sysdig

CHECKLIST

5 Steps to Securing AWS Cloud Infrastructure

5 Steps to Securing AWS Cloud Infrastructure

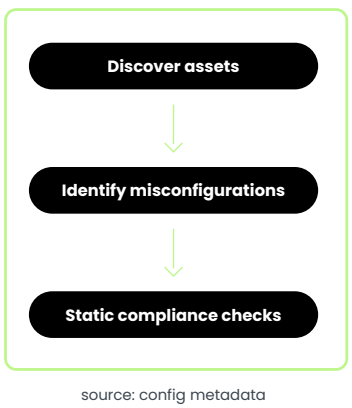
As cloud adoption accelerates, there is a growing need to manage security risks within these dynamic environments. Organizations can be overwhelmed by the sheer number of cloud services they need to secure. A single service misconfiguration can lead to a serious data breach, but the reality is that human errors are impossible to avoid. To stay on top of security gaps and risk, automation is required.

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 by 2025[1]."

Imagine a scenario where you notice someone is scraping user information from an Amazon S3 bucket that you thought was private. A security engineer investigates, and after a few hours of work, discovers a manual change that granted public access to the storage 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 AWS cloud services? How can you flag misconfigurations and suspicious activity? How do you focus on the alerts that signal a real threat? The ability to correlate cloud security posture management scans, cloud permission analysis, compliance checks, and real-time threat insights has been a significant gap for organizations adopting the cloud. Tackling security risks in the cloud 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.



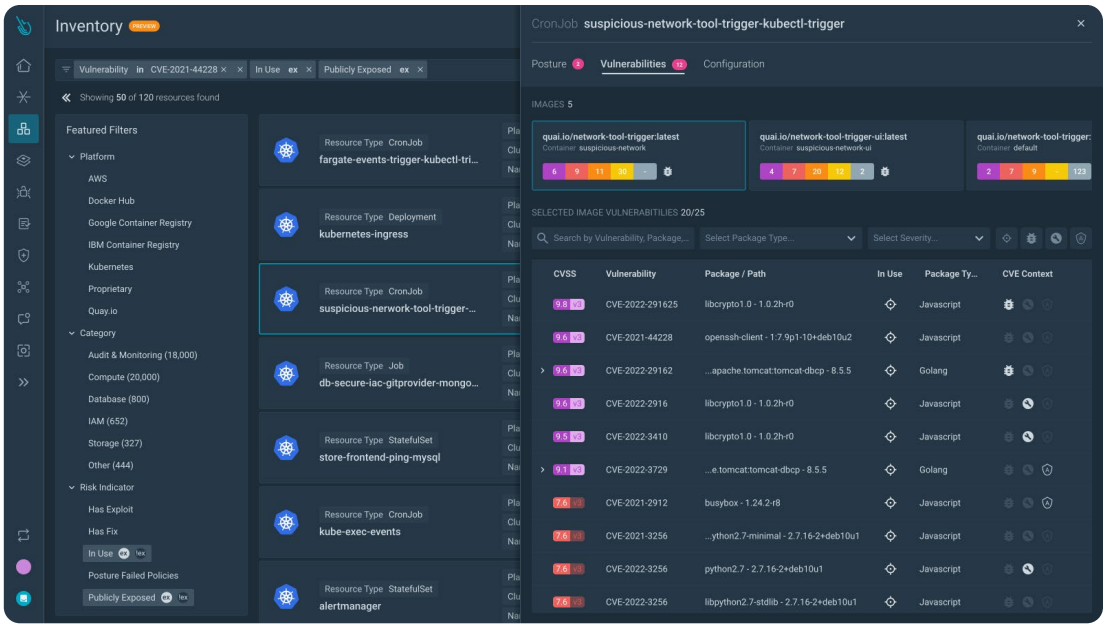
[1] Gartner, Risk-Based Evaluations of Cloud Provider Security, Charlie Winckless, Jay Heiser, 16 January 2023.

STEP 01

Discover Cloud Assets

- Identify the systems, services, and workloads running in your cloud environment. Determine if they are properly configured to be 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 your cloud environment.
- Monitor activity across the assets in your cloud environment.

In the dynamic landscape of AWS 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 of cloud activities, simplifying adherence to security and compliance standards. This strategic approach empowers your business to navigate the complexities of the cloud with confidence and precision, safeguarding your data and operations.

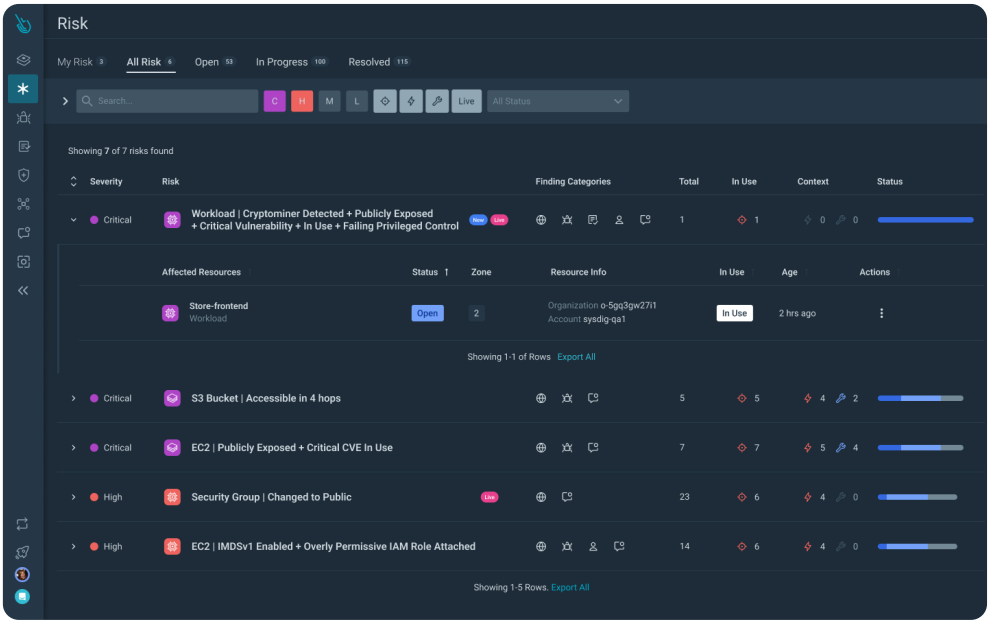


STEP 02

Manage Static Configuration Risk (CSPM)

- Identify risk, poor practices, or erroneous configuration settings, gaining visibility into the current security posture of your AWS cloud environment.
- Detect misconfigurations such as unsecured data storage, excessive permissions, use of default credentials and configurations, disabled security controls, unrestricted access to ports and services, and unsecured secrets.
- Get remediation procedures with implementation guidance using the AWS console, or CLI commands to harden your security posture. Automate remediation pull requests to the corresponding Git repository that holds your cloud and Kubernetes configuration.
- Check your cloud configuration against best practice standards for securing cloud services such as the CIS Amazon Web Services Foundations benchmark, community-sourced guidance, 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 critical practice for cloud security. Aligning cloud configurations with industry benchmarks and security baselines strengthens your overall security posture. Moreover, automating remediation procedures streamlines the process and reduces the potential for human error. In the pursuit of safeguarding your AWS cloud infrastructure and workloads, these practices collectively empower your organization to mitigate risks and effectively bolster your defenses



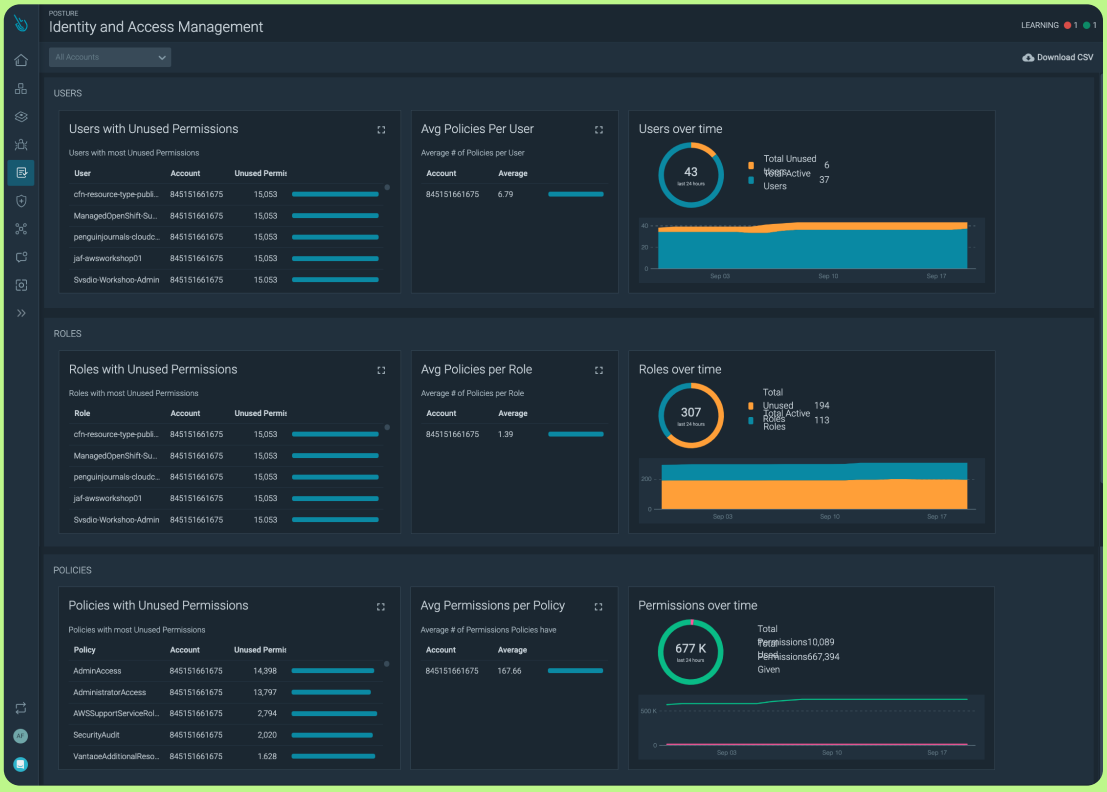
A stack-ranked list reveals the most concerning and urgent risks across your environments

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 your AWS identity and access management (IAM) permissions on a regular basis.
- Track your progress towards a stronger IAM security posture with visualization tools or dashboards that summarize risks.

Excessive permissions granted to accounts and roles present a prevalent security issue within the cloud. 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. Sound IAM practices help to thwart potential threats related to privilege escalation and lateral movement.



STEP 04

Continuously Detect and Respond to Cloud Threats

- Correlate assets with cloud 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 the 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.

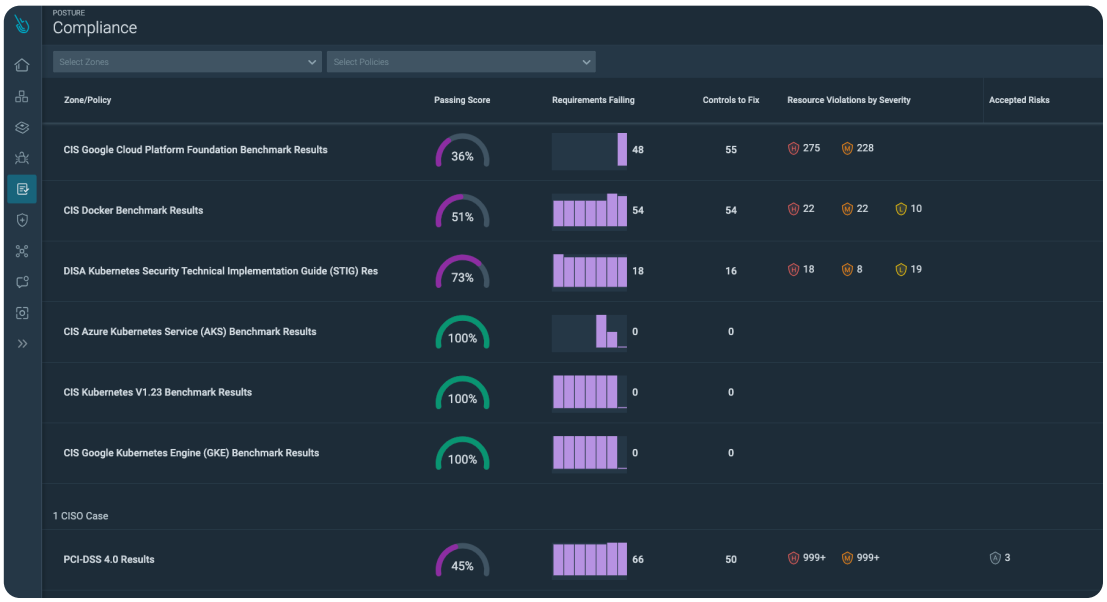
Real-time cloud activity monitoring is vital for identifying unusual activities within your cloud control plane, among users, and across services. Cloud attacks can occur within as little as 10 minutes following a breach. The effectiveness of detection hinges on knowing where to direct your focus. Without these elements, organizations may find themselves operating in the dark. A lack of information or, conversely, too much information with no clear identification of risk, leaves teams struggling to discern priorities and ultimately compromises your 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 to business units or environments so security teams can gain a deeper insight into the required security posture for workloads and the underlying infrastructure. This helps teams simplify compliance validation for auditors and 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 for AWS.

GET PERSONALIZED DEMO →

- DevOps Software Competency
- Security Software Competency
- Containers Software Competency
- Cloud Operations Software Competency