



Check Point®
SOFTWARE TECHNOLOGIES LTD

A BUYER'S GUIDE TO CLOUD SECURITY POSTURE MANAGEMENT

SECURE YOUR EVERYTHING™

TOC

Introduction	4
The Top 10 Considerations for Evaluating a Cloud Security Posture Management Solution	5
CloudGuard: Cloud Native Security Posture Management	6
How CloudGuard Extends Cloud Native Security Posture Management	8
How CloudGuard Compares with the Competition	10
Five Questions You Must Ask Cloud Security Posture Management Vendors	11
Conclusion	12

Introduction

According to [Gartner](#), “Through 2025, 99% of cloud security failures will be the customer’s fault.” It is no wonder, therefore, that 68% of the respondents in our [2020 Cloud Security Report](#) cited cloud platform misconfiguration as one of the biggest security threats in public clouds while 42% listed legal and regulatory compliance as one of their biggest cloud security concerns.

Public cloud infrastructure is programmable by design. Within the shared responsibility model, the cloud provider secures the compute-store-network infrastructure resources, but the user, via APIs, is responsible for ensuring that its public cloud accounts are configured securely.

Meanwhile, the growing complexity of the security threat landscape has increased the risk of system compromise. On top of this, companies are under even closer scrutiny by end-users and regulators, who have high expectations that sensitive data is being effectively protected against loss or exposure. In short, maintaining a robust security posture has become a business-critical requirement.

It is against this backdrop that cloud security posture management (CSPM) solutions have taken the stage to help enterprises secure their cloud assets—in a compliant manner—across multiple accounts, multiple clouds, and ephemeral workloads. CSPM platforms leverage cloud-native security tools and services in order to provide dynamic, end-to-end visibility into configuration compliance, automated misconfiguration remediation, proactive threat intelligence and prevention, and insightful security visualizations.

In this Buyer’s Guide, we explain what the key considerations and questions should be when evaluating a cloud security posture management solution.

The Top 10 Considerations for Evaluating a Cloud Security Posture Management Solution



Automated asset discovery

In today's complex multi-cloud hybrid environments, one of the first security posture challenges is ensuring coverage across all assets. An undiscovered asset is a monitoring and compliance blind spot. Your CSPM solution must be able to automatically discover assets across all environments in order to build and maintain a comprehensive real-time inventory. It should also be able to automatically identify high-risk assets, such as those that store or process sensitive data.



Context-aware, enriched asset visualizations

Lack of actionable visualization continues to be one of the biggest cloud security posture challenges. The ability to visualize network architecture and inspect the relationships between asset policies across segments and multi-tier applications is essential for detecting and fixing misconfigurations. Your CSPM solution should be able to build and maintain a real-time topology of all assets connected to your organization's network.



Pre-deployment evaluation of impact on security posture

The trend toward Infrastructure-as-Code is a challenge for cloud security posture management. If there is a misconfiguration or any other kind of vulnerability in an infrastructure-architecture template, it will be inherited by all instances provisioned and deployed via that template. Thus, it is important that your CSPM solution can inspect and assess the security posture impact of IaC repositories, prior to deployment.

4

High-fidelity visibility

There's visibility, and then there's deep, real-time, explorable, and centralized visibility. Your CSPM solution must be able to integrate via APIs with all the environments and entities that comprise your infrastructure architecture. The solution must then aggregate and analyze the various monitoring data streams to deliver true situational awareness, providing real-time insights into every data flow and audit trail.

5

Continuous compliance

There are three compelling trends that have made periodic, sporadic compliance checks obsolete: the DevOps culture of continuous product and feature integration and deployment; the widespread use of ephemeral components such as containers, serverless functions, and microservices; and the highly elastic and dynamic nature of public cloud infrastructure. In order to keep up with the velocity of your business today, your CSPM solution must scan frequently and regularly, as well as be able to initiate on-demand scans.

6

Out-of-the-box support for frameworks and best practices

Organizations must navigate an intricate landscape of government- or industry- mandated compliance frameworks and best practices such as [SOX](#), [PCI DSS](#), [GDPR](#), and [HIPAA](#), to name just a few. To add to the complexity, each cloud provider has its own unique compliance rule sets and processes that must be taken into account. There are also recommended cybersecurity and compliance best practices, such as [CIS Controls™](#) and [CIS Benchmarks™](#). Your CSPM solution should provide out-of-the-box, always-up-to-date support for all compliance frameworks and best practices.

7

Customizable and flexible

Every organization has specific governance challenges that arise from its particular products, processes, and architecture. Not all requirements of a compliance framework or set of best practices are relevant to an organization and those that are relevant may need to be tweaked. Thus, your CSPM solution must be customizable and flexible so that you can tailor its functions to your organization's unique requirements.

8

Rules-based, automated compliance

For effective compliance enforcement and management, your CSPM solution should support the translation of governance requirements into error-free, easy-to-understand rules.

These can then be applied seamlessly and consistently across infrastructures. In addition, the rules and policies should update automatically and dynamically in response to changes in your environment.

9

Intuitive, customizable queries and reports; always audit-ready

Enterprise-grade CSPM enforcement and management deals with numerous, heterogeneous, and very large data streams. Your CSPM solution must allow you to easily

query that data in order to gain meaningful insight into the different aspects of your organization's security posture status. It should also provide a toolbox of out-of-the-box yet customizable reports so that you are always ready for an audit.

10

Proactive protection

The cloud security posture management cycle doesn't end with the passive detection of misconfigurations and other vulnerabilities. Your CSPM solution should be capable of

alerting stakeholders to detected policy violations and intrusions so that they can take protective action in a timely manner. Two other important proactive protection features are the prevention of unauthorized tampering with security policies and automatic remediation of misconfigurations.



" When deploying a multi-cloud environment, you need to have a consistent tool that plays across all the platforms. Using the cloud-agnostic CloudGuard Posture Management service, I only need to train an individual on one set of tools and he can manage our total cloud environment very effectively."

Sreeni Kancharla, CIO & Sr. Group Director, Cadence

CloudGuard: Cloud Native Security Posture Management

[CloudGuard Cloud Security Posture Management](#) is an API-based agentless SaaS cloud- compliance and orchestration platform that is an integral part of [Check Point cloud native CloudGuard security](#), as shown in Figure 1. CloudGuard Posture Management automates governance across multi-cloud assets and services including the visualization and assessment of your security posture, detection of misconfigurations, and enforcement of security best practices and compliance frameworks.

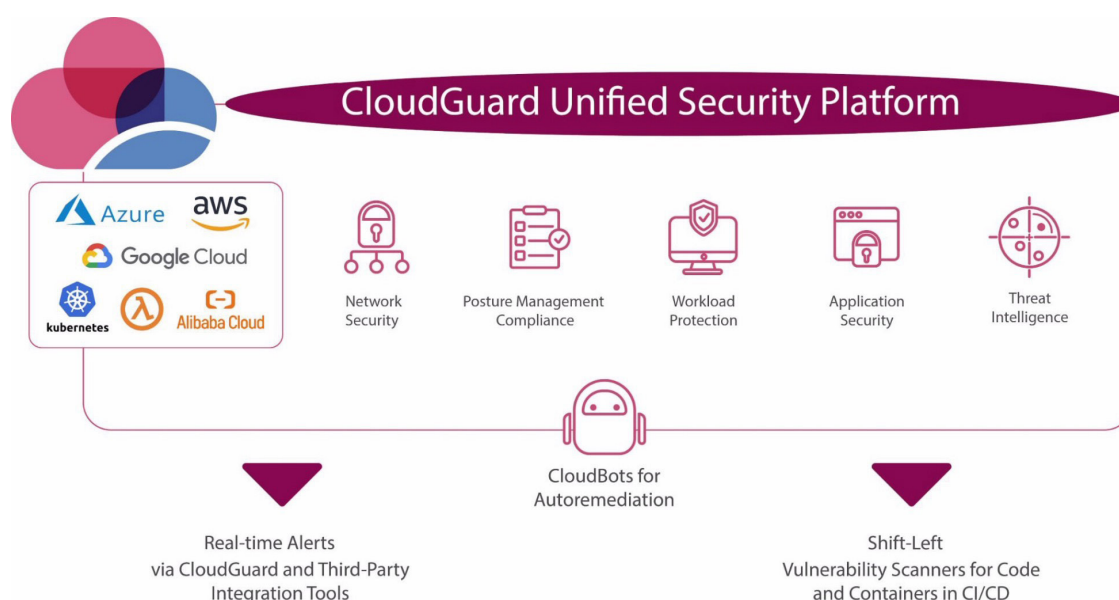


Figure 1: Check Point Cloud Native Security architecture

The capabilities of CloudGuard Posture Management include:

Automated asset discovery and enriched visualizations. The CloudGuard Posture Management Configuration Explorer automatically discovers cloud assets and adds context to the diverse streams of log data. Assets are graphically visualized by levels of exposure, and administrators can easily zoom in and inspect asset configurations.

Pre-deployment assessment. CloudGuard Posture Management can provide an initial security posture score for an environment prior to deployment by investigating deployment and other Infrastructure-as-Code templates. In addition, CloudGuard instantly shows the security posture impact of asset policy changes before they are deployed into the customer's environment.

High-fidelity visibility. CloudGuard Posture Management provides high-fidelity visibility into an organization's security posture with support for 225+ API calls and virtually no delay between asset discovery and the onset of traffic and security information. CloudGuard Posture Management integrates natively with Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), Alibaba Cloud, and Kubernetes clusters for centralized compliance visibility and consistent policy enforcement across hybrid and multi-cloud environments.

Continuous compliance. CloudGuard Posture Management conducts full compliance scans across an entire environment once an hour, delivering near real-time discovery of vulnerabilities, compromised workloads, open ports, or misconfigurations. In addition, compliance scans can be initiated manually, or on-demand.

Built-in, but customizable support for frameworks and best practices. The CloudGuard Posture Management compliance engine supports more than 50 frameworks, including HIPAA, CIS Benchmarks, NIST CSF/800-53, and PCI DSS, and conducts 2,400+ best practice checks out of the box. Compliance rules are easily customized using a simple human-readable syntax and a building-block methodology that require no programming skills.

Rules-based compliance management. CloudGuard Posture Management makes it easy to translate governance requirements into policies that are error-free and easy to understand. The rules are created in the simple and expressive Governance Specification Language (GSL) using an intuitive building-block methodology. Rules that would require 100+ lines of code in cloud-native tools are written in under 100 characters. The policies can then be applied seamlessly and consistently across all environments.

Flexible queries and reports. CloudGuard Posture Management supports out-of-the-box security posture queries, as well as an intuitive query builder for specialized data interrogation. Plus, reports are kept up-to-date automatically for management and auditing purposes. In fact, audit efforts that typically take several hours are often reduced to minutes.

Proactive protection. With CloudGuard Posture Management, it is easy to find compliance issues, fix them, and make sure they stay fixed. CloudGuard Posture Management does not just passively monitor the organization's security posture. It provides enriched vulnerability findings that reduce risk by better identifying, prioritizing, and auto-remediating. It enforces compliance and provides proactive protection against attacks by, for example, employing timed privilege authorizations, region locking, and blocking the reversal of security policy configurations.

"Speed is a key benefit in secure DevOps, but teams often think that there's a tradeoff between speed and security. That's not always the case. With CloudGuard Posture Management's Dynamic Access Leases, we were able to provide just-in-time access for our DevOps teams to allow for rapid yet secure access which was a major enabler for our IT operations."

Robert Berger, CTO & SVP Engineering, Omnyway

How CloudGuard Extends Cloud Native Security Posture Management

CloudGuard integrates seamlessly with the leading CSPs to extend their cloud-native security posture management services.

The key AWS and Azure compliance management and threat detection services are:



	COMPLIANCE MANAGEMENT	THREAT DETECTION
	<p>AWS Security Hub: Collects security data (AWS, 3rd party); runs CIS compliance checks; displays security issues, failed compliance checks, limited set of managed insights.</p> <p>AWS Config: Rules for compliance checks; customization is a complex process.</p>	<p>Amazon GuardDuty: Monitors and analyzes events across AWS logs, including AWS CloudTrail; identifies, prioritizes potential threats.</p> <p>Amazon Macie: Automatically discovers, classifies, and protects sensitive data stored in Amazon S3 object storage.</p>
	<p>Azure Security Center: Assesses security posture against generic best practices and limited set of regulatory frameworks; generates recommendations, priorities; complex process to customize rules & initiatives.</p>	<p>Azure Sentinel: AI-powered SIEM solution that detects and stops threats; built-in orchestration and automation.</p>

Table 1: AWS/Azure compliance management & threat detection services



Table 2, below, summarizes how CloudGuard Posture Management extends the capabilities of these cloud-native services in order to deliver enterprise-grade automated compliance management with a wide range of out-of-the-box, but highly customizable rules, policies, and queries. CloudGuard also provides powerful visualizations and advanced proactive protection.

Automated Compliance Management	Built-in support for a complete range of compliance frameworks and best practices
	More frequent scanning, at a near real-time cadence, with discovered assets included instantly in the scan coverage
	On-demand scans, at any time
Intuitive Query & Policy Customization	<p>Easy rule creation using the simple and expressive Governance Specification Language (GSL) and an intuitive building-block methodology. For example, the syntax for a rule to check if servers are accessible from the internet would be expressed as follows in GSL (versus 100+ lines of code in a cloud-native tool):</p> <pre>Instance where isPublic=true should not have inboundRules contain [scope isPublic()]</pre>
Actionable Visualizations	<p>Intelligent visibility and clear situational awareness of cloud security, including:</p> <ul style="list-style-type: none"> • Auto-classification of protected assets based on level of exposure • Real-time topology of assets and interrelationships between asset policies • Visualization of traffic flow and dropped traffic, as well as user actions and attributions across accounts • Graphical views of infrastructure-architecture templates
Advanced Proactive Protection	<p>The industry's most complete and proactive threat-prevention solution, featuring:</p> <ul style="list-style-type: none"> • Global coverage (versus region-based protection) • Real-time anomaly detection and intrusion alerts • Tamper protection for asset configurations • Granular IAM control, just-in-time privilege elevation • Region lock of egress rules for newly detected assets • Automated remediation with Cloud Bots • High-quality, actionable forensics based on context-enriched traffic

How CloudGuard Compares with the Competition

Table 3 compares CloudGuard and the cloud security posture management solutions of leading cloud security vendors:

KEY CONSIDERATIONS	CLOUDGUARD	CLOUD SECURITY VENDOR COMPETITORS
Asset Coverage and Discovery	Covers the full range of asset types (compute instances, load balancers, serverless, etc.), with automated discovery across multi-cloud/hybrid environments	Often does not cover all asset types across all environments, and discovery is not automated. These gaps can create dangerous blind spots
Visualizations	Context-enriched graphic visualizations of assets and their levels of exposure, with easy inspection of asset configurations	Partial and limited visualizations, based primarily on traffic logs, with minimal or no context across diverse data sources
High-Fidelity Visibility	API integrations with cloud-native and 3rd party tools; immediate onset of information flow; single source of compliance authority	Partial and limited integrations with the organization's existing SIEM and collaboration stack, with no single-pane visibility
Continuous Compliance	Full compliance scans across the entire environment in near real-time, plus on-demand scans	Compliance events and issues are reported after long delays (in the best case, several hours)
Frameworks / Best Practices Support	Built-in support for 36 compliance and best practice standards, with easy customization interface	Out-of-the-box support for far fewer frameworks; compliance-rule customization is highly complex
Rules-Based Compliance Management and Auto-Remediation	1500+ easily customizable compliance rules that are enforced automatically; auto-remediation of detected misconfigurations	Fewer built-in rules that are difficult to customize; primarily manual enforcement and remediation (tedious and error-prone)
Proactive Protection	Real-time detection and alerts of prioritized vulnerabilities, with advanced threat intelligence and analytics to minimize or prevent attacks	None of the leading vendors provide robust, proactive protection against misconfigurations or active threats

5

Five Questions You Must Ask Cloud Security Posture Management Vendors

Q1 How do you enforce compliance and governance?

Staying ahead of the compliance curve across complex infrastructures requires advanced compliance and governance management capabilities that are as automated as possible. Make sure that it is easy and intuitive to create and deploy policies and rules that are environment-agnostic. It's also important that policies and rules update automatically in response to detected changes in the environment. You need to be sure that the compliance-scan cadence is frequent and that you will be alerted immediately to policy violations and misconfigurations. Even better, the platform should also be able to carry out pre-approved, automated remediation.

Q2 What visualizations do you offer and how actionable are they?

The ability to visualize the network architecture topology and inspect the interrelationships between asset policies across segments and multi-tier applications is essential for detecting and fixing misconfigurations. How effectively does the product visualize the security posture of the organization's entire cloud environment? How well does it track and display traffic flow, dropped traffic, user actions, and attributions across accounts? Can you graphically inspect infrastructure-architecture templates so that their impact on your security posture can be assessed prior to deployment?

Q3 How many frameworks/best practices do you support out of the box?

You cannot take for granted the number of compliance frameworks and best practices that your solution will need to support. Make sure that your needs are covered, and verify that the vendor takes responsibility for ensuring that the frameworks and best practices that it does support are always up-to-date.

Q4 How can we adapt your platform to our unique cloud security posture needs?

The platform must be easily customizable so that it can meet your unique and dynamic security posture needs today and well into the future. This flexibility should apply to all layers, including rules, visualizations, queries, and reports.

Q5 How do you proactively protect our cloud environment?

First, you must ensure that the platform itself provides protection against unauthorized changes to security rules and their deployment. The last thing you want is accidental or intentional security posture lapses. Second, you must clarify what the solution does after it detects a security posture violation. Can it leverage external threat intelligence in order to contextually assess the risk level of the vulnerability? Can it trigger immediate remediation steps to block an exploit before it can do harm? In short, make sure that the solution does not deliver just threat detection, but rather, true threat prevention.

Conclusion

We hope that you have found this Buyer's Guide useful as you consider which cloud security posture management solution is optimal for your organization. Empower your cloud security team with an enterprise-grade platform that provides real-time and actionable visibility into the security posture of all your cloud assets across your multi-cloud infrastructure. Make sure that your cloud security posture management framework is flexible, agile, and dynamic so that you can conduct business at scale and speed without sacrificing security.

[Contact Check Point for more information](#) or to discuss your cloud security posture management needs with a cloud security engineer, or [schedule a demo](#) of CloudGuard to understand the best and easiest way to protect your cloud assets.

Worldwide Headquarters

5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters

959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com