cloudtamer.io

Continuous Compliance in the Cloud

The Complexity of Compliance

For many organizations, maintaining compliance in the cloud is a top priority. Yet the compliance gap, or the gap between the policies organizations adopt and those which they can actually enforce, is a real issue. According to one study, 77% of IT decision makers believe that they would not pass all of their cloud compliance audits for cloud resources.[1]

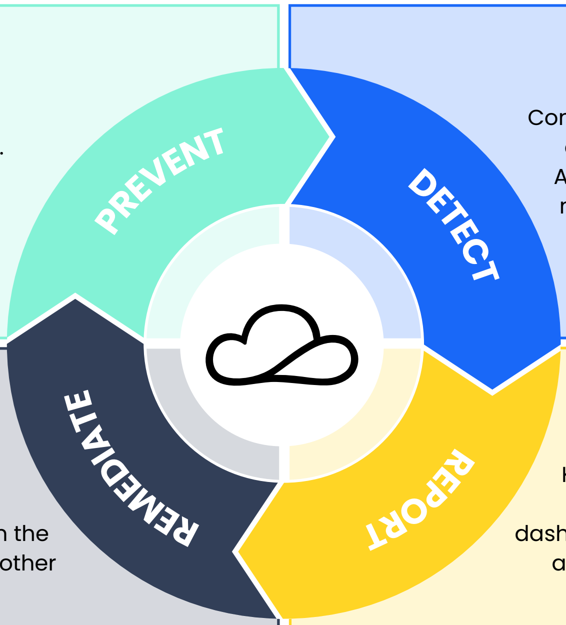
Compliance in the cloud is complex. Whether you follow established guidelines such as NIST or HIPAA or you define your own standards, the sheer number of policies and resources in the cloud make manual tracking a logistical nightmare. NIST 800-171 alone — just one example of NIST's security standards — includes 110 policies, and each policy can apply to multiple resources. You could spend hundreds of hours tracking compliance manually. If you don't, you risk non-compliance, which leaves you exposed to potential security breaches or even civil or criminal penalties if you violate guidelines required by law. And with the elastic nature of the cloud, achieving compliance at one moment in time doesn't ensure compliance going forward.

So how can you get the full picture and close the compliance gap when compliance is so complex?

A 360-Degree Solution for Continuous Compliance

We're here to help you simplify with continuous compliance.

At cloudtamer.io, we already provide robust tools to establish boundaries in the cloud. Our newest features go beyond these proactive rules, providing reactive checks to get a near-real time view of policy violations within our cloud governance solution. Using our compliance jumpstarts, compliance checks and compliance dashboard, you get powerful 360-degree coverage to prevent, detect, report, and remediate compliance violations.



1. PREVENT

Compliance Rules:

Establish boundaries to prevent non-compliance with cloud rules. Use our compliance jumpstarts, which consist of plug-and-play cloud rules, to enforce policy with minimal configuration.

2. DETECT

Compliance Checks:

Continuously monitor your cloud with customizable compliance checks. Apply these checks only where you need them, conducting scheduled and manual scans for 24/7 coverage. We provide many checks to get you started.

3. REPORT

Compliance Dashboard:

Keep eyes on the compliance gap with clear visual indicators on the dashboard. Track violations found and addressed and sort by compliance standard (such as NIST or CIS).

4. REMEDIATE

Compliance Automation:

Enable automatic remediation of issues to fix compliance findings without manual intervention. Gain the visual clarity to find and address other issues manually.

[1] Logicworks 2019 State of Cloud Compliance Annual Survey

Preventing and Detecting: Customize Your Rules and Checks

We've expanded our cloud rules and harnessed the power of the open source Cloud Custodian rules engine to provide you with powerful methods to prevent and detect non-compliance. Using the built-in compliance engine, you can create compliance checks or individual policies that find cases of non-compliance and, if desired, automatically fix the issue. We provide many checks to get you started, as well as compliance jumpstart resources, or pre-configured cloud rules that uphold individual compliance standard controls.

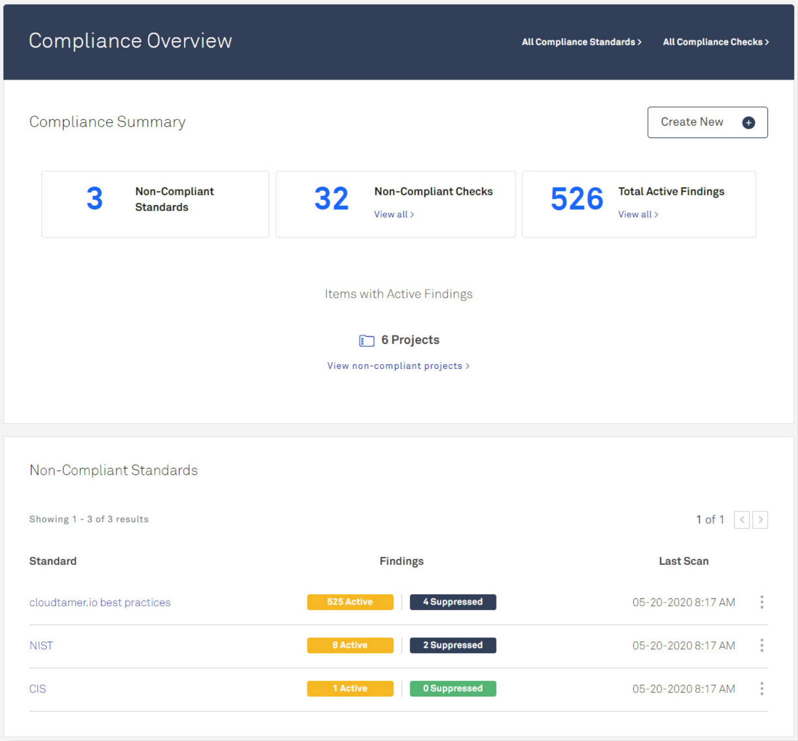
Need more flexibility? No problem. These tools are fully customizable, so you can:

- **Apply checks only where you need them.** Compliance standards are attached to inheritable cloud rules, which apply only where you specify. Resources can also be exempted from checks.
- **Run them on your own timeline.** You can set the compliance check frequency, running scheduled checks automatically or running ad hoc manual scans whenever you need them.
- **Write your own rules and checks.** We now provide a form to enter your own code for compliance checks, so you can craft custom checks using YAML.
- **Go beyond the built-in engine.** You can connect with an external compliance engine instead of Cloud Custodian to pull those findings into cloudtamer.io.

Reporting and Remediating: Visualize Your Compliance

Our new dashboard, which shows how many of your compliance checks were found non-compliant, gives you insight at-a-glance into compliance violations and lets you fix them easily. Using this dashboard, you can:

- **Find the hot spots.** You can view findings by resource to see which areas have the most compliance issues.
- **See the impact of automation.** You'll get information on how many non-compliant checks were automatically remediated, so you'll know the impact of the automation you've put in place.
- **Let your team take action.** Allow your security team to view active findings, intervening manually or suppressing the finding if it's not relevant, and build in automatic remediation wherever you need it.
- **Keep your fingers on the pulse of your cloud compliance:** Managers can easily learn how many compliance checks failed and exactly how they were handled by your team (whether ignored, addressed, or suppressed).



Compliance Overview

Compliance Summary

3 Non-Compliant Standards

32 Non-Compliant Checks

526 Total Active Findings

Items with Active Findings

6 Projects

Non-Compliant Standards

Showing 1 - 3 of 3 results

Standard	Findings		Last Scan
cloudtamer.io best practices	525 Active	4 Suppressed	05-20-2020 8:17 AM
NIST	8 Active	2 Suppressed	05-20-2020 8:17 AM
CIS	1 Active	0 Suppressed	05-20-2020 8:17 AM