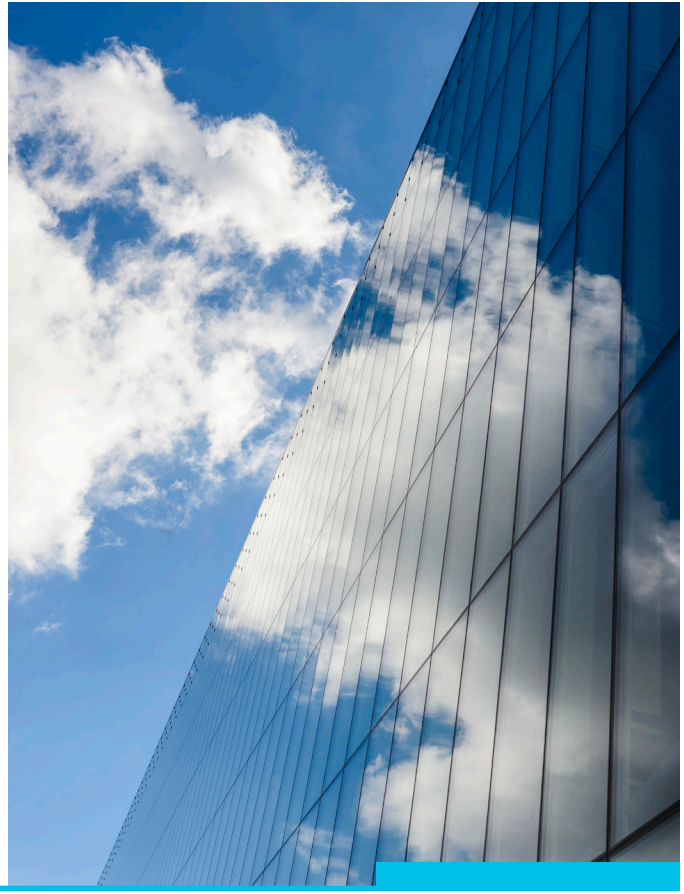
Guide to Cloud Security Posture Management Tools

paloalto NETWORKS | PRISMA BY PALO ALTO NETWORKS



Proper cloud security hygiene starts with complete visibility into the security and compliance posture of every resource you deploy into your cloud. It's one thing to achieve this visibility in a single cloud environment—you can lean heavily on the native monitoring and auditing tools of your cloud provider, using third-party solutions to fill in gaps (e.g., threat detection).

But in a multicloud architecture, maintaining robust cloud security posture becomes exponentially more complex. It's far more difficult to achieve centralized visibility, as well as consistently enforce policies and compliance rules within a multicloud environment. It's also more complicated to detect threats and fix vulnerabilities quickly due to the web of threats across distributed, multilayered architectures. You can address these challenges, though—and you need to—if you want to take advantage of multicloud architecture without compromising your security.

This guide will walk you through the challenges of cloud security posture management (CSPM) within a multicloud architecture. We'll also discuss how to build a CSPM tool set and strategy that effectively address your challenges by providing centralized visibility, compliance management, threat detection, data protection, and automation built for multicloud environments.

The Unique Challenges of Multicloud CSPM

CSPM that works in a single-cloud environment can't simply be scaled up to meet the needs of a multicloud architecture. From a security perspective, multicloud environments differ from single cloud environments.

Disparate, Distributed Data

Data in a multicloud environment is spread across multiple clouds. You can store high-volume data in one cloud to take advantage of lower cost, for example. At the same time, you might keep other data in a cloud that charges more but offers faster access to the data. In another scenario, you might distribute data between different cloud regions to place it closest to end users who will access it.

When data is distributed, ensuring it's secure and malware-free is more challenging. You need to make sure that proper identity and access management (IAM) rules are in place for each datastore on each cloud. You also need to ensure each bucket is properly configured—and "proper" differs across cloud service providers (CSPs).

Distributed Applications

Applications, and the tools that deliver them, also tend to be distributed across multicloud environments. For instance, you may run duplicate instances of the same application in different clouds to ensure it's available if one cloud fails. Perhaps you choose to host a development toolchain in one cloud but deploy from it into another.

Effective CSPM in this context requires an understanding of the security posture of all the individual services and resources that compose the application. It's not enough to monitor each instance of a multicloud application separately. You need to know how the security state of one

instance could impact others. Can instances interact in ways that would allow a breach in one cloud environment to escalate into another, for example? Continuously monitoring application configurations to ensure they don't deviate from the policy guardrails helps protect against these risks.

At the same time, because deploying applications across multiple clouds is complex, it becomes vitally important to integrate security into the application development pipeline, rather than tacking it on as an afterthought. It takes far more effort to address a vulnerability once the application reaches production—and more if the vulnerable code is deployed across multiple environments. By integrating security controls into the application development pipeline, you minimize the need of performing reactive, corrective actions for applications already in production.

Multiple Threat Types and Vulnerabilities

Modern threats come in many forms, ranging from malicious insiders misusing APIs to cryptojacking, data exfiltration, malware inside a container image, SQL injection vulnerabilities, and more. No one type of threat detection can guard against every threat. Malware scanning or configuration auditing won't protect your environments.

You need to analyze threat intelligence from a variety of sources and map the results to known threats. You also need to augment rule-based policies with machine learning-based policies to detect unknown threats.

Multiple Users and Multiple Permissions

Single cloud environments already challenge security teams to enforce good IAM hygiene. Consider the litany of access policies—CSP or user-managed policies and policies for various groups, roles, resources, and access control lists. With numerous policies attached to users, enforcing least-privileged access for a single cloud is difficult.

Multicloud environments compound the single-cloud challenges, as user permissions and entitlements are inconsistently defined across CSPs. You not only need to monitor a different set of IAM configurations for each cloud but also need to correlate user roles and permissions with users' requirements, as defined for each cloud. You can't simply audit for the same set of credentials for the same users on every cloud.

Broader Attack Surface

More clouds mean more accounts, access control policies, services, and so on. All of this adds up to a broad attack surface with more potential opportunities for attackers to take advantage of a misconfigured resource, lax permissions, or a code vulnerability.

At the same time, the lack of centralized visibility and control into a multicloud environment makes vulnerabilities and threats difficult to detect. When you can't monitor and audit all your configurations across all your services using a single CSP's tools, it's difficult to prevent the breach a misconfiguration can lead to.

Mastering Multicloud CSPM: Five Key Features

Addressing the previously mentioned multicloud security challenges requires a CSPM strategy and tool set that provide five key features.

1. Complete Visibility, Compliance, and Governance

Successful CSPM for multiple clouds relies on the ability to continuously monitor and audit all resources across all CSPs. Whenever a new service or workload is deployed or a configuration is changed, your tools must detect and scan the update to ensure it complies with security requirements and best practices.

If the new deployment or configuration doesn't comply, the tools should alert your team that something is wrong and recommend ways to fix it. Your tools should also automate simple fixes (e.g., updating a mistyped IP address, adding a missing statement to an IAM policy), without waiting on security teams to make minor changes.

You want to prevent insecure configurations from reaching production to reduce the number of runtime alerts. Your CSPM tools should be able to scan infrastructure as code (IaC) templates for misconfigurations and enforce policies across the software development lifecycle—not just at runtime.

In addition to a simple list of misconfigured resources, teams need a CSPM tool that helps them understand overexposed cloud networks. By mapping all possible network paths to, from, or across cloud resources, CSPM can assess total internet exposure risks before generating an alert. This provides greater visibility while reducing alert noise.

2. Comprehensive Threat Detection

The complex nature of threats in multicloud environments means CSPM tool sets need to collect threat intelligence from a variety of sources to gain accurate risk clarity. Those sources include IaC configurations, container images, and cloud virtual machine (VM) images.

Many teams already scan for vulnerabilities, but simply scanning these components won't deliver full threat intelligence and detection. For that, your organization needs to maintain high-fidelity threat intelligence so you can identify the latest threats and assess their severity level. The ability to detect anomalies in the network and correlate them with other types of threat data is important for gaining context on the potential impact of threats. You need to do the same with user and entity behavior analytics (UEBA) data.

In other words, modern threat detection requires analysis of multiple data sources, combined with the ability to correlate and contextualize that data. This is integral to identifying threats within complex, multilayered environments, in addition to helping teams understand how to quickly prioritize risk and remediate threats. Only through comprehensive threat detection can you associate network anomalies with an insecure container image, for instance, or determine which account is the source of a breach. When your team can understand threats more quickly, you can fix them more quickly, minimizing your mean time to remediate.

3. Integrated Data Security

Regardless of the type of data you store in the cloud and whether it includes personally identifiable information (PII), keeping it safe requires a multipronged defense that provides deep visibility into the state and status of your data. That starts with the ability to monitor the configuration of each storage bucket across your various storage services to ensure data isn't accidentally exposed to unauthorized users or applications. You also need to audit the contents of buckets to determine whether they contain PII subject to compliance regulations and other requirements.

Detecting malware within data at rest, while critical for cloud data protection, is often overlooked. Malware identification requires scanning storage buckets, as well as databases, VM file systems, container storage volumes, and even short-lived container file systems.

Finally, because cloud data security often requires striking a balance between protection and availability, your CSPM tools should allow you to calculate the exposure risk of data and make recommendations to help limit the impact of a breach. Based on the sensitivity of the data, what level of access control is appropriate for your cloud data? Should you use less granular access policies to simplify management? Tools that can calculate exposure risk will help you answer these and similar questions.

4. Intelligent Identity Security

CSPM tools should go beyond misconfigurations and evaluate the overall identity risk in a cloud environment. Doing so requires the ability to calculate net-effective permissions, which refer to the complete set of permissions granted to an identity or group of identities, regardless of whether the identities are humans or machines. After understanding the overall access within cloud and multicloud environments, security teams can identify overly permissive access and remediate the associated risks.

5. Automated Alert Remediation

Enforcing vital security processes and oversight within multicloud environments is impossible without the help of tools that can automatically monitor for and help remediate security risks. This isn't to say multicloud CSPM should be totally hands-off. Manual intervention will always be necessary to respond to complex security incidents or assess risks too complicated for CSPM tools alone to handle. But routine security monitoring, audits, and remediations should be automated so your team can focus on the big-ticket items.

CSPM tools, in fact, should be able to find attack paths by correlating findings across cloud misconfigurations, vulnerabilities, excessive IAM permissions, and network exposures to identify harmful combinations that allow teams to prioritize and remediate the most potentially harmful risks.

The Limitations of Cloud Vendor Tools

CSPs provide a variety of tools that can address some of the risks described in this guide. Data protection services like Amazon Macie and Google Cloud DLP can assess data vulnerabilities in storage buckets and databases, for instance. Monitoring tools such as Amazon CloudWatch and Microsoft's Azure Monitor can generate alerts for certain types of events that may indicate security risks.

While these tools are useful—and you may want to use them to help build your CSPM tool set—they're subject to two limitations:

- **CSP tools aren't designed as comprehensive CSPM solutions**. They might be able to audit some configuration files or find some PII within certain datastores, but they can't continuously scan container images, detect network anomalies, or automatically remediate threats.
- **CSP tools only work within the CSP's cloud**. That means you only have visibility in one cloud, so you'd have multiple windows of visibility if you're trying to secure a multicloud environment.

Relying on CSPs' tools alone in a multicloud environment requires juggling a long list of disparate tools—a difficult and inefficient task. When you can't correlate data, you can't secure data.

Learn More

Multicloud CSPM requires a comprehensive security platform that can continuously monitor and alert on misconfigurations, vulnerabilities, and threats with high accuracy.

Prisma Cloud by Palo Alto Networks provides the automation and centralized visibility necessary to effectively address multicloud security challenges. By ingesting data from flow logs, configuration logs, and audit logs stored on each of the clouds you run, Prisma Cloud provides a centralized view for security teams to monitor the security and compliance posture of your entire environment.

Because Prisma Cloud provides threat detection based on anomalous activities and impact, it helps your team understand the severity of threats and take appropriate action. Prisma Cloud puts an end to the guessing game. No more time spent trying to prioritize which threats to respond to first. No more trying to identify the root cause of complex security incidents.

By taking advantage of the automated remediation features of Prisma Cloud, your team can quickly resolve many types of security-related misconfigurations while monitoring the status of remediation through a central dashboard.

See the platform in action to learn more about how Prisma Cloud can help your team manage your security posture. Better yet, why not book a meeting to talk with a Palo Alto Networks expert?

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com