SteelCloud

Major US Systems Integrator Reduces Classified STIG Compliance Effort by over 90%

CHALLENGE: Tackling the STIG process across 100s of DoD systems.

Before they can be deployed on individual devices, each of a system integrator's product operating systems must meet Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) requirements to ensure the security of the DoD IT infrastructure. Traditionally, STIG compliance is a long and laborious, manual process that needs to be done for each and every implementation of a classified system. Moreover, because these systems are classified, vendors only have limited access to them. As a result, they are known as Limited Application Access (LAA) systems.

To conceptualize the scope of effort the STIG process takes for an organization the size of this integrator, one server or workstation might take 16 hours to bring into (and sustain) compliance over an average year. Multiply that by 2500 supported systems—then add all the updates to STIG policy that come on a quarterly basis, not to mention OS updates and app stack releases—and it takes 20 people working full time just to keep these systems current and in compliance. This integrator's service locations also handle hardening and patching for these systems using different approaches. Ultimately, they all get the job done, but not in a standardized, scalable or cost-effective way.

This integrator was living with an overwhelming flow of STIG needs that required the talents of skilled (and expensive), highly sought-after engineers to complete. It wasn't until they met SteelCloud that they found a solution.

SOLUTION: Revolutionizing compliance efforts with automation.

A colleague at another office referred SteelCloud to a Subject Matter Expert at this major integrator. What they heard blew their minds—ConfigOS could automate the STIG process and cut the time from 16 hours down to an hour or less. They gave it a try and to their surprise, it delivered!

- ✓ STIG processes that used to average 16 hours per OS now take an hour or less
- ✓ The overall expenditure of man hours each year went from 40,000 using manual processes to 2,500 hours using ConfigOS—a 94% decrease in time spent

Now that all the integrator locations are using ConfigOS, the STIG process is standardized and scalable across the enterprise, making documentation and reporting easier. One report meets nearly all requirements at every site. The workforce is on the same page with a unified front and the integrator has created a well-organized, consistent and reliable framework for compliance that meets DISA requirements.

> ***STIG work and patching was the bane of our existence. Always STIGing. Now, with SteelCloud, STIG work is done more readily, and engineers can focus those saved hours on other initiatives and maintaining a competitive edge.***
>
> *Sr. Advanced Network Engineer, Major Integrator*

OUTCOMES: Avoiding millions of dollars in costs.

Perhaps the biggest impact that ConfigOS has had on this integrator comes from the man hours saved in STIG compliance. When calculated using the hourly rate for each engineer, this client estimates a cost avoidance of ~$3M annually to support their client in just one comparatively small program. Engineers are now available to support other projects and beat the innovation curve. Best of all, the integrator is now able to do a better job supporting our nation's defense.

The STIG process, and any downtime associated with it, also moves faster. And ConfigOS has revolutionized the consistency and validation reporting around DISA compliance mandates, including STIG Viewer integration and enterprise dashboard reporting.

The integrator is now a vocal proponent for SteelCloud, spreading the word among colleagues and clients. To date, SteelCloud's ConfigOS software had been deployed on all 2500 LAA systems this division supports and it is currently being rolled out on thousands more. And it all started with a 1-hour demo!

Supporting Evidence

Current costs without SteelCloud (Manual hardening)		Comments
Number of Workstations and Servers within [redacted]	2491	Number of computers supported by [redacted] Engineers. Assumes all computers will leverage SteelCloud for hardening due to RMF impelmentation.
Maintenace in support of system hardening	16	Average time (in hours) that an engineer spends administering a PC during the lifecycle of the PC (initial hardening, maintenance, audit support etc.)
Total Hours:	39856	
Avg Hourly Salary Per Engineer	$100.00	Average hourly rate for an [redacted] engineer/admin
Annual Labor Cost to Maintain all Systems:	$3,985,600.00	
Total Annual Costs:	$3,985,600.00	

Costs using Steelcloud		Comments
Labor Costs/Analysis:		
Number of Workstations and Servers	2491	Number of computers supported by [redacted] Engineers. Assumes all computers will leverage SteelCloud for hardening
Maintenace in support of system hardening	1	Average time an engineer would spend administering a PC during the lifecycle of the PC leverraging SteelCloud (initial hardening, maintenance, audit support etc.)
Total Hours:	2491	
Avg Hourly Salary Per Engineer	$100.00	
Annual Cost to Maintain all Systems:	$249,100.00	Assumes an engineer would spend at least an hour per PC even with SteelCloud automating most of the tasks.
Software Costs:		
Average SteelCLoud Subscription Cost per Workstation:	$125.00	Average price per computer to license
SteelCloud Foundry License	$7,500.00	Host based license that is used to create the security signatures that are deployed to the client computers.
Total SteelCloud Subscription annual costs:	$318,875.00	
Total Annual Costs:	$567,975.00	

Cost Savings Annually:		Comments
Total Costs Using SteelCloud	$567,975.00	
Total Costs Using Manual Hardening	$3,985,600.00	
Cost Savings Annually:	**$3,417,625.00**	Cost Avoidance/Savings to [redacted] by Implementing SteelCloud