts assigned to it. Only contacting the correct stakeholders to receive notification ensures that the routing per account is as streamlined and effective as possible. Organizations may use tools such as PagerDuty to route notifications to the correct on-call DevOps engineer.

Ways DevOps Teams Can Support Cloud Security

- Conduct regular security training for team members to raise awareness of security risks and best practices.
- Use automated tools to detect and address potential security vulnerabilities during development.
- Implement security controls, such as access controls and monitoring, to protect software applications in the cloud.
- Work closely with the cloud security team to ensure security is integrated into the software development process.

Understanding the Role of Platform Engineering in Cloud Security

Platform engineering is a technology approach designed to accelerate the delivery of applications to support the specific needs of the business. Constantly evaluating the software development lifecycle, its function improves the productivity and experience of developers so that they can move from source to production efficiently.

Their role within the greater cloud security strategy is to ensure that security is built directly into the organization's platform. Platform engineering teams are also an essential element in ensuring that cloud infrastructure is secure and reliable. This includes implementing security controls to protect cloud infrastructure from potential security threats (e.g., ensuring that DevOps engineers can only access cloud resources with secure defaults and that cloud workload protection platform (CWPP) agents are embedded into golden images.

Ways Platform Engineering Can Support Cloud Security

- Regularly review and update security policies to reflect changes in the organization's operations and the latest security threats.
- Implement security controls such as firewalls and intrusion detection systems to protect cloud infrastructure from potential security threats.
- Conduct regular security audits and vulnerability assessments to identify and address potential security risks.
- Work closely with the cloud security and DevOps teams to ensure security is integrated into the infrastructure and platform design process.

Understanding the Role of Compliance in Cloud Security

Compliance teams ensure that an organization meets regulatory and compliance requirements. This includes maintaining compliance with industry standards and regulations, such as PCI DSS, HIPAA, and GDPR.

Compliance in cloud security includes implementing security controls to protect sensitive data stored in the cloud and providing access to cloud resources is restricted to authorized personnel.

Ways Compliance Teams Can Support Cloud Security

- Ensure that regular audits and assessments are conducted to ensure ongoing compliance.
- Regularly review and update compliance policies to reflect any regulatory and compliance requirements changes relating to cloud computing.
- Implement security controls, such as access controls and encryption within the cloud infrastructure.
- Work closely with all teams involved with cloud security to ensure that security controls are implemented in compliance with industry regulations and standards.

Conclusion

Like other security aspects, an effective cloud security posture requires achieving a synergy between people, processes, and procedures within the organization. An essential first step toward that objective is understanding the roles and responsibilities of the cloud security team, DevOps, platform engineering, and compliance teams.

Singularity Cloud Workload Security is a runtime cloud threat protection, detection, and response for multi-cloud workloads. Whether your workloads run the on-prem or public cloud, in VMs, containers, or Kubernetes clusters, SentinelOne works alongside other security controls to do what they do not: stop runtime threats like ransomware, zero-days, and memory injection. To learn more, visit our product page to find customer testimonials, whitepapers, and more.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- Detecting a Rogue Domain Controller – DCShadow Attack
- Demystifying the Top 5 Myths About Cloud Computing Security
- Surviving the Storm | Defending Against Cloud Misconfigurations, Vulnerabilities, and Insider Threats
- Threat Landscape | The Most Dangerous Cloud Attack Methods In The Wild Today
- Accelerating Your Cloud Security with Workload Protection
- EDR for Cloud Workloads Running on AWS Graviton