

# The Case for Revolutionizing STIG Policy Automation

## Overview – An Opportunity for \$200M in Near-term Savings

The Department of Defense (DoD) protects its 15,000 networks by defining, implementing, and auditing "best practices" for installation and maintenance of its information technology resources. The Defense Information Systems Agency (DISA) develops and publishes policy, in the form of the Security Technical Information Guides (STIGs). While significant advances have been made in the areas of threat definition and vulnerability assessment, little progress has been made in automating the arduous tasks of creating and maintaining STIG policy execution on all of the thousands of servers operated in the DoD. The cost savings opportunity by automating STIG policy is significant - easily exceeding \$200 million per year. In addition to reducing costs, STIG policy automation will significantly reduce the need for highly specialized IT support staff, will enhance systems availability, and through improved compliance, will significantly improve the military's critical cyber security posture.

## The Server Policy Problem

Of the functions mandated by the STIGs, set-up and maintenance of server policy settings is by far the most time and labor intensive. In reality, vendor applications are rarely designed to operate in STIG environments. To allow these applications to operate, server policies must be manually adjusted on an application by application, server by server basis. The policy update process also results in server downtime - both planned and unplanned. With our experience in working with commands across the DoD on server security support issues, we calculate that the military spends in excess of \$10,000 annually, per server instance (both physical and virtual) in maintaining STIG policy compliance. While significant initiatives are underway within the DoD to automate auditing of server policy, little has been done to automate the actual set-up and maintenance of STIG-compliant server environments.

## The Solution - Revolutionizing Server Policy Execution with ConfigOS

SteelCloud has seen firsthand, the challenges that the DoD has in balancing mission, security, resources, and costs in an attempt to keep their IT infrastructure up to date and in compliance with ever advancing computer systems security policies. SteelCloud's **ConfigOS** is a new patent-pending technology that converts the DISA server policy STIGs into machine readable secure XML signatures used to update server policies. **ConfigOS** will allow commands to automatically update DISA policy by applying these simple signatures – even across secure enclaves and security domains. The previous multi-day process becomes a 5 minute activity. **ConfigOS** will reduce the DoD's server STIG maintenance expense by over 70%. Besides the cost savings, **ConfigOS** is a low disruption platform - no changes need be made in the DoD's networks - no new hardware is required – its unique capabilities do not overlap with any other technology implemented within the DoD. And, being a started task, **ConfigOS** will not affect the capacity or throughput of any application or infrastructure. Unlike typical "boil the ocean" enterprise projects, **ConfigOS** represents enterprise efficiency without the overhead, leading to a much higher level of actual security compliance. **ConfigOS** will pay for itself in the same budget year.

## Now is the Time

With tight budgets making security compliance resources scarce, policy automation is critical just to maintain the DoD's current security posture. **ConfigOS** represents the perfect convergence of near-term significant cost/resource savings with increase security compliance – utilizing a simple to implement approach that pays for itself the first time it is used. ConfigOS will also enhance the products and programs delivered by ISVs and systems integrators.

## SteelCloud

SteelCloud, LLC, located in Ashburn, VA, makes "hard things simple" by turning "projects into products." We develop STIG-compliant products and tools to create plug-&-play solutions that focus on ease of deployment, STIG policy compliance, and high availability.



# SteelCloud<sup>®</sup>

*Simplifying Cyber Assurance*

**Brian H. Hajost**

President & CEO

T: 703.674.5561

M: 703.926.8291

[bhajost@steelcloud.com](mailto:bhajost@steelcloud.com)