SteelCloud

DATA SHEET

10 REASONS
to Automate STIG Compliance

How unified automation helps organizations reduce manual effort, preserve baseline integrity, and sustain cyber readiness.

Implementing Security Technical Implementation Guides (STIGs) across a complex environment requires significant time, expertise, and coordination. The work continues after the initial configurations are applied. STIG updates, system changes, customized policies, exceptions, and new assets must all be managed without compromising the integrity of the approved security baseline.

Unified automation gives organizations a more efficient and consistent way to manage these responsibilities across the STIG lifecycle.

Here are ten reasons to automate your STIG compliance program.

1. ACCELERATE STIG IMPLEMENTATION

Manually assessing systems, applying controls, and validating results can consume valuable time across an enterprise. Automation significantly accelerates these activities, helping organizations secure new and existing assets faster and respond more efficiently to mission requirements.

2. REDUCE MANUAL EFFORT AND COMPLIANCE COSTS

Repetitive implementation, remediation, validation, and documentation place a heavy burden on cybersecurity teams. Automation reduces the hours required per endpoint and limits the need for senior personnel to spend their time on routine compliance tasks. Organizations can use limited expertise, staffing, and budget more effectively.

Proven Customer Results

90% reduction in STIG effort	**93%** fewer hours required per endpoint	**62%** lower costs

3. IMPROVE ACCURACY AND CONSISTENCY

Manual processes can produce different results depending on the administrator, system, or point in time. Automation applies approved policies consistently and reduces the risk of human error, helping organizations achieve more predictable outcomes across their environments.

4. OPERATIONALIZE CUSTOMIZED SECURITY POLICIES

Published STIGs provide a strong starting point, but most organizations must tailor them to their missions, systems, and risk requirements. Automation helps teams turn those decisions into enforceable policies that account for approved waivers and exceptions and can be applied consistently across the environment.

5. UNIFY THE STIG COMPLIANCE LIFECYCLE

Disconnected tools and processes create additional work and make it harder to maintain a clear view of compliance. Unified automation brings policy management, scanning, remediation, validation, and reporting together, giving teams one coordinated approach to managing the entire STIG lifecycle.

6. PRESERVE BASELINE INTEGRITY

An approved baseline must continue to reflect the organization's operational and security requirements. Automation helps teams identify deviations, apply the correct policies, and return systems to their approved state before compliance drift becomes widespread.

7. RESPOND FASTER TO STIG UPDATES AND SYSTEM CHANGES

New STIG releases, software updates, system modifications, and infrastructure changes can quickly affect compliance. Automation enables organizations to evaluate those changes, update policies, and implement approved requirements more efficiently across impacted systems.

8. SCALE ACROSS COMPLEX ENVIRONMENTS

Large organizations may need to manage thousands of endpoints across multiple domains, enclaves, operating systems, and application types. Automation allows teams to implement and maintain approved policies at enterprise scale without increasing manual effort at the same rate as the environment grows.

9. STRENGTHEN VISIBILITY AND AUDIT READINESS

Preparing for an audit should not require teams to reconstruct months of compliance activity. Centralized visibility and reporting help organizations understand the current state of their systems, identify outstanding issues, and produce defensible evidence when an assessment occurs.

10. MAKE CYBER READINESS MORE SUSTAINABLE

STIG compliance is an ongoing operational responsibility. Automation helps organizations manage change, maintain baseline alignment, and address compliance requirements as part of regular security operations. The result is a more sustainable program that supports cyber readiness between audits and throughout the system lifecycle.

Sustain STIG Compliance with ConfigOS

SteelCloud ConfigOS unifies policy management, scanning, remediation, validation, and reporting to help organizations operationalize STIG compliance at scale. By automating work across the STIG lifecycle, ConfigOS reduces manual effort, preserves baseline integrity, and helps teams sustain a defensible security posture.

Learn how ConfigOS can make STIG compliance more efficient, consistent, and sustainable. Schedule a demo today!

SteelCloud
20110 Ashbrook Place, Suite 200 | Ashburn, VA 20147
1.703.674.5500 | info@steelcloud.com | **steelcloud.com**