SteelCloud

DATA SHEET

7 REASONS to Automate Your CMMC Program

Cybersecurity Maturity Model Certification (CMMC) is now part of the contracting landscape for the Defense Industrial Base. Contractors need to be prepared to meet the cybersecurity requirements applicable to the federal contract information (FCI) and controlled unclassified information (CUI) they handle.

ConfigOS can eliminate months of labor-intensive security configuration work by automating the implementation, remediation, and sustainment of security configurations across complex environments. Used throughout the federal government to support cybersecurity compliance at scale, ConfigOS helps contractors build a more sustainable approach to CMMC and NIST SP 800-171, better protect sensitive information, and support the cybersecurity representations they make to government customers.

Here are seven of the most valuable benefits of compliance automation:

1. **REDUCE THE SKILLS GAP WITHIN YOUR ORGANIZATION.**
   Finding experienced cybersecurity talent can be difficult and costly, particularly for organizations building a CMMC program from the ground up. Automating the technical implementation and sustainment of NIST SP 800-171 security requirements reduces reliance on manual expertise and helps existing teams manage compliance more efficiently.

2. **MINIMIZE THE COST AND EFFORT OF MEETING CMMC REQUIREMENTS.**
   Automating security configurations using established security content can reduce the time and cost associated with implementation. Instead of manually researching, applying, and updating configurations system by system, teams can consistently implement approved policies across their environments. This reduces both the initial effort and the ongoing work required to sustain them.

3. **IMPLEMENT AND SUSTAIN A COMPLIANT INFRASTRUCTURE.**
   Security configurations can drift as systems, policies, and operational requirements change. Automation helps teams apply approved configurations consistently, remediate deviations, and maintain a reliable baseline over time. It also produces repeatable results that can support self-assessments and other compliance activities.

4. **SUPPORT CONTINUAL COMPLIANCE ASSURANCE.**
   CMMC requires more than a point-in-time view of an organization's security posture. Systems, threats, and security guidance continue to evolve, making configuration management, remediation, and documentation ongoing responsibilities. Automation helps teams identify and address configuration drift while maintaining technical evidence of the work performed.

5. **SIMPLIFY SECURITY POLICY UPDATES.**
   Manually applying policy updates across complex environments takes time and can produce inconsistent results. Automation simplifies the process of ingesting, customizing, testing, and deploying updated security content, freeing teams to focus on higher-value security responsibilities.

6. **STANDARDIZE PROCESSES FOR CONSISTENCY.**
   Manual processes can introduce errors and inconsistencies, particularly when configurations must be applied across large or diverse environments. Automation creates repeatable, standardized processes that improve consistency and reduce operational risk over time.

7. **CENTRALIZE ONGOING COMPLIANCE MANAGEMENT.**
   Managing security configurations across disconnected tools and teams can increase costs, create gaps in visibility, and make compliance harder to sustain. Centralized management provides a clearer view of configurations, policies, deviations, and remediation activity across the environment.

Key Features of CMMC 2.0

CMMC Model 2.0	Model	Assessment
LEVEL 3 EXPERT	**110+** practices based on NIST SP 800-172	Triennial government-led assessments
LEVEL 2 ADVANCED	**110** practices aligned with NIST SP 800-172	Triennial third-party assessments for critical national security information; Annual self-assessments for selected programs.
LEVEL 1 FOUNDATIONAL	**17** practices	Annual self-assessments

Meet customer expectations for protecting sensitive information.

CMMC establishes three levels of cybersecurity and assessment requirements based on the type and sensitivity of information an organization handles. Contractors and subcontractors must understand which requirements apply to their contracts and implement the safeguards necessary to protect FCI and CUI.

ConfigOS helps organizations automate technical security requirements across applicable systems while documenting configuration, remediation, and policy activity for reporting and assessment support.

ConfigOS automates the implementation and sustainment of security configurations while documenting activity for reporting and assessment support. Using proven automation to maintain accurate configurations and address drift helps contractors demonstrate a disciplined, repeatable approach to protecting sensitive information.

Remain agile as requirements evolve.

Cybersecurity compliance requires an ongoing cycle of assessment, remediation, validation, and reporting. CMMC requirements and implementation timelines may continue to evolve, but contractors remain responsible for protecting sensitive federal information and meeting the requirements included in their contracts.

ConfigOS gives organizations a scalable way to implement and sustain security configurations as policies, systems, and operational requirements change.

Trust a proven unified automation solution for 800-171 compliance.

Federal organizations have used ConfigOS for years to automate security configuration management across complex environments. Defense contractors can apply that proven capability to the technical implementation, remediation, and sustainment work behind NIST SP 800-171 and their broader CMMC programs.

See how ConfigOS can simplify the technical work behind your CMMC program.
Book your free demo at www.steelcloud.com

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