Deloitte.

Cloud security posture management

A guide for government agencies navigating the cloud

MAKING AN IMPACT THAT MATTERS since 1845

Introduction

Cloud technology continues to become more widespread across state, local, and federal governments, as well as higher education organizations. As the adoption rate of cloud continues to increase, so too does the need for attention to detail when applying appropriate security measures. Trying to maximize the benefits of the cloud while developing a strategy that adheres to security, compliance, and regulatory requirements for cloud infrastructure can be challenging.

The purpose of this document is to educate readers on leading practices for implementing cloud security within cloud infrastructure. It will provide an overview of familiar challenges agencies face when thinking about cloud security, a proposed solution to cloud security in cloud security posture management (CSPM), CSPM options, and considerations to help agencies get started.

Common agency challenges

Some challenges that agencies commonly face when trying to account for cloud security include adhering to regulatory compliance frameworks when initially configuring environments, properly identifying and remediating infrastructure misconfigurations in real time, and properly implementing procedures for securing newly deployed resources.

Adhering to regulatory compliance frameworks

Using cloud technology presents new requirements to government agencies in terms of security and compliance. A commonly used framework to achieve government cloud security is the Federal Risk and Authorization Management Program (FedRAMP). FedRAMP provides a standardized approach to security assessment, authorization, and continuous monitoring specifically for cloud products and services used by federal entities that store, process, and transmit federal information.[1] FedRAMP is a cloud-specific implementation of the National Institute of Standards and Technology Risk Management Framework (RMF) and is a more targeted iteration of the Federal Information Security Modernization Act of 2014. FedRAMP requires a rigorous authorization process and has three main impact levels of low, moderate, and high, dependent on the number of applicable controls. Often, compliance requirements force agencies to consider authorization procedures for RMF in addition to FedRAMP, where RMF serves as a general framework to which FedRAMP controls can be applied. There is also StateRAMP, which is essentially a version of FedRAMP aimed to help speed up the FedRAMP authorization process for state and local governments. Understanding the similarities and differences of these frameworks can be confusing for agencies newly migrating to the cloud. Agencies should have a simplified mechanism for understanding where they fall on the FedRAMP spectrum and how to achieve and maintain ongoing compliance in an automated manner.

Identifying and remediating infrastructure misconfigurations in real time

Part of maintaining ongoing FedRAMP compliance includes proper configuration management for cloud solutions. Cloud misconfigurations represent one of the biggest threats to cloud security. They can expose the environment and leave it vulnerable to breach, something government agencies cannot afford to have happen. Misconfigurations come in various forms, from overly permissive security settings to unintended exposure of sensitive data, making it a multifaceted problem that requires constant attention. The interplay of human error and complexity of modern cloud infrastructure can make it difficult to keep track of every configuration of every resource. Ever-changing cloud environments require dynamic solutions rather than point-in-time scans to identify deficiencies.

Government agencies should consider taking additional measures to properly identify in real time and remediate misconfigurations that occur at the cloud infrastructure layer on a continuous basis.

In the broadest sense, most cloud misconfigurations are settings left in a state that is favorable to the aims of malicious attackers. Here are some common categories:

- Unrestricted ports, both inbound and outbound
- Secrets-data management failures, such as passwords, encryption keys, application programming interface (API) keys, and admin credentials
- Leaving open the Internet Control Message Protocol
- Disabled logging and monitoring
- Unsecured backups
- Non-validation of cloud security controls
- Unblocked non-hypertext transfer protocol secure /hypertext transfer protocol ports
- Excessive potential access to containers, virtual machines, and hosts.
- Dangling domain name systems (This results from changing a subdomain name without removing the underlying canonical name entry, which may allow an attacker to register it)[2]

Securing newly deployed resources

Part of continuous monitoring for cloud misconfigurations includes accounting for constantly changing environments. The shift from manual deployments to a development, security, and operations (DevSecOps) approach represents a fundamental change in software development and information technology operations. Manual deployments involve time-consuming, error-prone processes, whereas DevSecOps emphasizes automation, continuous integration, security integration, infrastructure as code, and efficient resource management. This transition enables faster, more secure, and scalable resource management, aligning development and operations for improved efficiency and reliability. One of the main benefits of cloud is the simplicity of provisioning resources as an organization expands its cloud footprint. New resources are often deployed in the form of storage, accounts, and servers to support application runtimes. As previously mentioned, these resources present gateways to common misconfigurations that occur in cloud environments. Government entities should consider ways to maintain an asset inventory that shows resource compliance and make sure that an initial security/compliance check is performed on newly deployed resources to help mitigate concerns.

Cloud security posture management

With so many challenges, it is a leading practice to adopt an approach to cloud security that is detailed and adaptive so that it may be applied across both the breadth of different cloud service provider (CSP) environments and depth of each account.

CSPM can help streamline an agency's approach to cloud security. Using the tools and services offered by CSPM, an agency can automate its security and compliance activities within the cloud, reducing the need for manual effort. CSPM can identify misconfigurations within a cloud environment and produce automatic alerts to allow teams to respond quickly and remediate issues.

As the CSPM landscape has evolved, two directions have emerged for agencies to consider when getting started: *cloud-native* and *third party*. These two distinct approaches offer individual advantages and considerations, each shaping the way

organizations harness and leverage technology to achieve their goals. Let's delve into the key differentiators between these approaches, introduce a few examples, and explore how they can affect an organization's mission.

Cloud-native

Cloud-native CSPM solutions are native to their respective CSP. These solutions cover the basic security needs for an organization and are often simple to configure. The three major CSPs (Amazon Web Services (AWS), Google Cloud, and Microsoft Azure) each possess native services that enable CSPM capabilities. These solutions offer tools for securing cloud resources and are tailored to their corresponding cloud environment, offering integrations within their native infrastructure.

Overall, cloud-native solutions include flexible cost dependent on resource consumption that can be scaled as needed, and simpler integrations between other associated native cloud services. Each of the three major CSPs offer CSPM services with FedRAMP low, moderate, and high authorization. This translates to a suite of more than 400 applicable controls, which are commonly implemented and referred to as "policies" or "policy-as-code." Users can activate cloud-native CSPM capabilities without lengthy installation processes and can expect to find out-of-the-box tools for policy configurations of the amount of data the environment is processing, scaled according to need.

Cloud-native solutions, collectively speaking, are not cloud agnostic and require additional third-party connections to operate effectively in environments that leverage multiple CSPs (herein referred to as "multi-cloud environments"). The additional complexity of a multi-cloud environment creates elevated risk of misconfigurations and oversight. Furthermore, cloud-native solutions typically offer fewer features than third-party solutions. Because of this, customization is limited to what the respective service has available, which may be confining for agencies that need further flexibility.

The use case for a cloud-native CSPM solution is generally a single-cloud environment with a small to medium number of accounts.

Third-party CSPMs

Third-party CSPM tools are those that have not been created by a CSP. These solutions are often cloud agnostic, meaning agencies can use the solution regardless of being a single-cloud or multi-cloud entity. Third-party CSPM solutions allow organizations to gain a unified view of their overall cloud posture. Ideally, when choosing a third-party solution, an organization would have to procure only one solution as opposed to multiple to cover their environments.

One of the main perceived functionalities of utilizing a third-party CSPM is platform consolidation. For more complex entities, having a single, unified view of overall security posture is a significant upgrade from having to manage each CSP platform individually. This includes not only asset management but also vulnerability scanning and alerting. For analysts whose job is to monitor and protect the environment, having a centralized hub for tickets and violations can help to better optimize their time. Additionally, some third-party CSPMs allow for automated remediation of violations in real time, which is a vast improvement from having to manually address violations individually. Furthermore, third-party CSPMs allow for enhanced customization because of the connective nature of the solutions. Entities can choose to implement services in unison as desired and can leverage API connectors with the solution to achieve additional functionality.

Third-party solutions often come with licensing fees (price varying by solution) and increased risk exposure, as they require additional configuration to be compatible with respective CSPs. Agencies should consider collaboration with the creator's development team to properly implement them in the target environment as well as confirm if the third-party solution is FedRAMP compliant. If not, additional Authority to Operate procedures may have to be performed to enable compliance with FedRAMP standards.

The main use case for a third-party solution is a multi-cloud environment that has the appropriate resources to lead installation and low to moderate security requirements.

CSPM options

When considering whether to leverage a cloud-native or third-party CSPM solution, it is important to remember that each option will come with distinctive features and functionality. Below are a few options to consider for both cloud native and third-party solutions:

Cloud-native

AWS Security Hub

AWS Security Hub is a CSPM service that performs automated, continuous security best practices and checks against AWS resources to identify misconfigurations; aggregate security alerts (i.e., findings) in a standardized format; and enable users to digest, research, and remediate findings.[3] AWS offers a community knowledge base for resource support and infrastructure maturity. AWS Security Hub is FedRAMP authorized and utilizes several frameworks and standards to deliver current guidance and security leading practices for users. Some of the supported standards include National Institute of Standards and Technology (NIST 800), Payment Card Industry Data Security Standard (PCI DSS), and AWS Foundational Security Best Practices (FSBP). The ability for Security Hub to integrate with other AWS services such as AWS CloudTrail, Amazon Detective, and Amazon Inspector further enriches the reporting and monitoring efforts for the CSPM solution.

Microsoft Defender

Microsoft Defender CSPM possesses anti-malware and data security capabilities and can be used across various cloud platforms, offering CSPM for AWS, Azure, and Google Cloud infrastructures.[4] Features of Microsoft Defender CSPM include risk-based vulnerability management and assessments, attack surface reduction, automatic investigation and remediation, regulatory compliance dashboard and reports, and adaptive application controls. The Microsoft Defender CSPM solution uses controls mapped to regulatory benchmarks, including NIST and Center for Internet Security, to perform assessments and is FedRAMP (high and moderate) authorized.

Security Command Center (SCC)/Google Cloud Risk & Compliance as Code (RCaC)

The RCaC solution is a stack of compliance and security control automations that deliver a CSPM solution with a focus on reducing misconfigurations. Three of these Google Cloud services, Assured Workloads, SCC, and Risk Manager, offer CSPM benefits around regulatory compliance, misconfiguration monitoring, and risk monitoring and reporting. RCaC automates routine compliance checks. Through automation, RCaC offers security and compliance monitoring of code. Regarding SCC and other integrations, RCaC utilizes the Google integration partners to accelerate time to value for customers.[5] SCC offers several CSPM features to be leveraged by RCaC.

SCC is the security and risk management solution designed to identify misconfigurations, vulnerabilities, and threats to Google Cloud environments. Some features of SCC include attack path simulation, where paths of least resistance to critical resources are identified and exposure is scored; threat detection through specialized Google Cloud detectors for identifying compromised data and data exfiltration; and security information and event management and security orchestration and automated response integrations for detailed analysis on security events and findings.[6]

AWS Security Hub

Attributes:

- Community knowledge base
- FedRAMP authorized
- Integrable

Microsoft Defender

Attributes:

- Cloud agnostic
- FedRAMP authorized
- Auto-remediation

Security Command Center/Risk & Compliance as Code

Attributes:

- Automatable
- FedRAMP authorized
- Auditability and reporting

Third-party

Wiz.io

Wiz.io (Wiz) is an agentless CSPM solution that uses APIs to perform analysis on the respective resources being governed.[7] Wiz leverages frameworks like NIST, Health Insurance Portability and Accountability Act, and Payment Card Industry Data Security Standard to perform compliance checks on an organization using policy-as-code, and it has a proprietary framework that weights violations based on severity. Wiz's CSPM makes recommendations on violations based on perceived order of importance. The issues are modeled in the Wiz Security Graph to allow for a security engineer to view the issues spanning across the enterprise.[8]

Prisma Cloud

Palto Alto's Prisma Cloud provides visibility into systems across multiple cloud environments and analyzes the amount of risk associated with each, enabling the identification of misconfigured systems and/or those operating without the appropriate security standards in place. Prisma Cloud also provides analytics into users who access different systems. Prisma Cloud's User and Entity Based Analytics uses machine learning to view data points of previous user/system behaviors to determine if a user or entity is behaving inside or outside their normal uses.[9] Prisma Cloud has also received the FedRAMP moderate Authority to Operate.

Wiz.io

Attributes:

- Agentless (no installation needed)
- Prioritization of violations
- Compliance reporting
- Cloud agnostic

Prisma Cloud by Palo Alto

Attributes:

- UEBA and ML capabilities (auto-remediation)
- FedRAMP authorized
- Cloud agnostic

CFO insights

CSPM serves as a critical linchpin for a Chief Financial Officer (CFO) function, offering a practical solution that addresses both the nuts and bolts of technology and the bottom-line concerns of the business.

CSPM acts as a front-line defense, promoting the integrity of cloud infrastructures by identifying and remediating vulnerabilities. This technical fortification directly aligns with the CFO's responsibility to safeguard digital assets and ensure compliance with industry regulations.

From a business perspective, CSPM mitigates the risk of data breaches and optimizes cloud resources for cost effectiveness. By implementing CSPM, a CFO function may realize operational cost savings and potentially ward off financial losses from bad actors attempting to exploit vulnerabilities.

Forward-thinking federal and state government executives should continue to consider how potential applications of CSPM could transform their operations, increase cloud security, and deliver value.

Meet The Team

Mason Evans
Managing Director
Deloitte & Touche LLP
masevans@deloitte.com

Dean Lee
Specialist Leader
Deloitte & Touche LLP
deanlee@deloitte.com

Daniel Briggs
Senior Consultant
Deloitte & Touche LLP
dabriggs@deloitte.com

Endnotes

1. Tony Bai, "What is FedRAMP? Complete guide to FedRAMP authorization and certification," *CSA Blog*, November 7, 2022.
2. Mike Elgan, "Why are cloud misconfigurations still a major issue?," Security Intelligence, November 1, 2022.
3. Amazon Web Services (AWS), "AWS Security Hub features," accessed November 8, 2023.
4. Microsoft Defender for Cloud, "Cloud security posture management (CSPM)," last updated February 11, 2024.
5. Zeal Somani and Anton Chuvakin, "Modernizing compliance: Introducing risk and compliance as code," *Google Cloud Blog,* November 12, 2021.
6. Google Cloud, "Improve cloud security oversight with Security Command Center," accessed November 8, 2023.
7. Wiz, "Wiz for cloud security posture management," accessed November 8, 2023, p. 6.
8. Ibid, p. 9.
9. Palo Alto Networks, "Prisma Cloud for cloud security posture management," 2023.

Deloitte.

This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional adviser.

Deloitte shall not be responsible for any loss sustained by any person who relies on this document.

Product names mentioned in this document are the trademarks or registered trademarks of their respective owners and are mentioned for identification purposes only. Deloitte is not responsible for the functionality or technology related to the vendor or other systems or technologies as defined in this document.

As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2024 Deloitte Development LLC. All rights reserved.