SteelCloud

DATA SHEET

Typical Use Cases for SteelCloud's automated hardening solution, ConfigOS.

ConfigOS is SteelCloud's automated security policy remediation solution. This easy to implement software product is designed to simplify the process of achieving, maintaining, and continuously delivering a defect-free, policy-compliant environment. ConfigOS allows mission-critical software applications to perform reliably, while maintaining compliance with comprehensive security baselines.

In government and commercial environments, ConfigOS scans, identifies and remediates issues in significantly less time than by using manual processes. ConfigOS is agent-less and does not require changes to endpoint software stacks. SteelCloud designed ConfigOS to operate effectively in the most complex and secure environments. ConfigOS does not require internet connectivity, web servers, database servers, or license servers. It currently operates in cloud, lab and tactical environments; including both classified and unclassified networks.

The following use cases have been proven in some of the world's demanding computing environments.

Accelerating Risk Management Framework (RMF)

ConfigOS is the best tool for automating the entire STIG process – from adapting policy, documenting waivers, and integrating with government tools, such as STIG Viewer. It decreases the effort required to manually establish & maintain continuously compliant, defect-free environments by over 90%. ConfigOS impacts the RMF effort by:

- ✓ Simplifying the process of testing and hardening STIG controls around an application stack;
- ✓ Documenting the controls that have conflicts with the application stack and need to be waivered;
- ✓ Creating RMF artifacts and integrating this information into STIG Viewer;
- ✓ Setting up an ongoing methodology to continuously keep systems in compliance by automating remediation

Protecting controlled, unclassified information NIST 800–171/CMMC

The protection of controlled unclassified information (CUI) that resides in contractor systems is of paramount importance to the DoD, and directly impacts the ability of the federal government to protect its sensitive information. Currently, ConfigOS is currently being used by government contractors to achieve NIST 800-171 compliance required by the Defense Federal Acquisition Regulation Supplement (DFARS). As the DoD rolls out the Cybersecurity Maturity Model Certification (CMMC) starting in 2020, security policy compliance will become even more pressing, as RFIs/RFPs will require audited CMMC compliance by those organizations wishing to bid.

Safeguarding diverse computing systems by achieving NIST 800-53 compliance

ConfigOS offers a proactive and systematic approach to bringing and keeping systems into compliance with NIST 800-53 controls. Addressing the acceleration of upfront RMF activities as well as ongoing compliance maintenance, ConfigOS was designed to automate compliance in every phase of a program's development, delivery, and sustainment process. The net result is more complete and consistent results for every program, in every environment. By simplifying STIG compliance, users benefit by achieving more secure and more resilient environments.

Helping deliver compliant infrastructures with Continuous Diagnostics & Mitigation (CDM)

In support of government-wide and agency-specific efforts to provide adequate, risk-based, and cost-effective cybersecurity, the Department of Homeland Security (DHS) established the Continuous Diagnostics and Mitigation (CDM) Program. The CDM program coordinates approval and adoption of cybersecurity tools, integration services, and dashboards to participating agencies who are looking to:

- ✓ Reduce agency attack surface
- ✓ Increase visibility of key cyber-hygiene shortfalls
- ✓ Improve federal cybersecurity response capabilities
- ✓ Streamline Federal Information Security Modernization Act (FISMA) reporting

ConfigOS is on the CDM approved product list (APL) and is currently provided through the CDM GSA schedule.

Facilitating compliance while reducing effort Command Cyber Operational Readiness Inspection (CCRI)

Since its inception, the Command Cyber Operational Readiness Inspection (CCRI), focuses on evaluating an organization's compliance with the Department of Defense security orders and directives; assessing network vulnerabilities; and analyzing 3 levels of effort to review operational risk: mission, threat, and vulnerabilities. ConfigOS automates the process of establishing a secure baseline, passing a CCRI audit and maintaining a security compliant, defect-free environment. During that time, ConfigOS delivers a 70% reduction in the time, effort, and manpower that system integrators, defense contractors and government entities need to remain STIG compliant.

Supporting FedRAMP and accelerating cloud migrations

For over 5 years, ConfigOS has been used by government organizations and their mission partners to accelerate their cloud migration efforts. SteelCloud's patented software quickly hardens cloud infrastructures and produces the compliance artifacts necessary to support FedRAMP and RMF initiatives in the fraction of the time and effort required by traditional methods.

Operating in the most sensitive environments Air-Gapped Labs, Portable & Modular Data Centers, and Sensitive Compartmentalized Information Facilities (SCIFs)

Because ConfigOS has been designed to operate without access to the Internet, it is well suited to automate security policy compliance for virtually any air-gapped environment. Additionally, ConfigOS runs on a single physical/virtual system and does not require the installation of clients or agents. It provides an extremely light-weight footprint within these sensitive IT environments. Being both "self-contained" and "clientless", ConfigOS is perfect for:

- ✓ Tactical applications where installing software on endpoints is not possible
- ✓ Agile lab environments
- ✓ SCADA implementations
- ✓ Classified networks

Enabling secure development and maintenance DevOps

ConfigOS has the singular, unique capability of providing automated assessment and automated STIG remediation across all infrastructures and phases of your DevOps process. Supporting compliance within both legacy and new development environment, ConfigOS provides for the rapid set-up, test, and tear down of security policies. Additionally, security controls can be inherited across processes and infrastructures. ConfigOS reduces the effort and ensures the security of every phase of the DevOps process:

- ✓ Planning
- ✓ Coding
- ✓ Developing
- ✓ Testing
- ✓ Releasing
- ✓ Deploying
- ✓ Operating
- ✓ Monitoring

SteelCloud
20110 Ashbrook Place, Suite 170
Ashburn, VA 20147
1.703.674.5500
info@steelcloud.com | **steelcloud.com**

For more information on ConfigOS Command Center and to see a short product demo, visit us at
https://www.steelcloud.com/configos-cybersecurity/