



CYBERSECURITY **Compliance, Simplified.**

Automated STIG & CIS Remediation

SteelCloud®

Simplify Cyber Policy COMPLIANCE

Software applications are rarely designed to operate in government and commercial organizations that have mandated compliance requirements, so they get stuck on the starting line waiting months for the authority to operate (ATO). Meanwhile, system policies are manually adjusted on an application-by-application, system-by-system, and location-by-location basis. This process results in unplanned downtime or accepting a much higher cybersecurity risk, driving costs up and mission effectiveness down.

SteelCloud has been automating and remediating STIG/CIS policy compliance for over a decade. We knew there had to be a way to make the process easier, reducing the time it takes to harden systems for mandatory RMF compliance - thus freeing up critical technical resources. So, we invented it. The results have been nothing short of astonishing:

- ✓ Securing environments in hours, not weeks or months—routinely reducing the time to harden an environment around an application by over 90% and continual maintenance of cyber compliance efforts by more than 70%.
- ✓ Hardening the first DoD applications to get an ATO in the Amazon AWS commercial cloud.
- ✓ Delivering swift remediation in virtually every environment, including classified, tactical, weapon systems, SCADA, air-gapped labs, and the commercial cloud.
- ✓ Addressing RMF, NIST 800-171, and CMMC compliance requirements across Federal enterprises and their mission partners.
- ✓ Reducing timelines and labor requirements necessary to deliver compliant programs and infrastructures in every phase of the development to sustainment process.

Stun even the **most JADED** compliance professionals

The center point of SteelCloud's security solution is ConfigOS. ConfigOS is a patented software suite that allows anyone to quickly establish a STIG/CIS-compliant environment by automating remediation of security controls, dramatically simplifying an organization's most time and labor-intensive information assurance function. Eight out of the top ten federal integrators, along with major Civilian agencies, the Intelligence Community, the Department of Defense, commercial and technology vendors, all utilize ConfigOS to deliver policy compliance on their programs. The response remains the same—stunned.

ConfigOS takes two minutes to install, two hours to train, and then you're hardening systems around applications in an hour rather than the weeks or months it takes to harden systems manually.



ConfigOS 2 minutes to INSTALL
hours to TRAIN

ConfigOS allows a user to evaluate and harden STIG/CIS controls around an application, creating a securely “perfect” environment whether you’re working in Windows or Linux - on premise or Azure/AWS.



ConfigOS achieves similar results for any organization with secure policy requirements, including:

- ✓ Scanning a single endpoint or your entire infrastructure. With SteelCloud’s patented scanning engine, each instance of ConfigOS can scan 10,000-20,000 endpoints per hour – supporting the requirements of even the largest infrastructures.
- ✓ Remediating STIG or CIS security controls using your customized policies. With its patented remediation engine, each instance of ConfigOS can remediate 3,000-5,000 endpoints per hour.
- ✓ Reporting in an organized, easy-to-understand format. Customize and filter your results with our built-in-tools. Complete STIG Viewer checklist integration is at your fingertips, including the automatic entry of full finding details and waiver descriptions.
- ✓ Freeing up the workforce. Through massive manpower savings, ConfigOS allows for re-skilling, cross-training and re-deployment of talent across the enterprise.

Complete your **CYBER-HARDENING** in less than an hour.

If you want to achieve ATOs faster than you imagined possible, contact SteelCloud to see ConfigOS for yourself and become a believer. Time and again, users are shocked that it performs as advertised or better, and in awe of the savings it delivers in terms of time, manpower and budgets.



1.703.674.5500



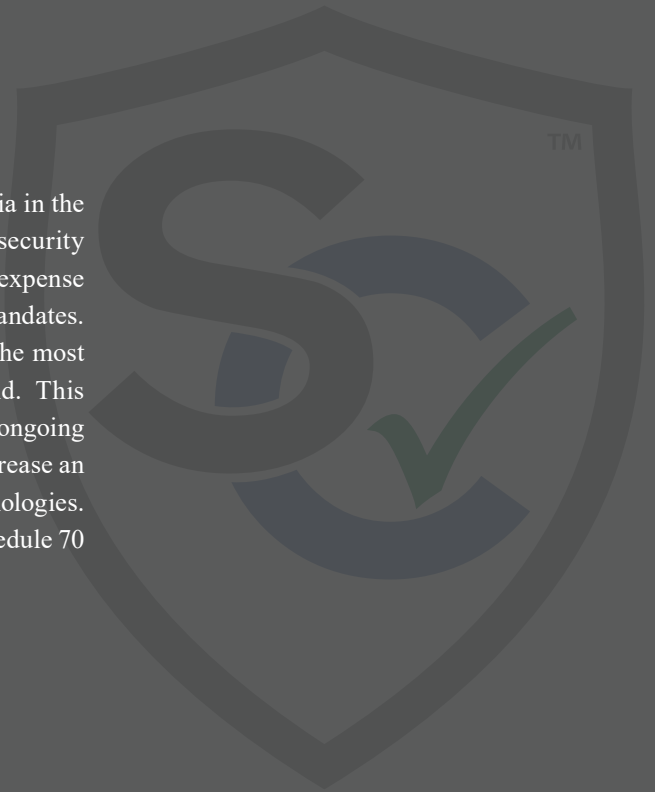
info@steelcloud.com

Simplify **CYBER COMPLIANCE** for any use case:

- RMF Risk Management Framework
- NIST 800-171
- NIST 800-53
- CCRI
- FedRAMP
- CMMC
- Cloud migration
- Air-gapped labs
- Classified
- DevOps
- Tactical
- SCADA

About SteelCloud

SteelCloud is a U.S. small business located in Northern Virginia in the metropolitan Washington DC area. We automate policy and security controls remediation by reducing the complexity, effort, and expense for meeting STIG, CIS and other government security policy mandates. SteelCloud's patented products have been proven in some of the most secure and policy-compliant organizations around the world. This confirms our ability to reduce hardening time by over 90% and ongoing STIG compliance costs by more than 70% and dramatically increase an organization's capacity to implement and accredit new technologies. SteelCloud's products are easy to license through our GSA Schedule 70 contract. For more information, visit [www:steelcloud.com](http://www.steelcloud.com).



SteelCloud

20110 Ashbrook Place, Suite 170 Ashburn, VA 20147

1.703.674.5500

info@steelcloud.com

steelcloud.com

Trademarks are owned by their respective companies.