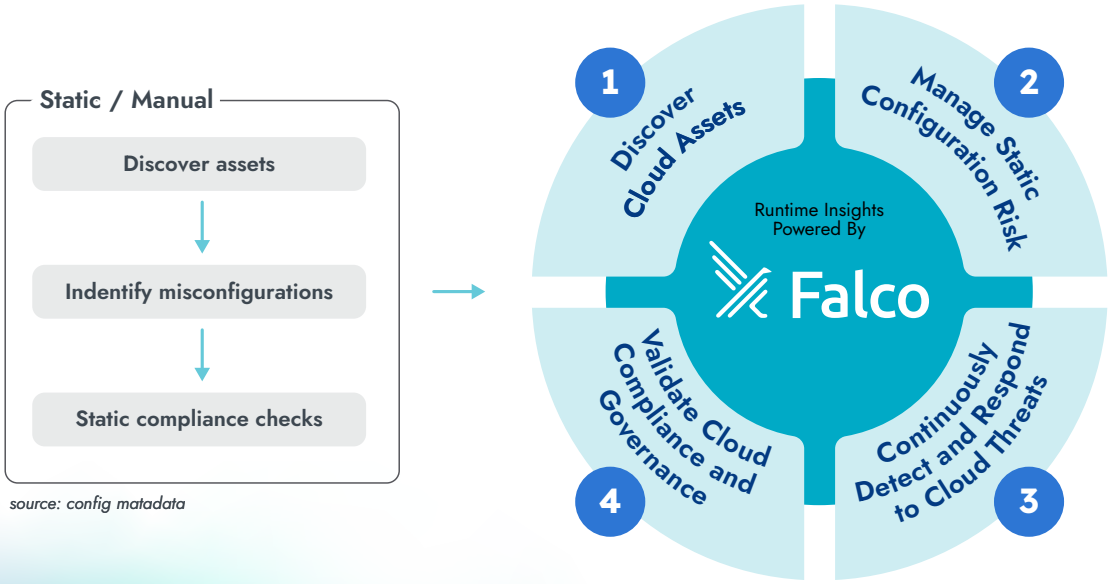
Continuous Cloud Security Checklist for Google Cloud

Cloud and Kubernetes costs is certainly a broad and complex topic. If you are early in your cloud-native journey, you'll soon realize that cost management is something that needs to be tackled, the sooner the better. Companies that don't take care of their Kubernetes and cloud costs are most likely to waste tons of money on their Kubernetes and cloud bills at the end of the month. This can sound pretty obvious, but many businesses don't realize how tough and necessary this task can be until they spend thousands of dollars.

So why is managing Kubernetes costs so challenging? Many factors contribute to this problem, but the nature of microservices is a key contributor. These new microservices architectures enable users, departments, and organizations to deploy and maintain applications easier and faster. In this new era, you have to pay attention to the associated costs of deploying and maintaining services in the cloud. Poor architectures and application designs, as well as deploying or scaling up applications easily are some of the factors that contribute to runaway costs. That's why you may end up overspending resources and money, making your Kubernetes and cloud bills grow significantly.



source: config matadata

1 Discover Cloud Assets

- Identify the systems, applications, services, and scripts running in your cloud environment. Determine if they are secure and compliant.
- Map your cloud assets including accounts, VPCs, regions, cloud storage buckets, Cloud SQL, etc.
- Understand where your sensitive data (e.g., customer data and data governed by compliance regulations), is stored and processed.

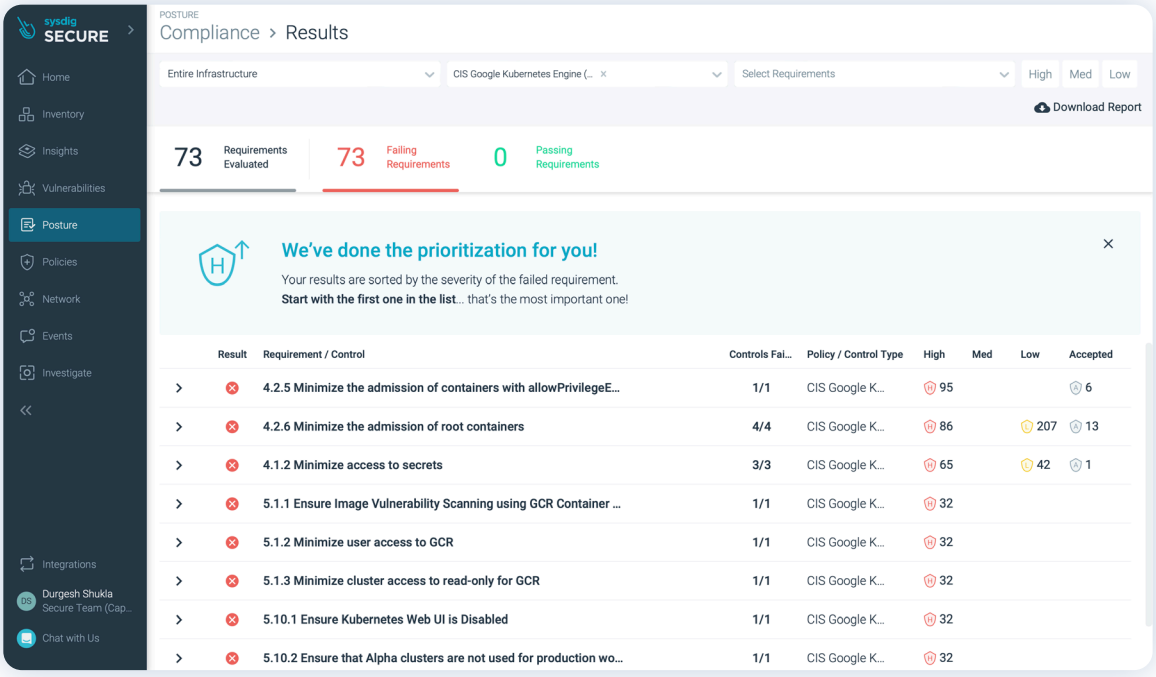
Understanding and tracking your in-use cloud assets will help baseline your current operating state and let you prioritize critical services that require careful monitoring to stay on top of potential threats and accelerate remediation.

2 Manage Configuration Risk

Identify risky configuration settings and gain visibility into the current security posture of your cloud and container environment. Detect misconfigurations, such as public storage buckets, exposed security groups, leaked secrets and credentials, etc. Also, determine if your environment and configurations have changed over time – commonly referred to as configuration drift.

Check your cloud configuration against CIS benchmarks for securing cloud and container services, community-sourced best practices, or your own security baseline. By periodically assessing your environment and Google Cloud accounts against a curated collection of checks, you will understand which services and configurations present a potential security challenge.

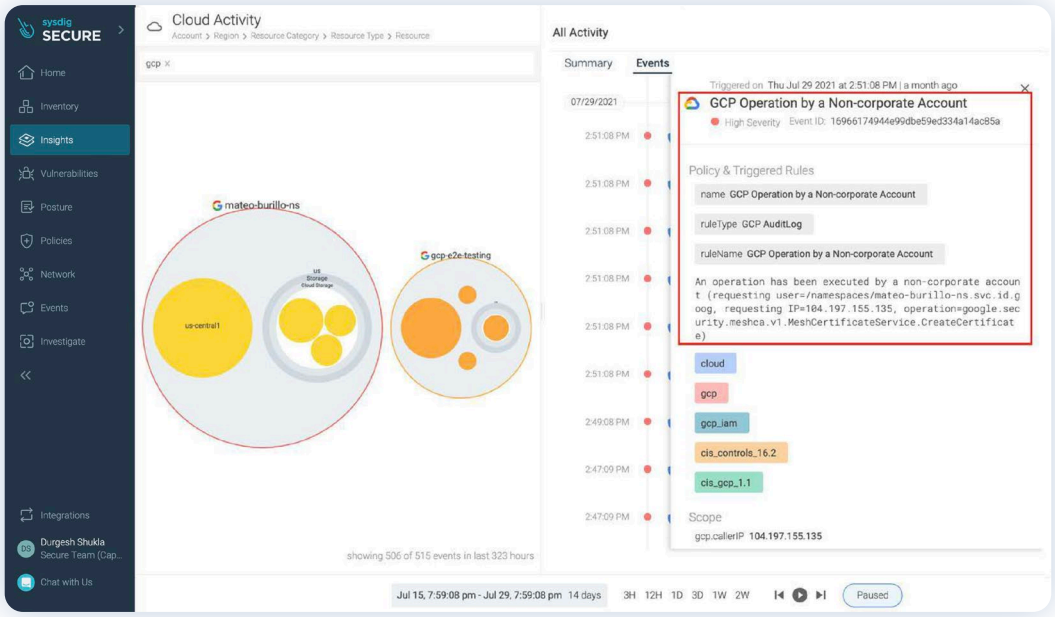
Following implementation guidance and remediation procedures will help you harden the security posture of your Google Cloud workloads and infrastructure.



3 Continuously Detect and Respond to Cloud Threats

Continuously detect suspicious cloud activity across all cloud accounts, users, and services by analyzing cloud activity logs.

- Look for abnormal patterns and unexpected cloud service or user behavior.
- Detect process execution patterns for suspicious behavior or remote code executions.
- Look for credential theft, especially for longer-lived credentials or high-privilege credentials.
- Identify changes in the configuration of cloud resources (e.g., Cloud Storage), infrastructure ports for virtual servers, containers, and container orchestration platforms.
- Identify data leaks or unintentional exposure of sensitive information.
- Examine data from past incidents to detect patterns.



Detect misconfigurations and unexpected activity when cloud resources are created, deleted, or modified across all of your Google Cloud accounts. This reduces your exposure to risk from compromised cloud accounts or unintended human error. Manage risk by using Google Cloud Audit Logs as a source of truth to detect cloud threats as soon as they happen. Leverage open-source Falco rules to automate detection, enable compliance, and capture data for risk auditing.

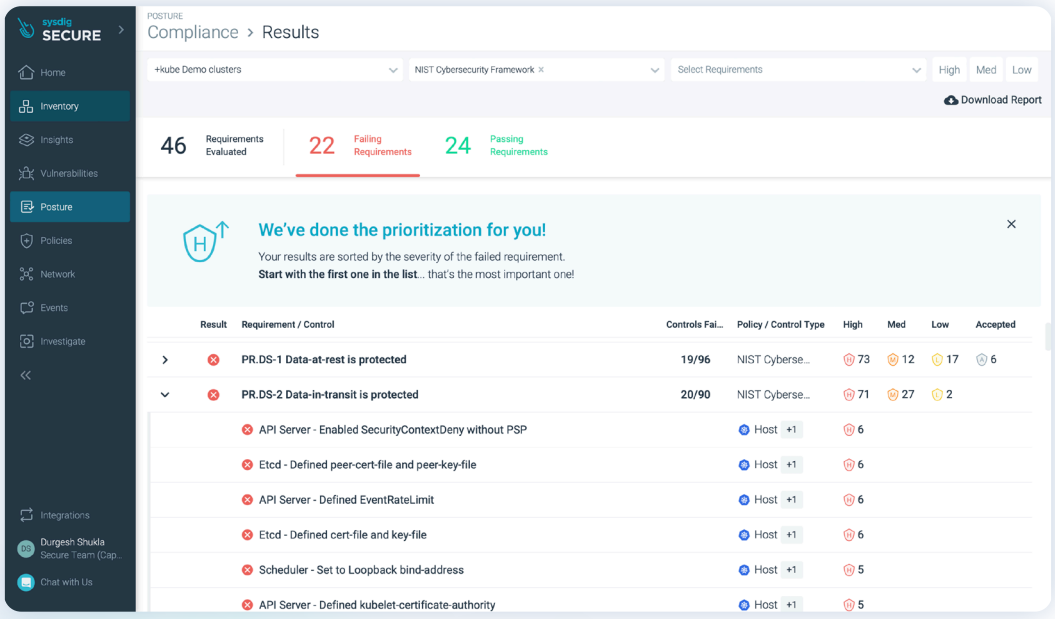
4 Validate Cloud Compliance and Governance

Achieve and maintain compliance with regulatory frameworks, like NIST, PCI DSS, SOC 2, ISO, HIPAA, MITRE ATT&CK®, and CIS, through a rich set of Falco rules designed to help you meet security standards. Enable governance and enforcement of your organization-specific security controls. This allows your DevOps and Cloud teams to easily validate compliance for auditors, your business, and customers.

Continuously track cloud compliance progress against benchmarks and standards with detailed reports and alerts. Accelerate mean time to response (MTTR) with guided remediation tips.

Using a comprehensive set of checks and policies, the Sysdig Secure DevOps Platform helps you continuously monitor and manage your security posture across your Google Cloud infrastructure. With solutions built on Cloud Native Computing Foundation® (CNCF®),open source projects, including Falco, the open standard for runtime detection, and Open Policy Advisor (OPA), Sysdig enables you to detect abnormal activities and changes across your cloud accounts and services. Continuously monitoring cloud runtime behavior can alert your team to possible risks and enable them to respond quickly.

By adopting the Sysdig platform, you can achieve cloud-scale and get enterprise support that helps you focus your resources on delivering applications, rather than managing security and visibility tools.



Powered by runtime insights, Sysdig helps you focus on the vulnerabilities and threats that matter most. From shift left to shield right, Google Cloud users can prevent, detect, and respond at cloud speed.

START YOUR FREE TRIAL

GET PERSONALIZED DEMO

www.sysdig.com

CL-015 Rev. B 8/23