SteelCloud

Making AUDITS worry-free while lowering overall compliance costs

CHALLENGE: Improving compliance and audit-readiness across Linux systems

You never need to fail a compliance audit to have the threat hanging over your head like a dagger. With compliance audits sometimes taking place quarterly or yearly, the pressure is real. And knowing that the goal is to remain continuously compliant just adds to the stress. That was the case with one of SteelCloud's Federal Civilian customers.

The customer was subject to STIG compliance mandates across their 131 endpoints, plus internal audits from leadership to prove their compliance. While they never failed, the threat was there. Their compliance percentages were usually in the 50s for their Linux systems. This put them in danger of having fines assessed and their reputation damaged. And they had a good idea what they could be doing better.

Their team had been automating their STIG compliance process with WatchMaker. This nonetheless required a good bit of manual remediation performed by subject matter experts. While the automation helped, the process still took too long to implement and too long to revise when DISA released updated STIGs every quarter. While they passed all their audits, they weren't able to do it efficiently or with confidence. It was time for an upgrade.

SOLUTION: Implementing customized policies—and a solution beyond compare.

When reviewing their automation options, they looked again at WatchMaker. There was a lot of coding required, little reporting capabilities available, it took specialized engineers to implement and their customization capabilities were lacking. The customer knew they wanted more customization and less effort. When SteelCloud announced coverage for Ubuntu LX on ConfigOS MPO, they knew they had finally found their answer.

ConfigOS MPO is a unified automation solution, which means scanning, remediation, maintenance and reporting are all part of a single, integrated solution. No more partial automation solutions or a series of solutions cobbled together. Everything was purpose built for STIG compliance automation. And its reputation in the Federal marketplace was well known.

ConfigOS MPO picked up where other solutions leave off. You can customize policy to fit your needs and remediate across all your endpoints at once, saving a lot of time and effort. And ConfigOS automatically creates artifacts and reporting, which is key to proving compliance. When compared side-by-side with their current solution, the customer felt their choice was clear.

A Comparison of STIG Compliance Solutions

	Previous Solutions	ConfigOS MPO
Purpose	DevSecOps framework that applies STIG code via Salt/SLS	End-to-end STIG automation, scanning, remediating, managing and reporting from a single solution
STIG Content	Community-maintained YAML/SLS STIGs	Vendor-maintained, validated content aligned with DISA
Skill Requirement	High—Requires knowledge of SaltStack, GitOps, YAML, CI/CD	Low—Wizard-driven workflow with no STIG/Salt/Pipeline expertise needed
Assessment	Limited scanning; mainly remediation	Full assessment + scoring + delta views
Reporting	Minimal; DevOps-style logging	Audit-ready HTML, XML, XCCDF and dashboards
Deployment	Requires pipeline setup, repo mgmt, Salt infra	Turnkey, installer-based, built for air-gapped environments
Coverage	For OS out of the box DISA STIGs	OS + 3rd-party apps + custom policies
Change Control	Manual pipeline governance	Automated, consistent, testable enforcement
Scalability	High with proper DevSecOps maturity	High by default—built for distributed and classified environments
Best Fit	DevSecOps shops with strong coding culture	Any org that needs fast, repeatable, audit-clean STIG compliance

OUTCOMES: Saving time, reducing effort and improving compliance while saving 62% of the costs.

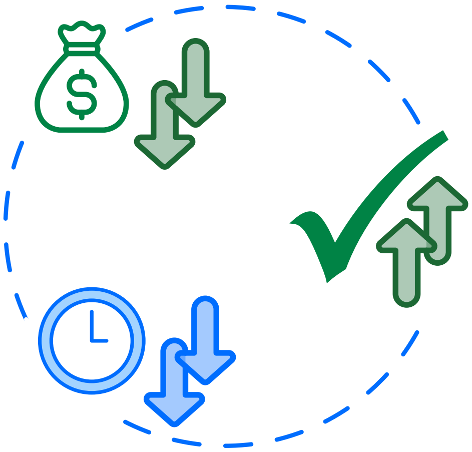
After implementing ConfigOS, the customer's compliance numbers soared. Now they have compliance rates of 90% and above on all Linux systems. Their audit-readiness is drastically improved, simplifying audits. They can easily customize policy, then automate remediation. Their team is more productive. And their overall security is improved and more consistent.

Remarkably, the customer realized a cost avoidance of $85K using SteelCloud as opposed to the manual methods they were using before, saving them 62% year over year in their cybersecurity and audit-readiness budget. Labor costs are roughly 94% lower with ConfigOS MPO.

ConfigOS MPO has proven itself to save time, effort and money while improving outcomes. As a result, the entire government entity the customer is a part of is considering making ConfigOS available to other agencies under their purview. Discussions are currently in process with their review board.

Rapid Improvements

- ✓ **Cost Avoidance:** 62% reduction in cost
- ✓ **Effort Reduction:** 93% reduction in hours/endpoint
- ✓ **Average Compliance Rate:** From 50% to over 90%



> **"Another great thing is that, when you're doing the scans, you can set up different policies to do different things. So if I wanted to set up certain ones to hold back certain things, I can pick it, and run the STIGs that way. Start with one policy and not have to do them over and over again."** *—Federal Civilian Customer's Engineer*