SteelCloud
AUTOMATING STIG & CIS COMPLIANCE

ConfigOS® MPO

Concept of Operations

Version 2.00

Last revised: *December 8, 2023*

Contents

1 Executive Summary

Maintaining Security Technical Implementation Guide (STIG) and Center for Internet Security (CIS) compliance is a challenging and costly task for government and commercial systems. The tedious and manual nature of the work requires specialized skills and security clearance. This can result in long hours and increased expenses for system administrators, hindering mission effectiveness and agility. Compliance operations face new challenges with the growing number of mobile workers, bandwidth-constrained networks, and increasing control policies for large-scale environments.

To address these issues, SteelCloud's ***ConfigOS MPO Suite*** offers an automated *Continuous Compliance at Scale* solution for maintaining a STIG and CIS-compliant cybersecurity environment. This solution removes months from the RMF cycle and manages complex policies and slow connections that are common with mobile workforces in large-scale network environments. ConfigOS MPO helps organizations achieve RMF closed-loop compliance with STIG/CIS standards through a set-and-forget approach. ConfigOS MPO includes policy content management, detection, and remediation automation for mainstream operating systems and application stack components. It is easy to use and customize, allowing you to perform automated enterprise-wide compliance auditing, scanning, remediation, and reporting.

ConfigOS MPO can be implemented in various environments, including classified, tactical/weapon systems, air-gapped labs, OT/SCADA environments, and commercial cloud infrastructures. You can achieve high compliance rates with continuous monitoring and compliance. The flexible infrastructure tree view allows for easy group management and drag-and-drop operations, with visual icons and colors to enable easy management, fixing, evaluation, rollback, and reporting of endpoints. ConfigOS MPO tracks what endpoints are on and off the network while ensuring each has the proper policies and schedules. ConfigOS MPO helps drive compliance throughout every stage in the development, authorization, and operations process.

2 Purpose and Intended Audience

This document acts as a Concept of Operations guide for potential SteelCloud customers. It was created for IT compliance decision-makers, compliance operation managers, system administrators, and anyone else involved in the planning, evaluating, and deploying of ConfigOS MPO. SteelCloud also maintains reference articles and videos on our website (https://www.steelcloud.com/).

3 Objectives and Requirements

3.1 Challenges

Traditionally, organizations begin their STIG compliance operations by building up operation teams and manually implementing STIG policies in their environments. They soon realize the following challenges:

1. Managing STIG compliance is a complex and expensive process. Organizations must hire and maintain technical experts with a combination of operating system knowledge and policy expertise. The tasks involved in maintaining a STIG-compliant environment are repetitive and time-consuming.
2. Some organizations use Microsoft GPO to implement STIG policies. However, GPO does nothing to confirm that compliance is being effectively applied.
3. The Defense Information Systems Agency (DISA) regularly publishes updates to STIG policies, and organizations must implement a process to ensure their policies are up-to-date and implemented in a timely fashion. This requires a systematic approach to policy management and an understanding of the implications of any policy changes.
4. Each system has its own unique set of controls that must be adapted or "tuned" for the organization. Waivers must be documented and approved for each non-compliant control that has been relaxed or ignored.
5. Large enterprises and agencies often struggle to maintain continuous STIG compliance due to the inherent complexity of their network environments and mobile workforce. Despite having centralized compliance operations in place, they often face significant challenges when dealing with large-scale and complex systems.

3.2 Automated Solution Requirements

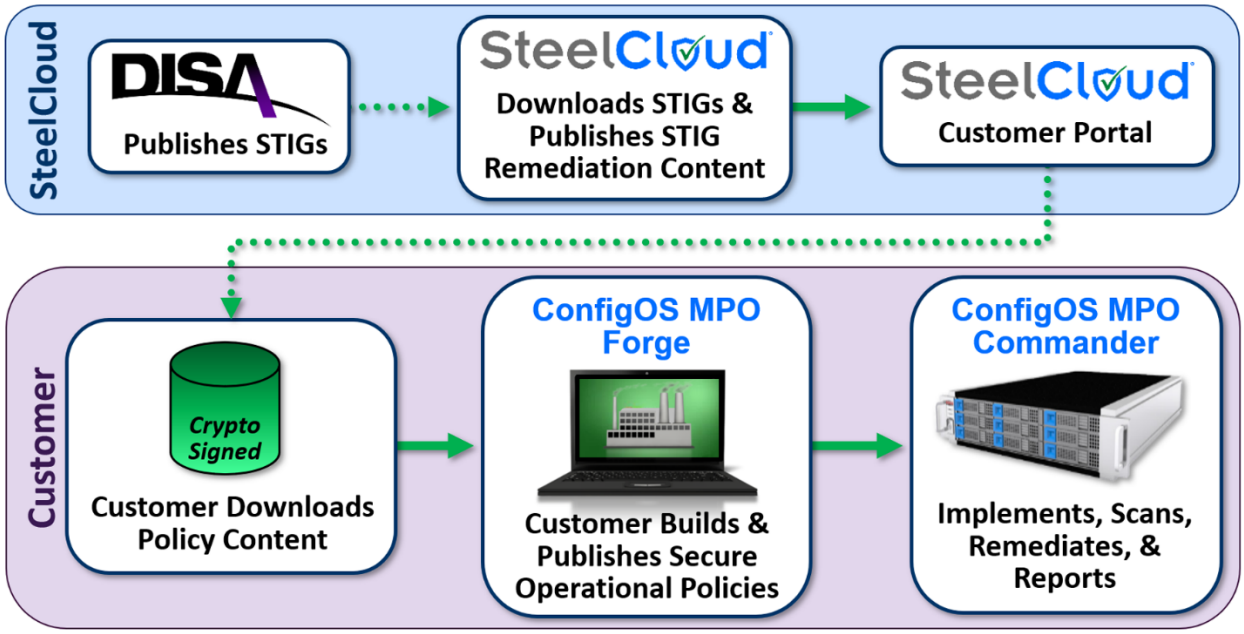
To support continuous compliance at scale efficiently and cost-effectively, the market demands an automated solution that can address the following requirements:

1. Efficiently managing the ongoing STIG policy updates is critical for organizations to comply with security regulations. The automated solution should offer a policy workbench tool that allows organizations to maintain their customer baseline policies, operational policies, waiver documentation, version control, workflow management, and more.
2. The automated solution should offer a secure policy compliance tool that enables organizations to manage the initial endpoint setup and ongoing scanning, remediation, and reporting operations with minimal human interaction.
3. The automated solution should address the complex demands of managing large-scale and complex network environments, as well as mobile workforces. The solution should provide a policy compliance tool that can adapt to different network infrastructures and provide reliable compliance operations for mobile devices used by the workforce.
4. A comprehensive compliance reporting and monitoring tool is crucial for organizations to maintain an up-to-date view of their compliance status. The automated solution should provide a holistic view of the organization-wide compliance status, including historical data, and enable organizations to monitor and report their compliance from different viewpoints.

4 Compliance Operation Process

To achieve compliance objectives, organizations must establish a clear and effective compliance operation process that outlines the roles and responsibilities of all stakeholders. While the process presented here provides a generic example, organizations should customize it to align with their needs and requirements. By doing so, organizations can ensure their compliance operation process is effective and efficient, allowing them to maintain compliance with regulatory requirements and protect their information systems from security threats.

SteelCloud's ConfigOS solution is based on the following workflow:



1. **DISA publishes STIG updates.** These quarterly policy updates provide structured guidelines for securely building and maintaining vendor-specific systems and software.
2. **SteelCloud publishes an updated SteelCloud Baseline Policy Collection.** SteelCloud's support team maintains a SteelCloud Baseline Policy Collection that includes all STIG/CIS benchmarks supported by ConfigOS.
3. **Customer downloads the collection from their SteelCloud customer portal account.** SteelCloud provides a fast turnaround time to deliver the updated baseline policy collection after receiving the STIG update notice from DISA.
4. **Customer's policy management team creates customer baseline policies and operational policies.** Using the SteelCloud Baseline Policy Collection as a starting point, the policy management team uses MPO Forge to create operational policies tailored to specific application stack segments of the organization. They can also include waiver documents and approvals for non-compliant controls in the collections.
5. **Customer's compliance execution team manages endpoints and their continuous compliance execution.** The compliance execution team uses MPO Commander to manage the continuous compliance execution for the organization's endpoints. The team updates Commander with the latest operational policies, assigns the policies to endpoint groups, and

schedules scanning and remediation jobs. Commander automatically propagates these changes to all paired Shields, which execute scan and remediation jobs according to their continuous monitoring schedules atomically, with or without the network connections. Eventually, all Shields will send their compliance data back to their prescribed Commander.

6. **Customer produces compliance reports.** The customer's compliance reporting team uses the Client to access Commander and generate compliance reports for eMASS or SIEM such as DashView. These reports provide insights into the organization's compliance status, enabling the team to take corrective actions as necessary.

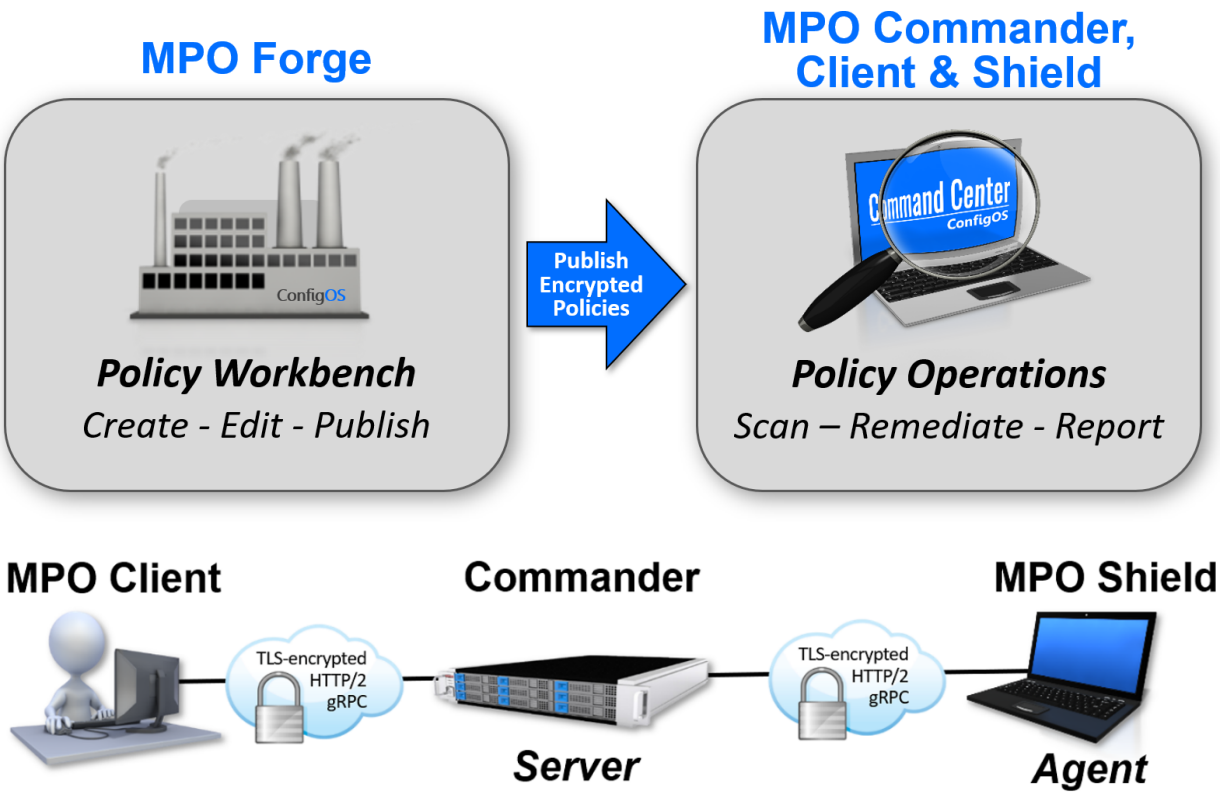
5 System Description

ConfigOS MPO is SteelCloud's patented compliance software suite that allows you to quickly establish a STIG or CIS cybersecurity-compliant environment. SteelCloud developed the ConfigOS MPO suite to help organizations efficiently manage their baseline and operational policies, quickly harden policy controls around their application environments, and keep systems in compliance with the latest security policies at the lowest possible effort and cost. Agent-based compliance automation addresses the market demand for managing large-scale and complex network environments, mobile workforce, and continuous compliance monitoring.

For government customers or those organizations that want to maintain STIG or CIS-compliant systems, SteelCloud provides frequently updated Baseline Policy Collections for users to download. SteelCloud Baseline Collections are machine-executable versions of the DISA STIG and CIS policies.

5.1 Application Architecture and Key Components

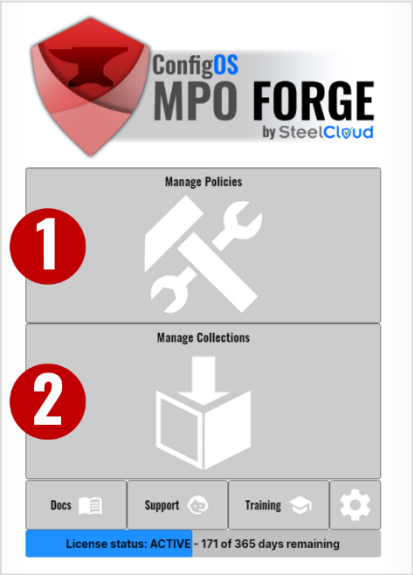
Forge	Allows you to manage your baseline and operational policies and generate policy collections for Commander. Provides internal workflow management, revision management, and automated STIG/CIS updating of operational policies.
Commander	The backend server that works with Shields to automatically register endpoints, exchange policies, continuous compliance automation schedules, and aggregate hardening results. Can only be managed through a Client.
Desktop Client	The Commander console that allows you to manage endpoints, set up compliance automation schedules and policies, manage users, and monitor the compliance automation results.
Shield	A Windows service, installed on endpoints, that works with Commander to provide automated hardening service and continuous compliance monitoring operations.



5.2 Forge

Forge is a policy management workbench that allows you to do the following:

1. Import SteelCloud baseline policies.
2. Create and manage customer baseline policies and operational policies.
3. Tune, edit, and extend existing policies.
4. Split a larger policy into smaller parts to determine which policies need to be adjusted to allow an application environment to run properly.
5. Create and manage the policy collections.
6. Manage the policy collection by using the built-in workflow status and version control.
7. Select the policies and control files (*e.g.,* policy documents, work instructions) to be included in deployment collections.
8. Export the deployment collection into a single data file that can be processed by the pairing Commander(s).



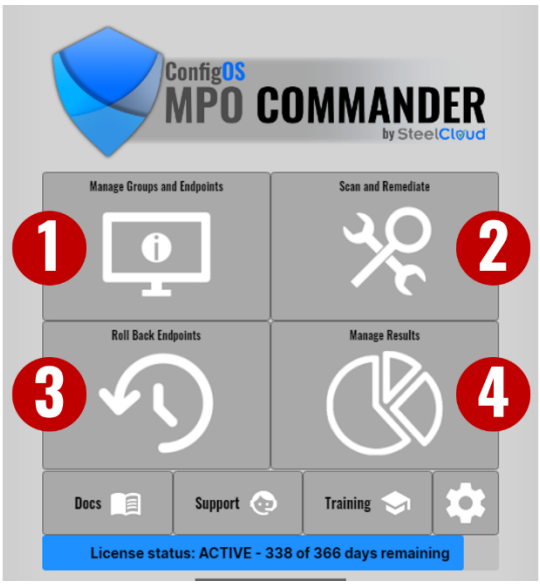
You usually perform the following workflow to create customer baseline policies, customer operational policies, and an operational deployment collection data file.

1	**Manage Policies**	Allows you to upload new SteelCloud baseline policies, as well as create and manage customer baseline and operational policies.
2	**Manage Collections**	Allows you to create a new policy collection by adding from baseline and operational policies and user-created documentation files. You can create policy collections by following the built-in workflow process.

5.3 Commander

Commander is a high-performance server that does the following:

1. Grant multiple concurrent users access, via Clients, to manage the hardening operations.
2. Allow you to import the policy collections from the paired Forge.
3. Allow Shields to self-register their hosted endpoints automatically.
4. Automatically distribute the latest policy collection to its paired Shields.
5. Automatically distribute the latest continuous compliance monitoring schedule to its paired Shields.
6. Provide continuous compliance monitoring through Shields' automated hardening and reporting.
7. Allow you to manually harden endpoints using STIG or CIS policies.
8. Allow Shields to report all hardening results.



After creating your policies and collections in Forge, you can proceed to the Commander landing page.

1 Manage Groups and Endpoints	Allows you to manage both groups and endpoints. Endpoints are the IT assets with Shields installed and have registered themselves onto Commander's Infrastructure Tree. Endpoints can be organized into groups by location, application type, or shared policies.
2 Scan and Remediate	After endpoints are set up, Shields deployed on endpoints run performance scan and remediation jobs automatically without human interaction. You can also use the *Scan and Remediate* screen to manually scan and remediate selected endpoints, roll back remediations, and view reports.
3 Roll Back Endpoints	Holds a complete history of available remediation rollbacks. From here, you can restore endpoints to a known good policy configuration. Rollbacks are sequenced, and Commander processes them in the correct order.
4 Manage Results	Reports endpoint compliance results. You can export results as JSON files; eMASS output files, or a STIG Viewer CKL file.

5.4 Desktop Client

Desktop Client grants you remote access to Commander, where you can do the following:

1. Manage user accounts (if you are an admin user).
2. Manage endpoints and groups.
3. Manually harden endpoints using STIG or CIS policies.

5.5 Shield

Shield is a Windows-based service you can silently install on an endpoint and manage its compliance automation. Agent-based compliance automation addresses the market demand for managing large-scale and complex network environments, mobile workforce, and continuous compliance monitoring.

Shield offers the following capabilities:

1. Automatically contact its paired Commander to self-register the hosted endpoint (*beacon capability*).
2. Continuously notify its paired Commander that the Shield is connected to the network (*heartbeat capability*).
3. Automatically receive and update the latest policy collection from its paired Commander.
4. Automatically receive and update the latest scan and remediate automation schedule.
5. Provide continuous compliance monitoring and hardening through its automation schedule.
6. Manually harden endpoints using STIG or CIS policies.
7. If offline, automatically save all hardening results to its local database.
8. When online, automatically reports the saved hardening results to its paired Commander.

5.6 Security

ConfigOS MPO is designed to be deployed on-premises within a customer's network environment, and all data is only communicated between Commander, Client, and Shields through TLS-encrypted HTTP2. This ensures data is protected in transit, and you have full control over the security of your data.

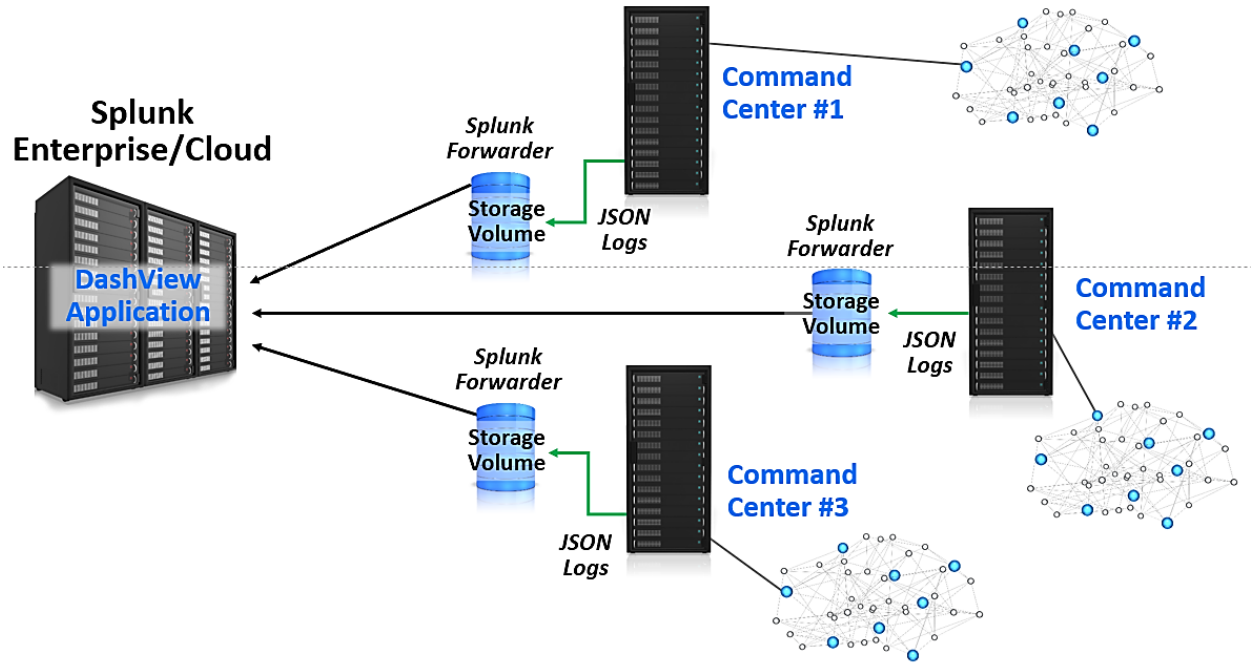
The security mechanisms within ConfigOS MPO provide additional safeguards to ensure it is used in a secure and controlled manner. For example, during installation:

- Forge creates a *Forge Pairing Key* to bind itself with Commanders. This ensures that data installed with the Commanders cannot be used to create rogue Forge instances or unverified policy content. The binding process binds to the Commander itself rather than the machine where Commander is installed. Forge signs the policies in its generated deployment baseline collections, which can only be used by the bound Commanders.
- Commander creates a *Client Pairing Key* to bind itself to Clients and a *Shield Pairing Key* to bind itself to Shields. This ensures that only authorized Clients and Shields can communicate with this Commander.

ConfigOS MPO has undergone thorough testing and certification by a third-party penetration test provider to ensure it meets industry-standard security requirements. These security mechanisms assure customers their data is secure, and they can use ConfigOS MPO in a secure and controlled manner.

5.7 DashView

DashView is an advanced compliance dashboard that SteelCloud delivers as a commercial off-the-shelf application to install on any Splunk infrastructure – Enterprise or Cloud. DashView provides a detailed hierarchical view of data, including enterprise, location, system, policy, and control. Dashboards also provide a "horizontal" view of data across operating systems and application stacks. You can also view waiver information across your enterprise. All data can be viewed across time, and compliance "heat maps" are included.



Splunk's standard forwarders combine data from multiple locations into DashView, which parses and ingests Commander's standard JSON output.

6 Stakeholder Roles and Responsibilities

Organizations can assign various user roles and responsibilities to effectively manage their compliance operations. The following roles are defined to ensure a streamlined compliance process:

Policy Management	Responsible for creating and maintaining an organization's compliance policies. Understands the organization's overall compliance requirements and uses Forge to create baseline policies and operational policies.
Compliance Execution	Responsible for executing compliance operations on endpoints within an organization's environment. Uses Commander and Client to set up initial endpoints and run manual scanning, remediation, rollback, and reporting jobs.
Compliance Reporting	Responsible for monitoring compliance results and providing compliance status reports. Uses Commander and Client to create different types of reports according to the requirements, such as generating eMASS and JSON files.

7 Additional Operational Scenarios

The following are examples of additional ConfigOS use cases beyond typical enterprise implementation.

RMF accreditation and ATO acceleration	To obtain an Authorization to Operate (ATO), organizations must complete multiple tasks, including documentation and system hardening. Traditionally, system hardening is a highly specialized manual process that can take weeks to accomplish. ConfigOS streamlines this process, reducing it to about an hour. ConfigOS not only accelerates the hardening process but also documents the results in a policy that can be used to automate consistent replication of the results across infrastructures. This makes it easy to transfer policies approved in the accreditation process to the production environment for ongoing assessment, remediation, and reporting. By using ConfigOS, organizations can reduce accreditation timelines by one to two months, ensuring compliance with Risk Management Framework (RMF) guidelines while streamlining the ATO process.
Gold disk support	While *gold disks* help implement new systems quickly, they do not address the ongoing cost and effort of keeping systems updated with the latest policies. ConfigOS is a great complement to a gold disk program because it enables simple policies to be published to keep systems updated with the latest policies. Over time, ConfigOS helps maintain policy compliance more efficiently and cost-effectively than relying solely on gold disks.
Mission partner support	Coordinating testing and deployment across multiple environments can be a challenge. ConfigOS makes it easy to include policies with applications as they move between different mission partners and infrastructures. Using ConfigOS, policies and configurations can be replicated and maintained as systems progress from development to accreditation and production. ConfigOS is lightweight and inexpensive, making it simple to implement across different mission and technology partners. ConfigOS secure policy collections can be easily transported with applications, making it quick and easy to implement compliance in application-specific environments.
CMMC/NIST 800-171 compliance	ConfigOS is a straightforward solution for DoD contractors to meet CMMC/NIST 800-171 compliance requirements. Contractors can quickly scan and fix non-compliances while hardening STIG/CIS controls around an application baseline. ConfigOS automates the compliance process, reducing the time and complexity involved in meeting the CMMC control mandate.
Software/technology product delivery	ConfigOS simplifies the process of commercial off-the-shelf software vendors ingesting compliance policies. Vendors can evaluate and develop their products to government standards using a simple policy collection. The policy can also document any waiver requirements for the products, allowing customers to automate installation and testing. ConfigOS helps vendors and their products become "STIG-ready."

Cloud migration and policy maintenance	ConfigOS is a lightweight solution that facilitates STIG compliance in commercial cloud environments. It can be used for even the smallest cloud prototypes and has been successfully implemented in commercial cloud environments such as MilCloud, GovCloud, AWS, and Azure.
Critical infrastructure	ConfigOS is a great solution for ensuring compliance in non-traditional computing environments like critical infrastructure, which can be difficult and expensive to harden using traditional methods.
Weapons and tactical systems	Like critical infrastructure, weapons systems incorporate many IT resources outside the mainstream of traditional enterprise IT. Organizations increasingly recognize the imperative to protect these assets. ConfigOS has been used extensively to address all non-traditional IT areas—from tactical/training/weapon systems to SCADA and industrial controls.

8 Implementation

When evaluating how ConfigOS MPO addresses compliance requirements, organizations should consider multiple implementation factors to determine the right number of MPO application instances.

8.1 Forge

Forge allows organizations to create and customize policies separately from their operational scanning and remediation processes. This separation creates an audit trail between policy creators and users, thereby enhancing security and control. Forge creates policy collections that can easily be moved between different network domains. The number of Forge instances required depends on the number of staff members involved in creating and publishing policies, organizational complexity, and the number of unique policies supported. While Forge and Commander can be deployed on the same system for smaller implementations, they are typically deployed on separate systems. Forge logs policy creation activity for auditing and tracking purposes.

8.2 Shield

Shield is a Windows-based service you can deploy silently to all endpoints in your organization. The deployment can be done using various solutions, such as Microsoft System Center Configuration Manager (SCCM), without any disruption to end users.

Once a Shield is deployed, it automatically registers itself into the Commander prescribed for it. This ensures the Shield is managed and monitored by that Commander, providing a centralized approach to synchronized policies, continuous compliance schedules, and compliance operation results.

8.3 Commander

Commander is a versatile and lightweight security tool you can easily install based on your organization's specific needs. It can run on workgroups and standalone systems and is not tied to any specific platform or security domain. Commander is a high-performance tool that is typically implemented based on operational and security considerations, rather than volume. This ensures it is deployed effectively to address specific security risks and compliance requirements. Organizations are licensed to install instances of ConfigOS anywhere a Windows endpoint has been licensed, providing them with greater flexibility in deploying and managing the tool.

To determine the optimal number of deployed instances of Commander, consider these key factors:

Total number of endpoints	Includes all Shields paired with a Commander. Although a Commander no longer has to perform scanning and remediation jobs for all its endpoints, it is still responsible for registering all its prescribed Shields, managing initial Shield setup, and providing initial and ongoing configuration updates to its Shields. A Commander is also the central point for receiving and aggregating all the compliance statuses sent back from each Shield.
Total number of policies applied to endpoints	For instance, an infrastructure with 500 server endpoints may only have two policies applied to each endpoint, resulting in a total of 1,000 policies applied during scanning/remediation. Conversely, 200 workstations with a dozen policies each would generate 2,400 total policies.
Scan/remediation frequency	Impacts the storage capacity of a Commander, particularly at higher endpoint counts. The frequency of processing is determined by the organization's business and security requirements.

Also, consider the following when planning an organization’s ConfigOS MPO implementation:

Security boundaries	Commander does not require domain services or Internet access. Licensing does not dictate the number of instances of Commander you can deploy. Typically, clients do not have an economic incentive to “pierce” protected networks to reduce the number of Commander instances. Policies are published as collections that can easily be moved around an organization (physically or electronically) to the instance of the Commander where they are to be used.
Standalone systems	Commander can be loaded and run directly on standalone Windows workstation and server endpoints. Commander can also run on a laptop and scan and remediate standalone Windows systems via standard network cable connection.
AD/GPO best practices	While Active Directory (AD) is a widely used tool in Microsoft infrastructures, extending Group Policy (GPO) for STIG compliance can be complex and challenging. GPO lacks certain features, such as rollback and Linux support, and organizational separation between AD/GPO and systems administration functions can lead to conflicts and added complexity. ConfigOS is a complementary technology that simplifies GPO implementation and automates STIG compliance across the DevOps lifecycle. GPO should be used for top-level controls common across all applications, while ConfigOS manages the complete control stack with agile reporting and interfaces to STIG Viewer. ConfigOS-specialized GPO conflict reporting helps keep GPO and ConfigOS aligned.
Policy publishing	SteelCloud designed ConfigOS to enable organizations to safely publish policies with minimal effort. Policy collections use client-specific ECDSA-signed and AES 256-encrypted keys, providing protection and ensuring that approved policies are secure and unaltered. This security measure allows you to use these policies in any environment, such as classified, tactical, and weapons systems, without fear of data breaches.

9 Support

SteelCloud's customer care team provides exceptional support services to both government and commercial customers, as well as technology partners. Our goal is to ensure that our customers achieve the highest level of productivity from their ConfigOS deployment. We offer a range of support activities that can be easily managed through our customer access portal, including:

Training Programs	Our comprehensive training programs are designed to provide in-depth knowledge and understanding of the ConfigOS platform. We offer hands-on training to give customers the confidence to use our product to its full potential.
Support tickets	If you need technical support or have any questions about licensing, billing, or customer access portal support, you can easily submit a support ticket. Our customer care team will respond promptly to provide the assistance you need.
Secure software download	We provide each customer with unique credentials and easy-to-follow instructions on how to safely download our software, policy collections, and product documents through our customer access portal. With our secure download process, you can be confident that you are getting the latest and most reliable version of our software.

At SteelCloud, we are committed to providing top-notch support services to our customers. Our customer access portal is designed to streamline your support experience, making it easy for you to get the help you need when you need it.

10 About SteelCloud

SteelCloud develops STIG and CIS compliance software for government customers and those technology providers that support the government. Our products automate policy and security remediation, reducing the complexity, effort, and expense of meeting government security mandates. SteelCloud has delivered security policy-compliant solutions to military components around the world that simplify implementation and ongoing security and mission support. SteelCloud products are easy to license through our GSA Schedule 70 contract. SteelCloud can be reached at **(703) 674-5500**. Additional information is available at www.steelcloud.com or by email at info@steelcloud.com.