sysdig

CHECKLIST

5 Steps to Securing Multi-Cloud Infrastructure

5 Steps to Securing Multi-Cloud Infrastructure

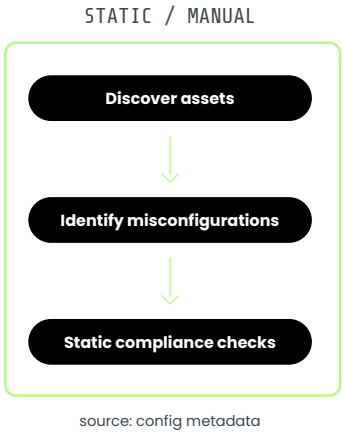
As cloud adoption accelerates, there is a growing need to manage security risks within these dynamic environments. With multi-cloud architectures, organizations can be overwhelmed by the sheer number of services they need to secure. A single misconfiguration in one service can lead to a serious data breach, but the reality is that human errors are impossible to avoid. Automation is required to stay on top of security gaps.

According to Gartner®, "through 2025, over 99% of cloud breaches will have a root cause of a customer misconfiguration or mistake." They also predict that "70% of workloads will be hosted in the public cloud and that 50% of enterprises will intentionally adopt multicloud by 2025[1]."

Imagine a scenario where you notice someone is scraping user information from a bucket that you thought was private. A security engineer investigates, and after a few hours of work, discovers a manual change that has granted public access on that specific bucket. Even worse, they discover many other unplanned storage configuration changes. They feel lucky that one of those modifications triggered the investigation.

How can you keep track of constant additions and changes to cloud services? How can you flag misconfigurations and suspicious activity across multiple clouds? How do you focus on the alerts that signal a real threat? Correlation of periodic scanning results from posture management policies and contextualizing data from multiple cloud sources has been a significant gap for organizations adopting the cloud. Those challenges impact cloud infrastructure management, permissions management, and compliance needs. Tackling these unique cloud security risks requires visibility powered by Runtime Insights.

Our five steps outline how organizations can set up the security strategy to follow as they move to the cloud.



source: config metadata

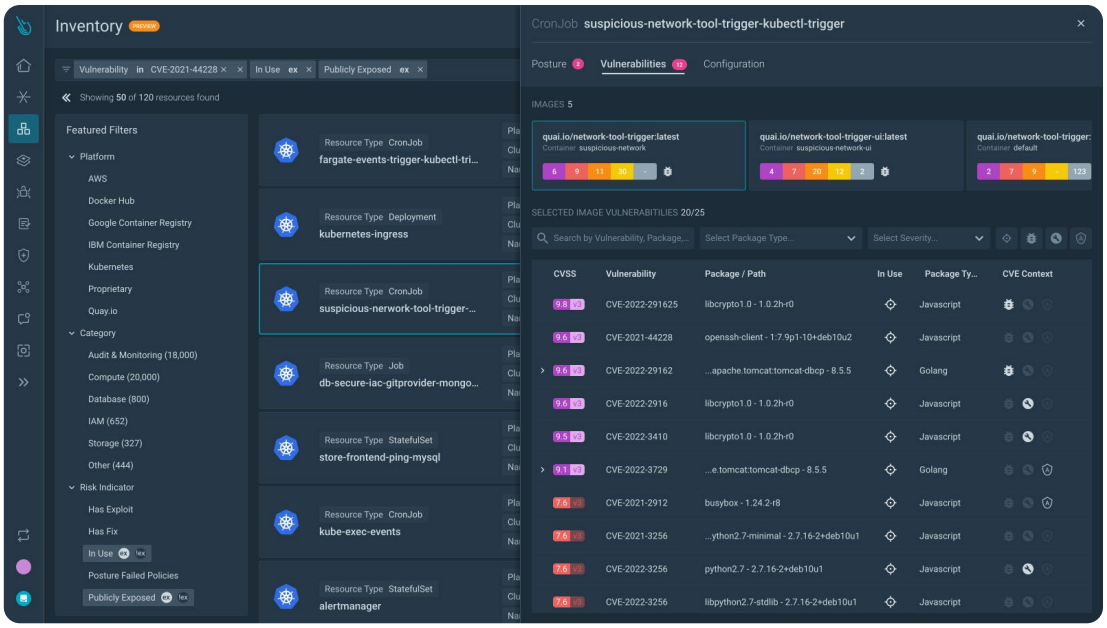
[1] Gartner, Risk-Based Evaluations of Cloud Provider Security, Charlie Winckless, Jay Heiser, 16 January 2023.

STEP 01

Discover Cloud Assets

- Identify the systems, applications, services, and workloads running in all of your cloud environments. Determine if they are secure and compliant.
- Map cloud assets, including accounts, VPCs, regions, storage buckets, databases, etc., to their corresponding IaC manifest.
- Understand where your sensitive data (e.g., customer data, data governed by compliance regulations) is stored and processed across all cloud environments.
- Visualize cloud activity across multiple cloud services.
- Unified view into discovery of cloud assets. No need to jump into different tools for each cloud provider.

In the dynamic landscape of multi-cloud environments, achieving robust security and compliance necessitates a holistic approach. This entails comprehensive identification and mapping of cloud assets, coupled with a keen understanding of sensitive data locations. Organizations benefit from a unified view into cloud activities across providers, simplifying asset discovery and ensuring adherence to security and compliance standards. This strategic approach empowers businesses to navigate the complexities of multi-cloud environments with confidence and precision, safeguarding their data and operations.

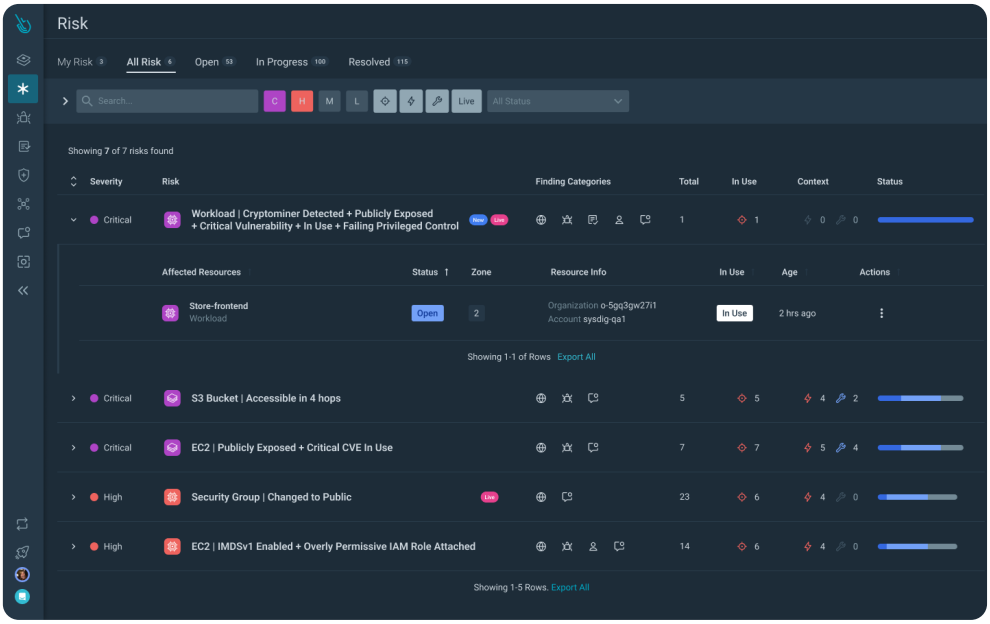


STEP 02

Manage Static Configuration Risk (CSPM)

- Identify risk, poor practices, or erroneous configuration settings, gaining visibility into the current security posture of your multi-cloud environment.
- Detect misconfigurations such as unsecured data storage, excessive permissions, unchanged default credentials and configurations, disabled security controls, unrestricted access to ports and services, unsecured secrets, and more.
- Automatically open a Pull Request to the corresponding Git repository that holds your cloud and Kubernetes configuration. Get remediation procedures with implementation guidance using the cloud providers Console, or CLI commands to harden your security posture.
- Check your cloud configuration against CIS Benchmarks for securing cloud services, community-sourced policies, or your own security baseline.
- Detect misconfigurations and compliance posture drift when cloud resources are created, deleted, or modified.

The proactive identification of risks – detecting and addressing misconfigurations – from unsecured data storage to unchecked access permissions, is a paramount concern. Aligning cloud configurations with industry benchmarks and tailored security baselines further strengthens the overall security posture. Moreover, automating remediation procedures through Git repositories streamlines the process and hardens security. In the pursuit of safeguarding multi-cloud environments, these practices collectively empower organizations to mitigate risks and bolster their defenses effectively.



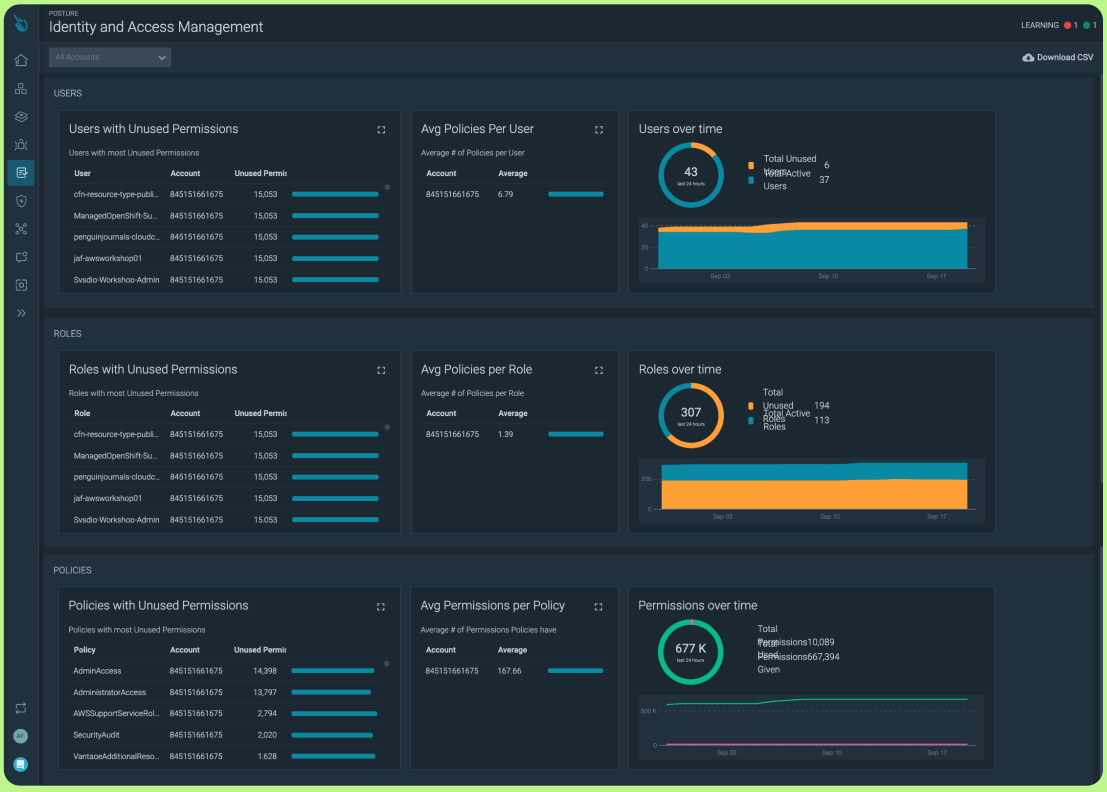
A stack-ranked list reveals the most concerning and urgent risks across your environments

STEP 03

Prevent Cloud Permission Risk (CIEM)

- Access reviews must include the identification of active and inactive users and their associated permissions.
- Apply the just-enough permissions needed to perform core tasks.
- Review these permissions on an ongoing basis.
- Track your progress towards a stronger IAM security posture with out-of-the-box dashboards summarizing the key risks.

Excessive permissions granted to accounts and roles represent a prevalent security issue within cloud misconfigurations. The complexity arises from the amalgamation of resources, actions, and identities within IAM policies. Implementing the principle of least privilege access is paramount in mitigating the risk of data breaches, as well as thwarting potential threats related to privilege escalation and lateral movement.



STEP 04

Continuously Detect and Respond to Cloud Threats

- Correlate assets with activity and visualize risks and exploitable links across resources.
- Combine context from runtime insights such as in-use vulnerabilities and in-use permissions with static assessments, including misconfigurations and known security flaws, to help prioritize what matters most.
- Identify changes in configuration of cloud resources (e.g., storage, databases), infrastructure ports for virtual servers, containers, and container orchestration platforms.
- Detect process execution patterns for unexpected behavior or remote code executions.
- Examine data from past incidents to detect patterns.

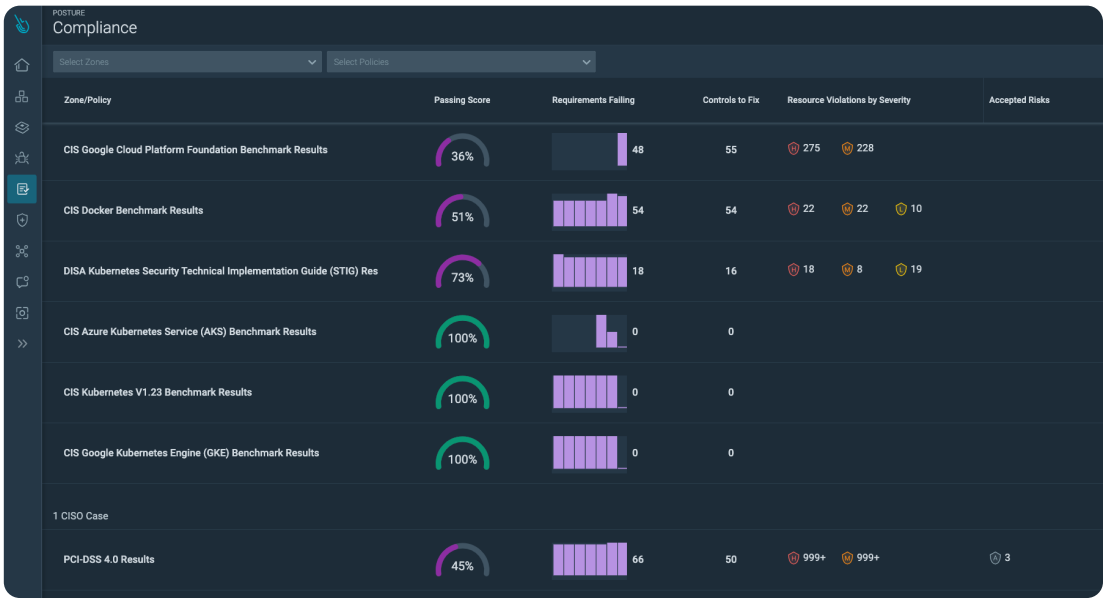
Real-time cloud activity is vital for identifying unusual activities within your cloud control plane, among users, and across services. As cloud attacks can occur within as little as 10 minutes following a breach, the effectiveness of detection hinges on knowing where to direct your focus. Without these elements, organizations operating in multi-cloud environments may find themselves operating in the dark, overwhelmed with information overload, struggling to discern priorities, and ultimately compromising their security posture.

STEP 05

Validate Cloud Compliance and Governance

- Adopt and automate compliance policies with policy-as-code controls that enforce security standards and frameworks like ISO/IEC 27001, NIST 800-53, PCI DSS, SOC 2, FedRAMP, and MITRE ATT&CK®, among others.
- Align resources strategically – business units or environments – so security teams can gain a deeper insight into the required security posture for the underlying infrastructure. This will allow your Cloud teams to easily validate compliance for auditors as well as customers.
- Continuously track cloud compliance progress against frameworks and standards, with detailed reports and security findings. Accelerate mean time to response (MTTR) with guided remediation playbooks and suggestions.

Managing compliance now means contending with a myriad of standards and regulations, some mandatory, some optional, some region-specific, and many overlapping. Failure to meet these standards and regulations carries substantial risks, including damage to reputation and hefty fines.



Summary

In the cloud, every second counts

Attacks move at warp speed, and security teams must protect the business without slowing it down. Sysdig stops cloud attacks in real time, instantly detecting changes in risk with runtime insights and open source Falco. We correlate signals across cloud workloads, identities, and services to uncover hidden attack paths and prioritize real risk. From prevention to defense, Sysdig helps enterprises focus on what matters: innovation.

Dig deeper into how Sysdig provides continuous cloud security across AWS, GCP and Azure.

GET PERSONALIZED DEMO →