International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 6 | Issue 2 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT206268

CSPM- Cloud Security Posture Management (Comprehensive Security for Cloud Environment)

Jyoti Bolannavar
Department of Computer Science, Sri Mariyappa Balappa Kalakonnavar Government First Grade College, Naregal, Dist: Gadag, Karnataka, India

ABSTRACT

As enterprises place more services in public cloud and as the public cloud providers introduce more infrastructure and platform services directly into the hands of developers, it is becoming increasingly complex and time-consuming to answer the seemingly straightforward question "Are we using these services securely?" and "Does the configuration of my cloud services represent excessive risk?" For example, manually assessing the secure setup and configuration in cloud environments across different services, each with varying granularities of authorization policies, is extremely difficult, if not impossible. Simple misconfiguration issues (such as open storage buckets) represent significant risk (see "Open File Shares Are Your Biggest Cloud Security Problem") and occur often, as evidenced by continuing publicized data disclosures from publicly exposed storage buckets.

Keywords : CSPM- Cloud Security posture management, CASB- Cloud Access Security Broker, CWPP- Cloud Workload Protection Platform, API- Application Programming Interface, IaaS- Infrastructure as A Service, PaaS- Platform as A Service, CSP- Cloud Service Provider.

I. INTRODUCTION

The Cloud Security Posture Management (CSPM) previously known as Cloud Infrastructure Security Posture Assessment was defined in response to the growing need of organizations to correctly configure public cloud IaaS and PaaS services and address cloud risks. CSPM is a class of security tools as defined by Gartner include use cases for compliance monitoring, DevOps integration, incident response, risk assessment, and risk visualization.

Definition

CPSM offerings continuously manage cloud risk through the prevention, detection, response and prediction of where excessive cloud infrastructure risk resides based on common frameworks, regulatory requirements and enterprise policies. The core of CSPM offerings proactively and reactively discover and assess risk/trust of cloud services configuration (such as network and storage configuration), and security settings (such as account privileges and encryption). Ideally, if a setting is noncompliant or a configuration represents excessive risk, the CSPM offering can take automated action to adapt, including remediation.

II. Continuous, Life Cycle Approach to Cloud Security Posture Management

As shown in Figure 1, CSPM should be thought of as a continuous process of cloud security posture improvement and adaptation with a goal to reduce the likelihood of a successful attack and the damage in the event an attacker gains access. Since cloud infrastructure is always in flux, the strategy for CSPM

should be one of continuous assessment and improvement throughout the life cycle of cloud applications, beginning in development and extending into production (left to right in Figure 1), responding and adapting where needed. Likewise, since new cloud capabilities and new regulations are continuously being introduced, the best practices for secure cloud usage will also always be in flux. The top part of Figure 1 shows that the CSPM governance strategy should be constantly evolving and adapting to emerging best practices, evolving industry standards and external threat intelligence, as well as adapting to observed risks coming from development and production.

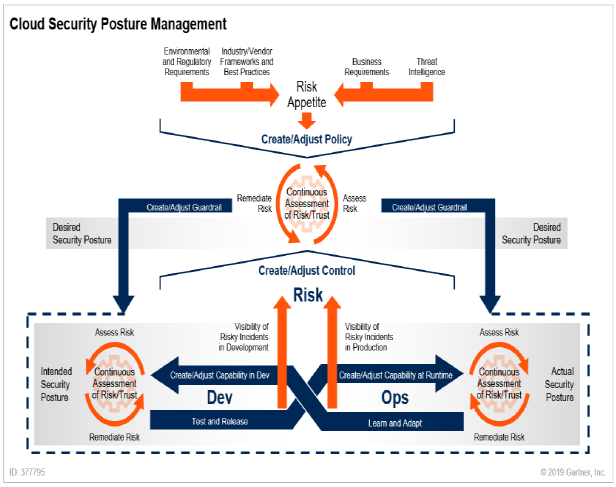

Figure 1. Continuous, Life Cycle Approach to Cloud Security Posture Management

A CARTA approach to CSPM delivers continuous cloud compliance. As shown in Figure 1, we are continuously monitoring for gaps between our desired security policy (driven from our cloud risk and governance processes), the intended security posture (what the developer/DevOps team intended) and the actual security posture observed at runtime. Nearly all successful attacks on cloud services are a result of customer misconfiguration, mismanagement and mistakes. CSPM offerings directly target this need.

The CSPM offerings discussed in this paper help to automate the CSPM process, make it repeatable and allow it to scale with the needs of digital business.

Why is CSPM Important?

Cloud Security Posture Management (CSPM) is defined by Gartner as "a continuous process of cloud security improvement and adaptation to reduce the likelihood of a successful attack." Because public cloud infrastructure is constantly changing, CSPM security tools continuously monitor enterprise cloud environments to identify gaps between their stated security policy and the actual security posture.

At the heart of CSPM is the detection of cloud misconfiguration vulnerabilities that can lead to compliance violations and data breaches. CSPM offerings typically use APIs of the underlying cloud providers to monitor public cloud environments for security or policy violations with the option of remediating the violations to ensure continuous compliance.

Benefits and Uses

CSPM offerings provide continuous monitoring and assessment of compliance and risk across the variety of cloud services an enterprise is using. This is accomplished using the APIs of the underlying cloud platform, avoiding the use of agents.

A. The benefits to security and risk management leaders include:

- Policy visibility and consistent enforcement across multiple cloud providers.
- Continuous discovery and identification of cloud workloads and services.
- Alerting on risky new deployments or changes to the cloud environment, hosts or services.

- Risk assessment versus frameworks and external standards (such as the International Organization for Standardization [ISO] and National Institute of Standards and Technology [NIST]).
- Risk assessment versus technical policies and best practices (such as Center for Internet Security [CIS] and cloud service provider [CSP] best practices).
- Continuous cloud risk management, risk visualization and risk prioritization capabilities.
- Verifying operational activities are being performed as expected (for example, key rotations).
- Continuous visibility into multiple public cloud environments of policy violations
- Optional ability to perform automated remediation of misconfigurations to ensure continuous compliance and protect critical cloud assets
- Leverage of prebuilt compliance libraries of common standards or best practices such as CIS Foundations Benchmarks, SOC 2, PCI, NIST 800-53, or HIPAA to verify that cloud configurations are compliant

The primary purpose of CSPM offerings is to continuously identify and remediate cloud infrastructure risks consistently across all of the cloud IaaS and PaaS platforms in use by an organization.

Assessments cover a hierarchy of security, compliance and risk management needs, including identifying:

- Where cloud configuration and settings violate compliance requirements, and where established account hygiene best practices are not being followed. This includes, for example, ensuring host OS logs are being gathered, API event logging is turned on and network flow logs are being gathered (if applicable).
- Excessive account permissions. Highly empowered accounts, or accounts where permissions are granted but are never used, represent an increased surface area for attack. Developers often provision accounts and services with more permissions than necessary in the name of development speed and to reduce runtime issues, but this increases risk.
- Accounts and services where multifactor or other strong authentication methods are not used. Excessive or misconfigured network connectivity. Public clouds enable micro segmentation by default to enforce the principle of least privilege. Network connectivity should be provisioned to the minimum needed (also referred to as zero trust networking).
- Assets/workloads/services with direct connectivity to the internet.
- SSH/RDP for remote management open to the public internet.
- Data storage exposed directly to the internet.
- Data storage and file shares that are promiscuously shared.
- Data/database storage services that are not kept encrypted at rest/ in transit.
- Improper use of encryption key management.
- Expired keys/certificates, or ones nearing expiration.
- Externally facing web servers without the use of a WAF or load balancer.
- APIs exposed directly to the internet.
- Use of API-based applications and services without the use of an API gateway control point.
- Any areas of infrastructure where the observed runtime state has deviated in a risky way from the desired state. Ideally, you should proactively identify where the intended state of the developer deviates in a risky way from the desired state before being placed into production.

B. CSPM Uses

CSPM offerings typically focus on identifying the following types of policy and security violations

- Lack of encryption on databases or data storage.
- Lack of encryption on application traffic, especially that which involves sensitive data.
- Improper encryption key management such as not rotating keys regularly.
- Overly liberal account permissions.
- No multi-factor authentication enabled on critical system accounts.
- Misconfigured network connectivity, particularly overly permissive access rules or resources directly accessible from the internet.
- Data storage exposed directly to the internet.
- Logging is not turned on to monitor critical activities such as network flows, database access, or privileged user activity.

III. General CSPM Considerations

In the growing market of CSPM providers, each has unique capabilities. The following sections address the business, technical and operational aspects to consider when evaluating a CSPM, and how to evaluate your ability to conduct an investigation.

CSPM Considerations Regardless of the vendor(s) you choose to use for CSPM, you should review a variety of business, technical and operational considerations.

Table1 : Business Considerations

Considerations	Details
Data retention	How long will indexed data from your cloud accounts be stored by the CSPM vendor? Do the retention policies align with your organization's approach? If you discontinue using the vendor, what will happen to your data in their systems? **Evaluate:** • Contract language • How data is anonymized for usage outside your tenant
Licensing	Understand the cost associated with bringing a CSPM to your organization and how the CSPM licenses their platform. **Evaluate:** • Per account monitored • Per resource monitored • Per feature used
Responsibility	Because CSPM is a SaaS platform, administrative overhead should be minimal; however, there is still administrative responsibility on the consumer. **Evaluate:** • Internal knowledge set • Teams that are connected with security efforts

Table 2 : Technical Considerations

Considerations	Details
Account integration	Evaluate how a CSPM authenticates to an organization's existing cloud footprint to determine whether it introduces risk. What changes must be configured within the account for the platform to function? **Evaluate:** • Authentication process for a cloud account • Resources that need to be configured for the CSPM to function
Authentication	Secure access to the CSPM, use authentication standards and ensure access can be easily disabled when a user is no longer authorized to access the CSPM.

	Evaluate: • Federated identity integration • Authentication standards supported (SAML and OpenID, for example)
API	APIs allow for access to functionality and extend CSPMs further by allowing programmatic access to data. **Evaluate:** • Documentation • Access controls specifically for API access, and access keys • Logging

Table 3 : Operational Considerations

Considerations	Details
Functionality monitoring	Understand your CSPM provider's connectivity to your AWS account(s). If the integration fails, it can be detrimental to functionality. **Evaluate:** • If the communication between a platform and account disconnects, how is the security team notified? • Is there any mechanism to pinpoint the failure for troubleshooting?
Custom alerts	CSPM tools come with pre-built alerts. However, your organization may have unique use cases requiring custom alerts. **Evaluate:** • Ease of alert creation • Customization options
	• Severity • - Auto-remediation
Reporting and dashboards	In order to articulate the security posture, executives may require different reports—or your security organization may have to produce proof of attestation. Understanding whether risk is increasing or decreasing can also aid the security team and developers in understanding any risk being removed or introduced from cloud service providers. **Evaluate:** • Report customization and generation • Dashboard customization • Ability to export metrics for more granular analytic tools

IV. LIMITATIONS

CSPM offerings fill an important gap, but there are limitations, such as:

- Visibility. CSPM tools can't assess what they can't see. If your enterprise hasn't yet taken steps to identify and curtail shadow IaaS/PaaS, the value of CSPM will be limited. Specifically, the enterprise should actively discourage and monitor for the personal use of cloud services where information security does not have visibility (for example, developers with personal accounts in AWS or Azure).
- Paying too much. Because of the immaturity of the market, pricing models are highly variable. At the high end, we have seen CPSM contracts priced at $4,000 to $5,000 per account per year. While this might be reasonable for enterprises with a few dozen admin accounts, it is not reasonable when organizations use accounts as an isolation

boundary. For example, we have seen cases where larger enterprises have more than 1,000 accounts in a single cloud IaaS platform. Increasing competition and newer market entrants have dropped pricing closer to $1,000 to $1,500 per account per year with volume discounts bringing this under $1,000.

- The stand-alone market for CSPM is unsustainable. The CSPM market has evolved to address a real and significant need, but it risks being subsumed into adjacent markets. The cloud providers themselves are improving their own capabilities. In terms of third-party alternatives, all leading CASB vendors provide some CSPM capabilities. In addition, some cloud workload protection platform (CWPP) vendors have added CSPM capabilities as well as entry by some vulnerability management vendors. At the same time, the cloud providers are building out their own capabilities for their customers — although for their cloud services only. The CSPM market will not support the current large number of stand-alone CSPM offerings. On a positive note, if your CSPM provider is acquired or goes out of business, switching vendors is relatively easy as they all use the documented APIs of the cloud providers.
- Lack of consistent breadth across cloud platforms. Most CSPM vendors are very good at assessing AWS because that's where the bulk of the enterprise IaaS workloads are. Many have introduced support for Azure. Very few support GCP, and even fewer assess VMware on premises. Most enterprises have a mix of several of these.
- Lack of consistent depth within a cloud platform. Even if AWS is supported by a CSPM provider, does it understand and support the assessment of all cloud services capabilities? The risk is that even with a CSPM tool in use, there are security blind spots that you aren't aware exist, creating a false sense of security.
- Lack of data context. Many CSPM solutions do not understand the context of the data — whether the content is sensitive or malicious — and both are critical to understanding and prioritizing cloud risk.
- Lack of workload vulnerability and configuration context. The control plane around a workload may be perfectly configured, but if the workload itself is missing a critical patch or setting, this is a risk that needs to be addressed. This typically is a requirement filled outside of the CSPM offering by more traditional vulnerability management vendors.
- Being reactive. Many CSPM tools are designed to identify risk and compliance issues after the cloud workload is already deployed, leaving a small window of exposure until the issue can be remediated. Further, even if issues are identified, many enterprises are reluctant to automate responses, increasing exposure. Ideally, the CSPM offering performs scanning pre-deployment, rather than just runtime assessments.
- Limited staff. CSPM offerings identify areas of excessive risk and noncompliance, but who exactly will monitor these alerts? A shortage of skilled cloud security resources risks limiting the usefulness of CSPM. Automated remediation capabilities help, but there will always be cases that require a person to get involved.

V. CONCLUSION

CSPM is a crucial step toward securing an organization's presence in a rapidly changing landscape. Pairing a CSPM with security teams and extending the CSPM for developers to leverage as a feedback loop will enable organizations to begin embedding security into the development process. Keep in mind that when operating in cloud environment, security becomes everyone's responsibility—and CSPMs make this process easier.

VI. REFERENCES

[1]. https://www.fugue.co/cloud-security-posture-management#whyiscspmimportant
[2]. https://pages.awscloud.com/rs/112-TZM-766/images/Whitepaper_AWS-CSPM-Jumpstart.pdf
[3]. https://emtemp.gcom.cloud/ngw/eventassets/en/conferences/sec25/documents/gartner-security-risk-management-summit-us-innovation-insight-2019.pdf

Cite this article as :

Jyoti Bolannavar, "CSPM- Cloud Security Posture Management (Comprehensive Security for Cloud Environment) ", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 2, pp. 251-257, March-April 2020. Available at doi : https://doi.org/10.32628/CSEIT206268
Journal URL : http://ijsrcseit.com/CSEIT206268