sysdig

CHECKLIST

5 Essential Capabilities for a Modern CSPM Solution

Checklist: 5 Essential Capabilities for a Modern CSPM Solution

Cloud is helping you drive innovation and develop new applications and revenue streams for your organization. However, migration to the cloud introduces security and compliance challenges. These include software vulnerabilities, overly-permissive user permissions, and potential cloud misconfigurations that can be actively exploited by attackers. On top of this, these issues can lead to hefty penalties from regulatory bodies if your organization was impacted by a security breach.

Today, there are a variety of cloud security posture management (CSPM) solutions trying to tackle the challenges stated above. Organizations of all sizes need posture management solutions capable of addressing their cloud security and compliance requirements. However, conventional CSPM solutions are struggling to keep pace with the ever-evolving security landscape.

Mind the Visibility Gap – Static Checks are Not Enough

Conventional CSPM solutions scan your cloud environment periodically, usually every few hours. This provides a point-in-time static assessment of the security posture and risks in your environment. This is fine, if you only care about periodic security and compliance audits. But the visibility gaps left between static checks opens wide huge opportunities for attackers to exploit weaknesses and go unnoticed.

Static checks are not enough given how fast cloud attacks move. Sysdig's "2023 Cloud Threat Report" found that opportunistic attacks average under two minutes to find a publicly exposed credential and 21 minutes from credential discovery to attack initiation.

Conventional CSPM that only correlates static findings of misconfigurations, network exposures, exposed secrets, vulnerabilities, or overly-permissive identities lack real-time awareness and tend to generate a lot of noise making static risks hard to prioritize.

Runtime Insights Highlight Active Cloud Risk

A modern strategy for CSPM solutions goes beyond static checks and is able to detect real-time activities and configuration changes to highlight active cloud risk. These solutions deliver runtime insights that provide actionable data, enabling the identification of high-impact issues that are happening right NOW in your cloud environments by drawing from real-time operational information.

Runtime insights from real-time detections and in-use analysis offer the most valuable insights on active cloud risk and what should be prioritized. For example, they can uncover risk identity behaviors, real-time configuration changes, in-use permissions, in-use packages with critical vulnerabilities, and workload threats. They bring static security controls to life with up-to-date information about what is in use or being exploited, compared to a static snapshot, allowing security teams to effectively address prevention and defense use cases with greater confidence and a proactive mindset.

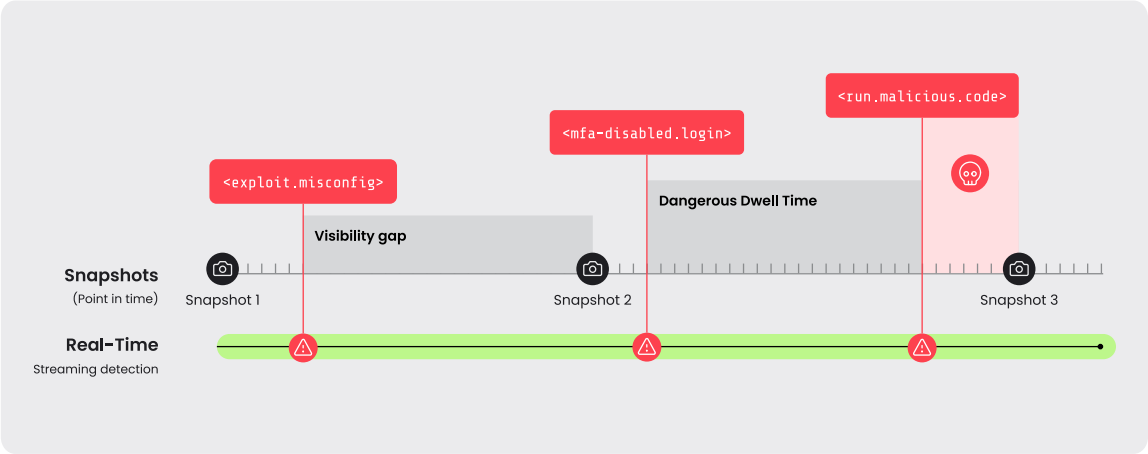

Figure 1: Real-time Active Cloud Risk Detection vs. Snapshots

Runtime insights increase visibility for deployed applications and systems as opposed to relying solely on periodic scanning, where most traditional CSPM fall short. CSPM solutions that use a hybrid deployment approach, with both agentless and agent-based instrumentation, deliver the best of both worlds – ease of deployment and maintenance, and ability to detect and combat active cloud risk.

What are the key attributes that your CSPM solution must have to continuously assess risk, implement robust mitigation strategies, and seamlessly scale your enterprise cloud security approach?

01

Detect and Prioritize Active Cloud Risk

As discussed above, it is important for your CSPM to be able to detect and prioritize active cloud risk. But the question you may be asking yourself is how? Your CSPM solution should be able to agentlessly detect configuration changes and anomalous activity in your cloud environment via cloud and SaaS audit logs in near real time. This goes beyond log parsing and processing, and requires log streaming to deliver the speed required for detection. In addition, you want the option to add agent instrumentation to gain further real-time visibility into workload threats and risks.

Your CSPM solution should detect active cloud risk, including real-time activities and dynamic changes in your environment, such as:

- Risky identity behavior (e.g., user actively logging in with no-MFA)
- Real-time configuration changes (e.g., connect to known malicious network)
- In-use permissions (e.g., high-privilege access activated with no prior use)
- In-use packages with critical vulnerabilities (e.g., actively running software package with high CVSS vulnerabilities)
- Workload threats (e.g., public encryption key uploaded)

More importantly, your CSPM should use runtime insights to enrich static risk findings and overlay active risk information to help you prioritize, investigate, and remediate complex issues and interconnected risks. The riskiest combinations of static and active risks are stack ranked and prioritized to the top. From there, you can drill down and visualize the interconnected risks (both static and active) using attack path analysis to speed your investigation. And within the same workflow, we provide guided remediation to help you fix the issue fast.

02

Keep a Live Inventory Database

With rapid innovation and development moving to the cloud, misconfigurations are bound to happen. Misconfigurations are commonly targeted and exploited by attackers. As new cloud applications are spun up and spun down, it's hard for security teams to keep tabs on what is actually active in their cloud environment at any given time. Having an inventory of cloud assets with corresponding security posture is the best way to keep organizations safe from unwanted configuration changes.

Choose CSPM solutions with an inventory database that allows users to search for compromised resources across a multiple asset categories and security domains (e.g., "Find all storage buckets with read access, publicly exposed to the internet, and violate PCI standard") to quickly check for exposure to high-severity misconfigurations, compliance violations, and vulnerabilities.

An effective CSPM tool will provide an inventory of all cloud assets by:

- Identifying the systems, applications, services, and workloads running in your cloud environment. Determine if they are secure and compliant.
- Mapping cloud assets, including accounts, virtual private clouds, regions, storage buckets, relational database services, etc., to their corresponding infrastructure-as-code (IaC) manifest.
- Consolidating and normalizing assets across cloud providers and services into easy-to-understand categories, like complete, storage, and network.
- Understanding where your sensitive data (e.g., customer data, data governed by compliance regulations) is stored and processed.
- Including metadata, configuration information, compliance violations, drift analysis (IaC vs. runtime), vulnerabilities, threat events, and resource history.

This helps establish a baseline for your current operating state, while context from runtime insights provides up-to-date, real-time information about every asset, enabling security teams to prioritize assets with the most critical risks and expedite remediation.

03

Secure the Infrastructure as Code

Hardening infrastructure that powers applications and services is fundamental to all security teams. Unneeded cloud services and known weak configurations should be disabled from the start, ideally using IaC and policy-as-code approaches. Continuously validating configurations will help ensure that an old misconfiguration doesn't creep back into the environment.

Detecting misconfigurations in production means that you may have already been exposed by cybercriminals. Enterprises need to apply preventive measures, such as securing IaC artifacts. By scanning IaC for security misconfigurations, you proactively address issues before they roll into production. Any organization looking to secure its IaC should consider these guidelines:

- → Integrate into DevOps pipelines, with build integration and rapid analysis of IaC artifacts and files.
- → Allow simple and flexible policy creation for configuration settings and misconfiguration remediation across all resources, with both runtime remediation and IaC remediation capabilities.
- → Use security policies consistently, with enforcement in IaC and runtime environments.
- → Look for solutions that generate IaC remediation code in common formats such as AWS CloudFormation, Terraform, or YAML.

Runtime insights take IaC security to the next level. When a CSPM tool is able to map IaC artifacts to what's actually running in the cloud environment, your teams can understand what has to be remediated earlier in the software life cycle, creating a virtuous cycle between prevention and detection security methods.

04

Address a Changing Regulatory Landscape

Regulatory compliance can no longer be centered around annual or quarterly audits. To address the ongoing surge of cyberattacks and the speed at which they move, new regulations from the SEC, as well as NIS2 and DORA in Europe, are implementing stricter controls with very aggressive requirements around time to disclosure to regulatory authorities in the case of a security event, privacy event, or breach. In the case of DORA, you only have four hours from the moment of classification of the incident as major to disclose, and with NIS2 and the SEC, you have 24 hours. This requires runtime insights to provide real-time visibility into any security event and address these disclosure requirements in a timely manner.

To effectively enforce governance and compliance controls across a multi-cloud environment, a CSPM tool must enable governance, regulatory, and compliance (GRC) and security teams collaborate by:

- Continuous assessment for active cloud risk and incident detection to address strict time to disclosure requirements, typically within hours.
- Automating and enforcing compliance controls with automated remediation across multiple cloud providers by mapping misconfigurations in production to IaC artifacts.
- Provide out-of-the-box policies and compliance checks for common regulatory frameworks e.g., PCI-DSS, GDPR, NIST 800-53, and ISO 27001) across containers, Kubernetes, and cloud environments.
- Implementing file integrity monitoring to detect tampering of critical system files, directories, and unauthorized changes.
- Showing proof of cloud and container compliance using cloud audit logs and container forensics data.

05

Enforce Least Privilege Access

The majority of cloud misconfigurations are related to permissions or access controls rather than an infrastructure configuration. Users are part of many groups. Users and groups are mapped to many roles. To be usable, roles tend to be overly permissive, and this comes at the expense of granularity and tight access controls. Cloud resources are numerous. Permissions change and expand over time as a result of functionality changes, employee turnover, employee job changes, customer attrition, changes to technology stacks, and more. Controlling and managing cloud access rights and permissions is very complex.

The principle of least privilege means only the necessary permissions required for a role should be used and nothing more, reducing your attack surface if the role was to be compromised. Therefore, a modern CSPM tool should be able to:

- Ensure full visibility into cloud assets and identities to detect and remove excessive permissions.
- Use runtime insights to assess which permissions are actually in-use to determine which access risks to fix first.
- Mark unused identities and excessive permissions as high-risk findings, since they are targeted as entry points for bad actors.
- Clearly understand the difference between human and nonhuman identities to reduce the risk of unauthorized access and ensure data privacy.
- Enforce access policies that grant the minimum permissions to perform necessary actions.
- Monitor and alert on entitlement or permission changes to identify suspicious activity (e.g., privilege escalation).
- Audit identity and access management permissions and controls to meet compliance requirements for standards, such as PCI, SOC 2, FedRAMP, and ISO 27001.

Incorporating identity and access-related metadata, such as user information, roles, permissions, and authentication mechanisms, helps attribute system call and cloud activities to specific users or entities. Runtime insights provide this contextual information to assist in auditing, compliance, and detecting potential security threats associated with user behavior.

> We like that Sysdig uses knowledge of what is in use during production to help us make better informed posture decisions. It can help filter out 80% or more of the noise. The bottom line is that CSPM is Sysdig's bread and butter, and that inspires confidence.

BIGCOMMERCE Senior Infrastructure Security Engineer

Choose a Platform with Runtime Insights

Clearly, your conventional security tools and/or legacy CSPM that use static checks are unable to address active cloud risk and the speed of cloud attacks. As you consider a better cloud security approach, look for platform solutions, such as a Cloud Native Application Protection Platform (CNAPP), that unify both static risk assessment and active risk detection capabilities to avoid deploying yet another point solution security tool.

Without runtime insights, attackers can exploit blind spots and remain undetected for extended periods of time, allowing them to carry out their malicious activities undisturbed. Choose a solution that delivers runtime insights to detect and prioritize active cloud risk in order to keep your cloud environments safe.

To learn more about Sysdig cloud security and CSPM solutions, visit **https://sysdig.com/solutions/cspm/**

PB-029 REV. B 3/24