Guide

Cloud Security Posture Management (CSPM): Everything You Need to Know in 5 Pages

uptycs

Table of Contents

What is CSPM?

As more organizations shift their workloads to the cloud, securing these environments becomes critical. Cloud misconfigurations, such as exposed storage buckets or improper access controls, have become a significant source of vulnerabilities, increasing the risk of data breaches.

Key to controlling these digital threats is a proper CSPM (Cloud Security Posture Management). CSPM solutions identify vulnerabilities and provide actionable insights to strengthen overall cloud configurations. They leverage behavioral baselines and advanced analytics to prevent potential risks before they escalate.

In this guide, we'll explore more deeply what CSPM is, its key capabilities, and its role in protecting cloud infrastructures from common misconfigurations. Whether you're looking to understand CSPM's meaning, its role in cloud security, or how it compares to other tools like CNAPP, we want to equip you with the knowledge to enhance your cloud security posture and prevent common pitfalls.

You'll also learn how Uptycs takes CSPM a step further by providing real-time discovery and inventory mapping for all cloud assets. This includes assessing threat boundaries, networking and IAM relationships, and correlating security findings across hybrid and multi-cloud environments.

01 Gartner's CSPM Meaning

As organizations increasingly adopt cloud infrastructure, Gartner highlights the need for Cloud Security Posture Management (CSPM) to address configuration vulnerabilities.

CSPM tools are designed to automatically detect misconfigurations, compliance violations, and other security risks across IaaS, PaaS, and SaaS environments. These tools also provide real-time asset inventory management to ensure continuous monitoring of all cloud resources and dependencies. By providing continuous visibility and monitoring, CSPM ensures that cloud resources align with best practices and regulatory standards, significantly reducing the risk of breaches.

As Gartner rightly says, this proactive approach helps organizations maintain a secure and compliant cloud environment as it scales and evolves. With increasing complexity in hybrid and multi-cloud environments, Gartner emphasizes the role of CSPM in maintaining a consistent security baseline.

02 Cloud Misconfigurations: The Weak Link, and an Invitation to Ransomware

CSPMs are so critical right now because of the rising threat of ransomware, and related malicious phenomena.

The global cost of ransomware is projected to reach $10.5 trillion annually by 2025, an increase from $6 trillion in 2021. These costs are due to lost data, downtime, and ransom payments. The level of sophistication and lucrative operation of ransomware cybercrime is compounding at a rate that's never been seen before - and even more exponentially amidst the chaos of the COVID-19 pandemic and its disorienting effect on the healthcare industry.

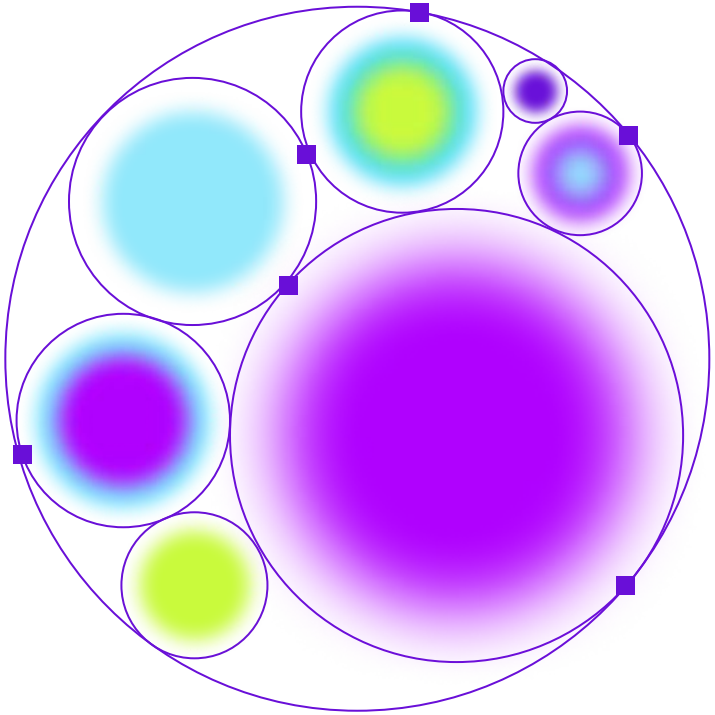
As of 2023, ransomware continues to be a major threat in the healthcare sector. Over 141 hospitals were directly impacted by ransomware attacks this year, underscoring how cybercriminals increasingly target critical healthcare systems. These attacks not only disrupt essential services but can also compromise sensitive patient data. Additionally, the FBI reported that cybercrime losses, driven in part by ransomware, reached a staggering $12.5 billion.

> "Pharmaceuticals, hospitals, healthcare, public companies, organizations that don't have the talent and skills to defend themselves - they're getting sucker-punched."
>
> **Kevin Mandia**

As organizations continue to transition into the cloud to scale operations and enable remote work, improper cloud configurations have emerged as one of the biggest global threats to business security. Misconfigurations are often overlooked because of the dynamic and distributed nature of cloud environments, where visibility gaps and human errors are common. These misconfigurations create vulnerabilities that cybercriminals, including ransomware operators, are quick to exploit.

Addressing these weaknesses through proper configuration is critical to avoiding data breaches and other major security incidents.

With Uptycs, misconfigurations don't remain hidden. Our CSPM platform proactively scans Infrastructure as Code (IaC) templates, such as Terraform and CloudFormation, to identify misconfigurations early in the development lifecycle. This ensures a secure foundation before deployment, reducing the risk of exploitable gaps.



03 How Cloud Security Posture Management Can Help

CSPMs are so critical right now because of the rising threat of ransomware, and related malicious phenomena.

Cloud Security Posture Management targets failures at their root, focalizing an organization's cloud configuration. Previously known as Cloud Infrastructure Security Posture Assessment, CSPM was defined in response to the growing need of organizations to correctly configure public cloud Iaas, PaaS services and remediate cloud risk.

CSPM uses automation to identify and remediate vulnerabilities within cloud infrastructures, and is known for its risk visualization and assessment, incident response, compliance monitoring, and DevOps integration enablement. CSPM tools also leverage anomaly detection by establishing baselines for expected system behavior and flagging deviations. Notably, CSPM is able to uniformly apply best practices for cloud security against hybrid, multi-cloud, and container environments.

With the dynamic nature of cloud environments, number of connected resources, and API driven approaches to integration, misconfigurations can easily be made. Cloud-based services include many moving parts, and when compounded with the lack of active observability lessen an organization's ability to discover and address configuration gaps.

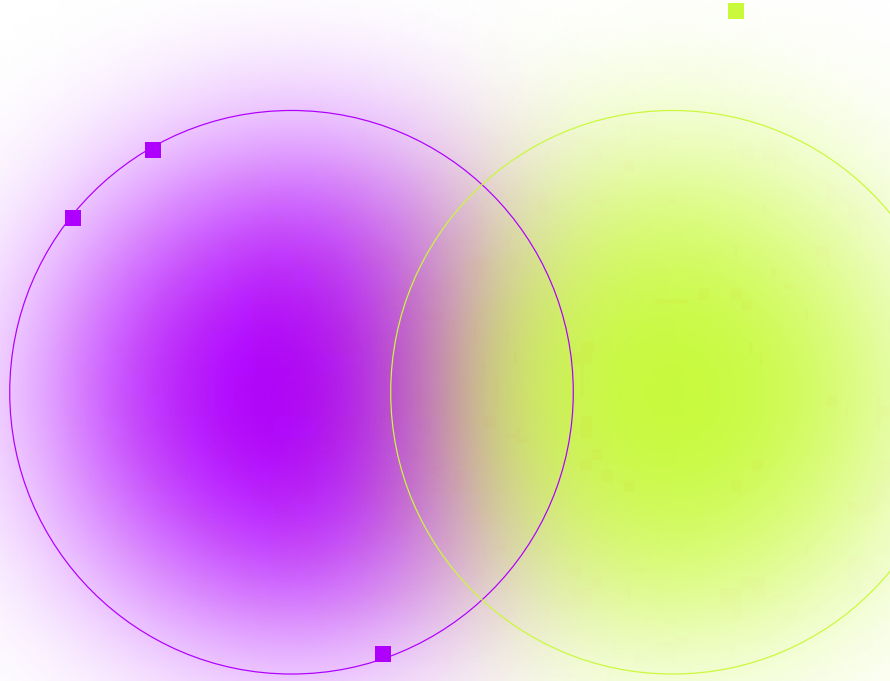
Accidentally granting public access to storage buckets or containers within the cloud that are otherwise assigned individually to storage classes is a common misconfiguration with considerable risk. Like an unlocked house, storage buckets that are left open are susceptible to attack by anyone who discovers them.

Effective CSPM platforms ensure encryption, version control, and access policy enforcement for cloud storage resources to mitigate these risks. The Uptycs platform not only automates detection and remediation but also uses advanced contextual risk prioritization. By correlating vulnerabilities, misconfigurations, runtime behavior, sensitive data, and identity risks, Uptycs pinpoints the most critical issues and highlights potential attack paths to key assets.

GREENLIGHT

"Uptycs contextualizes threat activity across K8s, cloud services, and laptops. We've dramatically shortened our threat investigation time."

Anwar Reddick
Director of Information
Security Greenlight Financial



04 The Key CSPM Capabilities – Basic and Advanced

CSPMs are so critical right now because of the rising threat of ransomware, and related malicious phenomena.

Automated detection and remediation: CSPM tools quickly identify misconfigurations and remediate security issues in real time.

Best practices inventory: CSPM maintains an inventory of best practices tailored to different cloud configurations, ensuring uniform security.

Configuration status mapping: This links cloud configurations to a security control framework or regulatory standard, streamlining compliance efforts.

Storage bucket monitoring: CSPM monitors cloud storage, ensuring encryption and access permissions are properly configured to reduce compliance risks.

Behavioral anomaly detection: CSPM uses machine learning to establish baselines for expected user and system behavior, identifying threats through deviations.

Cloud change monitoring: Track and report changes in public cloud environments in real-time, ensuring operational consistency across regions and accounts.

The above is table stakes. Ideally, you also want:

Cloud-Native Response and Threat Hunting: You want to go beyond posture management, offering threat detection and response capabilities, including forensics and blast radius analysis across workloads, Kubernetes, and cloud services.

Identity and Network Exposure Analysis: You need to detect internet exposure risks and potential lateral movements through a dynamic exposure scanner and identity risk engine, gaining insights into security gaps before they can be exploited.

Compliance Monitoring and Reporting: You want support for standards like SOC2, HIPAA, and PCI. A tool like Uptycs provides tailored compliance checks across environments. Automated reports ensure that organizations can meet regulatory requirements with ease.

With the scope of an organization's due diligence advancing and complexifying with every new cybercrime event, having a strong offensive stance that can detect and respond at the tempo necessary is a task that only Cloud Security Posture Management has proven to deliver.

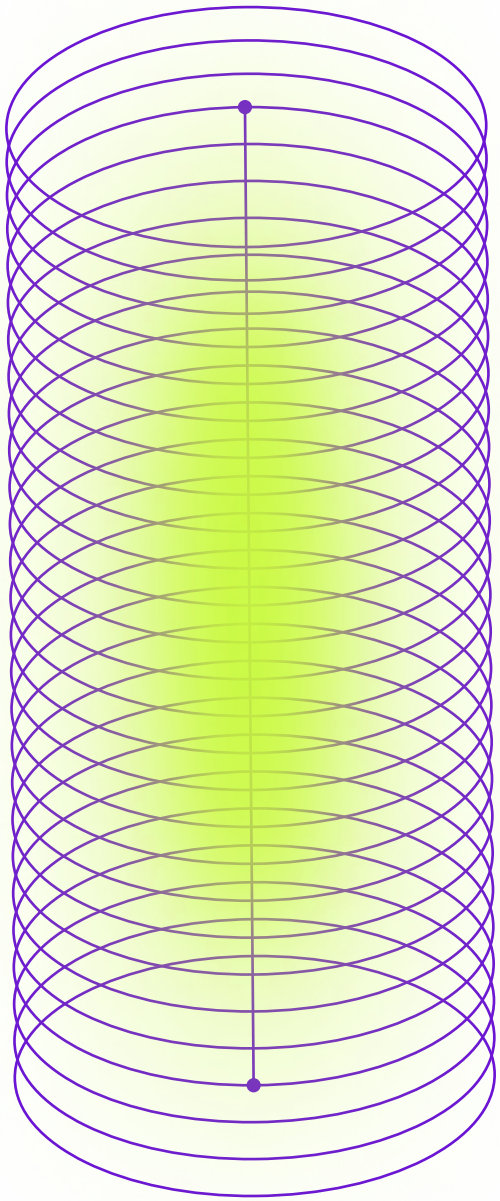
05 Strengthening Your Cloud Security Posture with Uptycs

When it comes to Cloud Security Posture Management (CSPM), Uptycs offers a unified platform that simplifies cloud security for hybrid, multi-cloud, and container environments.

- **Enhanced Visibility:** Gain real-time insights into cloud assets, map network topology, and uncover shadow communications to identify access and network relationship risks.
- **Automated Detection and Remediation:** Quickly identify and fix misconfigurations and vulnerabilities with extensible rules, Infrastructure as Code (IaC) scanning, and runtime monitoring.
- **Advanced Risk Prioritization:** Correlate vulnerabilities, misconfigurations, sensitive data, and runtime behavior to focus on the most critical issues.
- **Attack Path Analysis:** Identify hidden connections and potential attack vectors with actionable insights to protect high-value assets.

- **Identity and Network Exposure Detection:** Detect internet exposure and lateral movement risks using Uptycs' dynamic exposure scanner and identity risk engine.
- **Cloud-Native Threat Response:** Go beyond posture management with runtime threat detection, forensics, and blast radius analysis for a proactive defense.
- **Simplified Compliance:** Align with standards like SOC2, GDPR, and CIS through automated, customizable reporting across cloud environments.
- **Seamless Integration:** Add CSPM capabilities without disrupting workflows, ensuring compatibility with your existing tech stack.

By combining workload protection, security posture management, and threat detection into one unified platform, we deliver a holistic approach to cloud security, empowering your team to respond quickly and confidently to emerging threats.



Uptycs is dedicated to leading security innovations in hybrid cloud environments, ensuring robust protection and enabling our customers to innovate safely and efficiently. Included in the 2024 CNAPP Market Guide, Uptycs provides comprehensive security solutions that bridge the gap from code to cloud. Our platform excels in Cloud Workload Protection (CWPP), Vulnerability Management, Cloud Security Posture Management (CSPM), Detection & Response, Software Pipeline Security, XDR, and Risk & Compliance. Trusted by leading enterprises like PayPal and Comcast, Uptycs transforms potential vulnerabilities into fortified security, ensuring your digital environments are safeguarded from development through runtime.

Secure Everything from Dev to Runtime

Learn more at Uptycs.com