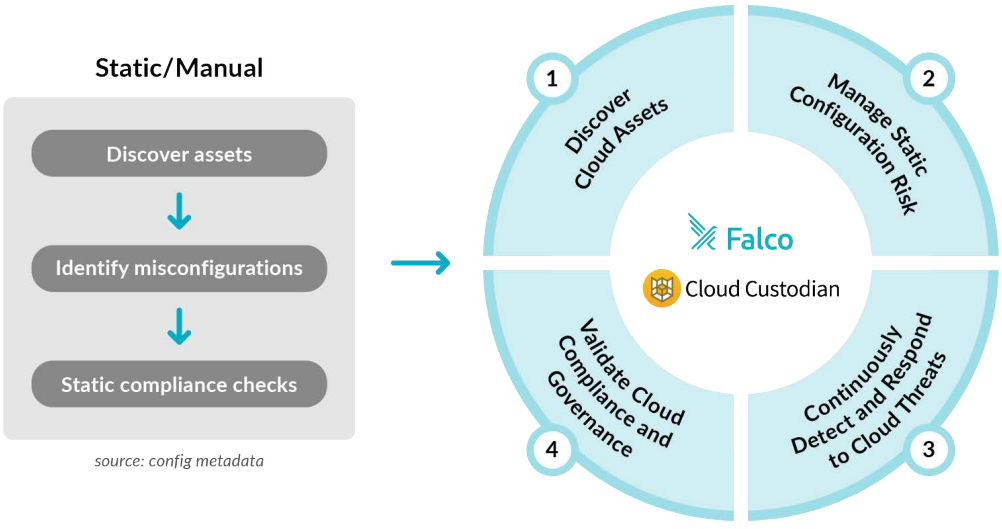
Continuous Cloud Security Checklist for AWS

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, "Nearly all successful attacks on cloud services are the result of customer misconfiguration and mistakes." They also predict that through 2023, at least 99% of cloud security failures will be the customer's fault.[1]

Imagine a scenario where one of your critical services suddenly stops working. A DevOps engineer investigates, and after a few hours of work, discovers a manual change to a firewall rule that should protect the failing service. Even worse, she discovers many other unplanned firewall rule changes. She feels lucky that one of those modifications triggered the investigation. How can you keep track of constant additions and changes to AWS services? How can you flag misconfigurations and suspicious activity across multiple clouds? How do you focus on the alerts that signal a real threat?

Tackling these unique cloud security risks requires a continuous and automated approach. Our Continuous Cloud Security checklist outlines how organizations can manage cloud security risk on AWS.



[1] Gartner: Innovation Insight for Cloud Security Posture Management

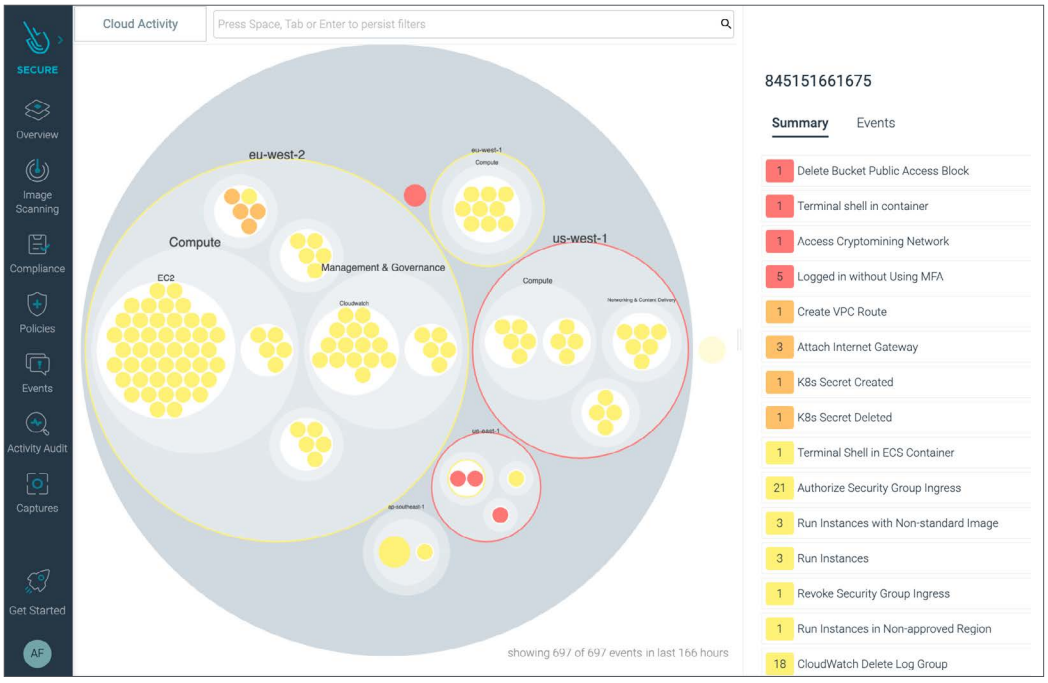
1

CONTINUOUS CLOUD SECURITY CHECKLIST FOR AWS

Discover Cloud Assets

- Identify the systems, applications, services, and scripts running in your cloud environment. Determine if they are secure and compliant.
- Map cloud assets including accounts, VPCs, regions, S3 buckets, RDS, etc. Understand where your sensitive data e.g., customer data, data governed by compliance regulations, is stored and processed.
- Visualize cloud activity across multiple cloud services.

This will help baseline your current operating state, as well as help you prioritize services with the most critical threats and accelerate remediation.



2

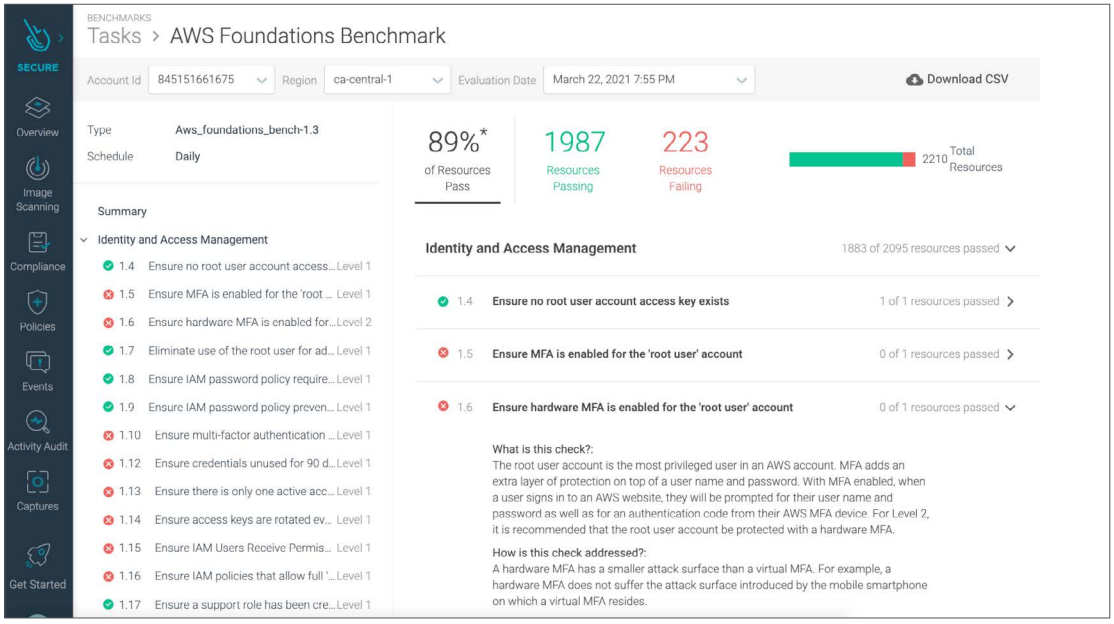
CONTINUOUS CLOUD SECURITY CHECKLIST FOR AWS

Manage Static 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/credentials, etc. Also determine if you have configuration drift.

Check your cloud configuration against CIS benchmark for securing AWS services, community sourced policies, or your own security baseline. With AWS Cloud Benchmarks, you can execute a curated collection of checks periodically on your AWS account that will inform you which services and configurations present a security challenge.

Get remediation procedures with implementation guidance using the AWS Console, or CLI commands, to harden your security posture.



3

CONTINUOUS CLOUD SECURITY CHECKLIST FOR AWS

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 suspicious patterns or abnormal behavior and use your data for incident response.
- Detect process execution patterns for unexpected behavior or remote code executions.
- Look for credential theft, especially for longer-lived credentials or high-privilege credentials.
- Identify changes in configuration of cloud resources (e.g., S3), infrastructure ports for virtual servers, containers, and container orchestration platforms.
- Identify sensitive data leaks through unintentional exposure of information.
- Examine data from past incidents to detect patterns.

Detect misconfiguration and unexpected activity when cloud resources are created, deleted, or modified across all of your AWS accounts. This will reduce your exposure to risk from compromised cloud accounts or unintended human error. Manage your risk by using AWS CloudTrail event logs and Falco rules as the source of truth for operational audit. Detect threats as soon as they happen, and enable governance, compliance, and risk auditing for your cloud accounts.

4

CONTINUOUS CLOUD SECURITY CHECKLIST FOR AWS

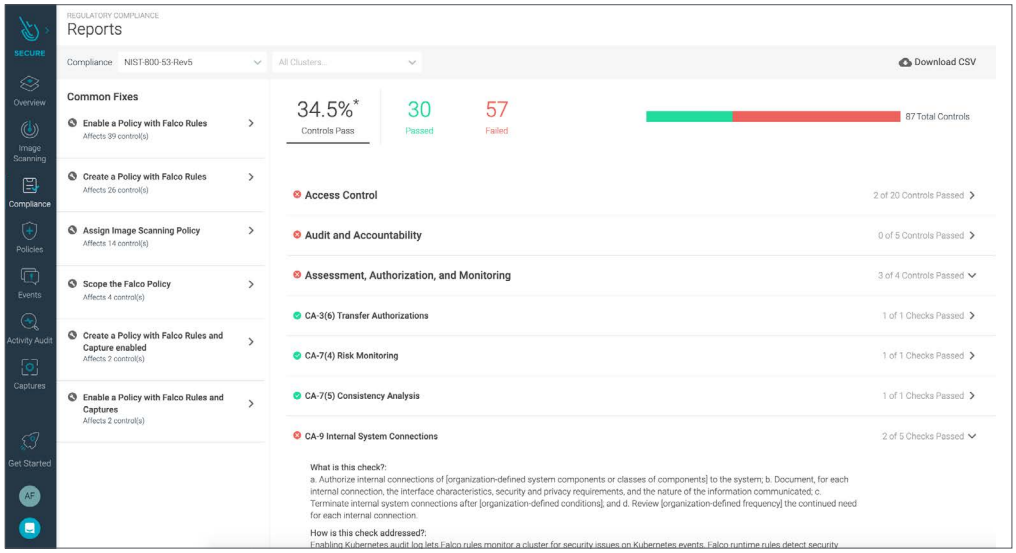
Validate Cloud Compliance and Governance

Achieve and maintain compliance with security frameworks through a rich set of Falco rules for security standards and benchmarks, like NIST 800-53, PCI DSS, SOC 2, MITRE ATT&CK®, CIS AWS, and AWS Foundational Security Best Practices. Enable governance and enforcement of your organization-specific security controls. This will allow your DevOps and Cloud teams to easily validate compliance for auditors as well as 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.

The Sysdig Secure DevOps Platform helps you continuously monitor and manage your security posture across multi-cloud infrastructure. It enables you to detect threats from abnormal activities and changes across all your cloud accounts using Falco, the open standard for runtime detection, and Cloud Custodian. Continuously monitoring cloud runtime behavior for changes and suspicious activity can alert your team to possible problems and enable them to respond quickly.

Open source tools take advantage of rapid community innovation and open standards. By adopting the Sysdig platform with enterprise-grade scale and support you can focus your resources on delivering applications, rather than managing security and visibility tools.



How Sysdig Extends Cloud Custodian	Cloud Custodian	Sysdig Secure
Support	Community	Sysdig
Continuous CSPM		
Asset discovery	✓	✓
Cloud security posture management and compliance	✗	✓
Cloud risk insights	✗	✓
Threat detection based on cloud logs (e.g., suspicious logins, file access, etc.)	✗	✓
Context enrichment	Cloud	Cloud, host, containers, and Kubernetes labels
Compliance benchmarks, dashboards, & guided remediation	✗	✓
Additional Container Security, Monitoring, & Troubleshooting	✗	✓

Dig deeper into how Sysdig provides continuous cloud security on AWS.
Start running containers and AWS cloud services with confidence for free.

Start Your Free Trial **Get Personalized Demo**