BUYERS GUIDE

Cloud Security Posture Management Buyers Guide

How to select the CSPM solution that is right for you

Cloud computing has modernized the way enterprise organizations build, operate, and manage infrastructure and applications. Cloud computing has helped organizations of all sizes to quickly spin up or spin down a resource to fulfill the increased demand for new application workloads. However, when working in a cloud environment, monitoring the security state of multiple workloads while meeting the growing number of compliance requirements can be challenging.

Unfortunately, for those responsible for protecting their organizations' cloud, it has never been more challenging to select the best solution for the job. With hundreds of options on the market and features that sound similar, choosing the right solution is anything but straightforward.

Sonrai Security recommends that a comprehensive and efficient Cloud Security Posture Management (CSPM) solution should include, but not be limited to, these solution areas:

- Continuously audit the cloud for security risks and misconfigurations
- Provide actionable response and auto-remediation
- Achieve consistent security across AWS, Azure, Google, and Kubernetes
- Track and enforce configurations to meet policies
- Continuous visibility of multi-cloud environments to identify cloud misconfiguration vulnerabilities
- Prevent cloud drift

In order to meet the security, compliance, and efficiency required to protect the modern cloud environment, Sonrai Security recommends that these areas be enabled across your cloud environments. Finally, those recommendations need to be combined with identity and data governance to improve security, performance, compliance, and risk.

Sonrai Security's award-winning identity and data governance platform integrates all those elements to secure AWS, Azure, GCP, and Kubernetes. Sonrai Dig's ability to reduce risk and continuously monitor for breaches makes it a true and proven cloud security solution.

According to **Gartner**, nearly all successful attacks on cloud services are the result of customer misconfiguration, mismanagement, and mistakes. In fact, **99 percent of cloud** security issues will be the customer's fault through 2025, according to the research firm. With industry analysts voicing concerns about the public cloud, and thousands of successful breaches clearly exposing the limitations of traditional security in organizations, security and risk management leaders are working fast to find the right cloud security solutions.

Gartner continues its recommendations by suggesting security and risk management leaders **invest in CSPM** processes and tools to avoid misconfigurations that can lead to data leakage or breaches. Although it is a relatively new class of tools, this recommendation comes with a reason - CSPM allows for just what its name implies - the management of cloud security.

However, finding the right solution can be a challenge. With the need for better cloud security comes a plethora of new cloud security solutions all claiming to be "game changers" and all covering different areas of cloud security. The confusion caused by the abundance of choices and the pressure to find the right solution can be overwhelming.

This Cloud Security Posture Management (CSPM) buyers guide was created to help security and risk management professionals by defining the critical elements and areas of cloud protection required to effectively protect an organization against cloud risks.

The cloud migration boom led to a data security crisis, as businesses quickly realized that they needed advanced mechanisms and processes to protect their digital environments and secure their data. With this new class of cloud security tools growing rapidly, we asked, "what exactly is CSPM?"

> " Security and risk management leaders should invest in CSPM processes and tools to avoid misconfigurations ."

Importance of Cloud Security Posture Management

Gartner **defines Cloud Security Posture Management** as "a continuous process of cloud security and improvement and adaptation, which reduces the likelihood of a successful attack." The unique nature of the cloud requires a new security concept that can address the distributed and constantly changing cloud infrastructure and those human and non-human identities within the infrastructure.

CSPM security tools are continuously monitoring enterprise cloud environments to identify gaps between their stated security policy and the actual security posture and mitigate any cloud security risks that might occur. However, it takes more than a collection of capabilities to qualify as a capable CSPM solution. To be truly effective, a CSPM solution must be designed to continuously stop breaches across the entire infrastructure, rather than simply accumulating isolated protection features added each time a new attacker technique is discovered.

The ideal solution should offer a complete package that not only provides more advanced features but also makes innovative use at preventing and remediating issues head-on.

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 environments for security or policy violations with the option of remediating the violations to ensure compliance with policies.

It Can Be Challenging to Secure Your Cloud

The public cloud presents tremendous challenges for security and risk professionals.

With a constantly increasing cloud footprint, DevOps and infrastructure teams are leveraging microservices by using a combination of containers, Kubernetes, and serverless functions, to run their cloud-native applications. This combination leads to a larger number of identities to protect, both in production and across the application lifecycle.

With cloud environments constantly changing due to the rapid-release cycles employed by today's development and DevOps teams, the security and risk management teams struggle to keep up with the changes. Enterprises deploy weekly or even daily, presenting a challenge for security personnel looking to gain control over these deployments without slowing down release velocity.

Architectures are no longer simple. Enterprises are using a wide range of public and private clouds, cloud services, and application architectures. Security teams that are responsible for addressing this entire infrastructure and how any gaps impact visibility and security are struggling to keep up.

Securing identities and their privileges and access to reduce your risk is different than the old world of network security. The old network perimeter, with its limited number of points of ingress secured with firewalls and other perimeter defenses, doesn't work in today's cloud environments. Today cloud identities (human and non-human) are the **new perimeter** with thousands of users and points of potential failure existing outside of your traditional security protocols.

Cloud Security Posture Management Uses

CSPM offerings focus on identifying policy and security violations. When policies are violated, it doesn't necessarily mean that it is a data breach. The severity of the actions will depend on the issue and how quickly it can be remediated. Common policy and security violations identified by CSPM:

- Misconfigured network connectivity, particularly overly permissive access rules or resources directly accessible from the internet.
- Data storage is exposed directly to the internet.
- Logging is not turned on to monitor critical activities such as network flows, database access, or privileged user activity.
- Lack of encryption on databases or data storage or on application traffic and improper encryption key management.
- Lack of adherence to compliance regulations and controls.
- No multi-factor authentication or password enabled on critical system accounts.

Many of the uses for CSPM can help prevent "data breaches" by preventing a cloud storage bucket containing sensitive data from being accidentally exposed to the internet. For example, in recent news, an unsecured AWS S3 bucket accidentally exposed sensitive records from a car manufacturer, Nissan North America. This is just an example of one type of misconfiguration. Others include the lack of encryption on data or overly permissive user permissions or violate access rules.

Cloud Security Posture Management Key Capabilities

CSPM solutions should support the capabilities needed to address these challenges in a consistent way across multiple cloud services. The key focus is on identifying and protecting the components of services delivered through the platform by mapping the cloud controls to required policies. Where there are deviations of these controls, an alert needs to be made to the right team at the right time and the team needs to take immediate action to remediate the issue. CSPM does not, in general, implement the controls, but rather they provide a consistent way to govern the functionality provided by the cloud services to meet these requirements.

Continuously audits the cloud for security risks and misconfigurations

Evaluation Criteria
Frequency and performance impact of updates provided by the vendor — the frequency demonstrates how often the product needs updating to stay efficient

Questions to ask
How often does the product need to be updated to ensure the highest level of protection?

What can the product prevent when offline, if the user opens a file or executable, or performs malicious actions when not connected to the internet?

Provides actionable response and auto-remediation for issues

Evaluation Criteria
List of actions the solution can take

List of existing security orchestration and ticketing systems the product integrates with

Questions to ask
How quickly are triggers deployed once an error occurs?

How does the product integrate with existing tools?

Do alerts provide context to improve overall response?

Can the product generate tickets from an alert to improve response times for remediation?

Achieves consistent security across AWS, Azure, Google, and Kubernetes

Evaluation Criteria
Built for scale to support multiple CSPs and teams across hundreds of cloud accounts, services, and identities

Questions to ask
How do you map directives back to an ever-expanding set of cloud services, especially relative to the set of defined configurations that often result in a violation of policy?

Does your solution protect cloud identities data end-to-end?

How often does your platform need to be updated to be effective?

Does your solution protect against unauthorized access?

Will the solution introduce scale or performance issues?

Track and enforce configurations to meet the policy

Evaluation Criteria
Ensure that authentication and access controls meet policies

Policy-based definition and enforcement over who can access what data, while ensuring compliance standards are met

Track and enforce configurations to meet the policy

Questions to ask
Which major compliance and security frameworks (such as ISO/IEC 27001, NIST, PCI-DSS, GDPR, CCPA etc) are out of the box?

Can you create custom controls?

Can your cloud environment enforce granular access controls to web apps, VMs, APIs, and apps based on a user's identity and context of the request — without the need for a traditional VPN?

Continuous visibility of multi-cloud environments to identify vulnerabilities

Evaluation Criteria
Extensive out-of-the-box reports for PCI-DSS, HIPAA, Web-Architected Framework, GDPR, CIS Benchmarks and for custom compliance requirements

Reports by region, cloud provider service category (such as AWS S3), severity level, etc

Customized alerts for specific types of checks and conditions

Questions to ask
Does your solution provide end-to-end real-time visibility and control?

Does your solution protect against unauthorized access?

Can the product generate tickets from an alert to improve response times for remediation?

Prevent cloud drift

Evaluation Criteria
Detects unmanaged configuration changes to stacks and resources

Assesses cloud network security posture, orchestrates, and visualizes workload across identities, data, and network

Questions to ask
How do you ensure continuous compliance in the dynamic and transient world of the public cloud and do so on a constant and consistent basis?

Can your solution help detect risky shadow IT activity?

Can your solution automatically detect infrastructure drift and automatically remediate drift events for critical resources?

Will the solution introduce scale or performance issues?

Optional ability to perform automated remediation of misconfigurations to ensure continuous compliance and protect critical cloud services

Evaluation Criteria
Select configurations should be automatically fixed if they drift out of policy

Questions to ask
Can your solution automatically detect infrastructure drift and automatically remediate drift events for critical resources?

How do you resolve the drift results?

How do you track down the root cause of an event?

How are alerts generated and prioritized?

History of Cloud Security Posture Management Solutions

Early CSPM solutions enabled businesses to identify their cloud environments, monitor for changes, and leverage policy visibility to ensure consistent enforcement across multiple cloud providers. These early services conducted these activities continuously while providing automation capabilities to correct issues without human intervention or delay. These early platforms scanned cloud instances for misconfigurations and improper settings. They also scanned databases and storage buckets for misconfigurations and provided auditing and reporting for compliance mandates.

Also, the early CSPM solutions provided a report on performance on risk assessments versus frameworks and external standards like the ISO, NIST, GDPR, and more. They were also able to verify that operational activities could be performed as expected while automating processes and remediating issues as needed.

Early CSPM solutions, however, had one major shortcoming: they lacked context.

Context is most often determined by how a piece of computer — like an identity or data point — is invoked. Based on learned function context, your cloud environment can enforce granular access controls to web apps, VMs, APIs, and apps based on a user's identity and context of the request — without the need for a traditional VPN.

Based on the least privilege security model, context-aware access enables your organization to provide simpler access for your users, enforce granular controls, and use a single platform for both your cloud and on-premises applications and infrastructure resources.

Today's CSPM with context include the features of basic CSPMs as listed above, while also:

- Verifying user identity and validating context before allowing access to apps, APIs, and more;
- Reducing complexity and costs by leveraging a unified access management platform and a single set of policies;
- Spending less effort and time to configure and enforce access policies; and
- Adding context to improve your organization's security posture as more workloads move to the cloud.

Today's approach enforces granular access control based on a user's identity and the context of the request. However, they have another shortcoming by excluding non-human identities. This is a major problem when considering the rapid proliferation of non-human identities in the modern enterprise (e.g., bots).

The next step in the evolution of this technology is intelligent CSPM, which includes data and identity governance. This involves using first-generation CSPM tooling with non-human identities and intelligence, including data automation and remediation.

Intelligent CSPM Approach

Many organizations today are still lacking key identity-related security controls. Meanwhile, the few companies that have started applying proper access controls are typically focusing on human users as opposed to non-human users.

Non-human identities are identities that act on behalf of a person. For example, they can be pieces of code, such as AWS Lambda functions, or pieces of compute, such as Azure VMs or other public cloud services.

Regardless of how you define them, they are extremely useful and often represent the vast majority of identities found in cloud deployments. They do, however, present some unique challenges that are only solved with intelligent CSPM.

With intelligent CSPM, organizations can continuously discover and monitor every possible relationship between identities and data that exists across the public cloud. Further, identifying security and compliance issues to help you improve the visibility and control of your cloud.

By uncovering all potential access paths to your data - regardless if by human or non-human identities, and categorized by privilege, your organization can get to and enforce Least Privilege Access. Monitoring for public 'buckets' is important but it's not enough. Your CSPM should extend monitoring to all data, resources, and microservices so you can answer key questions on your data like "Where is it?", "What is it?", "Who has access to it?", "What has accessed it?", "What did they do?", and "Where and why did it move?"

Your CSPM platform should automate the process of assessing your cloud against hundreds of configuration and security best practices identifying critical risks in your environment in human and non-human identities. These checks may include basic policies, like ensuring each account sends its logs to a secure log repository, requiring all admin users to log in with multi-factor authentication, or making sure no administrative identities are open to the public.

With intelligent CSPM, more complicated best practices can be assessed as well, including looking for excessive account permissions, making sure access to storage buckets only comes from authorized identities, or even detecting when an Identity can escalate their privileges based on their Effective Permissions. Running a cloud at scale requires you to quickly and reliably identify when your cloud deviates from security policies, and provide an instant notification within the tools you use to manage Operations, including HashiCorp, Slack, and Jira.

The next step in the evolution of this technology is intelligent CSPM, which includes data and identity governance.

Conclusion

Selecting a Cloud Security Posture Management solution can be challenging, as the cloud security market provides hundreds of options. Each product comes with its own set of features and technologies and the differences often are not easily discernible. To simplify and clarify things, Sonrai Security breaks down the requirements of a comprehensive and efficient SPM solution into these key elements that have been detailed in this guide:

- Continuously audit the cloud for security risk and misconfigurations
- Provide actionable response and auto-remediation
- Achieve consistent security across AWS, Azure, Google, and Kubernetes
- Track and enforce configurations to meet the policy
- Continuous visibility of multi-cloud environments to identify cloud misconfiguration vulnerabilities
- Prevent cloud drift
- Optional ability to perform automated remediation of misconfigurations to ensure continuous compliance and protect critical cloud services

While the idea of configuration drift can seem overwhelming, the good news is that configuration drift can be managed effectively. Any steps taken by a business to monitor system changes will help reduce some of the headaches that drift can cause.

In addition to addressing issues that arise as a result of configuration drift, management can impact other areas of the business as well. Effective drift management can ensure your infrastructure stays compliant, whether from security or regulatory standpoint, and enables proper management of your cloud resources, especially across a multi-cloud environment. Drift management also ensures that the resources in place are being used appropriately and efficiently, giving teams greater capacity to collaborate and coordinate, whether in person or remotely, resulting in a better experience for both internal clients and external stakeholders.

Whether leadership's biggest concern is compliance and risk, or the effect on customer experience, having a solution in place to address configuration drift once it is detected will reduce its overall impact on your company.

Learn More

To learn more about Intelligent CSPM solutions and how you can effectively manage cloud drift and configurations.

See the Platform

Request a demo today.

sonraísecurity.com
info@sonraísecurity.com
646.389.2262