SteelCloud®

AUTOMATING STIG & CIS COMPLIANCE

ConfigOS®

Concept of Operations

Automating Policy Compliance

Version 4.2

ConfigOS Rel. 2.8.4

December 2021

www.steelcloud.com **20110 Ashbrook Place, Ashburn, VA 20147** **703-674-5500**

SteelCloud
AUTOMATING STIG & CIS COMPLIANCE

ConfigOS Concept of Operations

A. Background

The Department of Defense (DoD) protects its thousands of networks by defining, implementing, and auditing best practices to install and maintain its information technology resources. The Defense Information Systems Agency (DISA) develops and publishes policies in the form of the Security Technical Information Guides (STIGs), which are used when hardening secure systems used in the DoD. While significant advances have been made in the areas of threat definition and vulnerability monitoring, there has been significantly less strategic effort around the arduous task of automating STIG remediation.

SteelCloud has been automating STIG compliance in the DoD for over 12 years. Having delivered and supported STIG-compliant technologies across the DoD and its mission partners and in major civilian agencies, SteelCloud has seen the operational issues involved in creating and supporting secure environments that support mission goals. Over this time, SteelCloud has developed a patented, easy-to-implement tool that will mitigate risk and reduce the cost of supporting applications in government-mandated secure environments.

B. Defining the Problem

It is widely recognized that supporting STIG-compliant environments is expensive and may impede agility and mission effectiveness. It is expensive because system STIG maintenance is time-consuming for systems administrators. STIG compliance is also tedious, as it is typically done on a system-by-system, application-by-application, and site-by-site basis thousands of times a day throughout the government. STIG maintenance also requires a high level of operating system knowledge and experience combined with policy expertise. Hiring people with the right combination of skills may be difficult, a situation exacerbated by the need for security clearances in some cases.

On its own, STIG compliance is not the cause of these concerns. If the same policies and configurations could be implemented on all systems, STIG compliance would be a rather straightforward exercise. Unfortunately, commercial and government-developed applications react to security policy differently. The controls for each system, therefore, must be uniquely adapted or “tuned.” Waivers are typically documented and approved for each non-compliant control that has been relaxed/ignored.

The problem, therefore, is not creating and maintaining secure, compliant environments. The problem is creating and maintaining secure, compliant environments where software applications will actually run reliably. Making software work in secure environments defines the intersection of operations/missions and security. SteelCloud has developed ConfigOS to address the problem of automating this intersection—by creating and maintaining secure, compliant environments specific to each application.

An effective solution really comes down to leverage. How can something be done right once and then be replicated across a government or contractor enterprise dozens, hundreds, or even thousands of times? The more times that a piece of automation can be replicated, the

greater the opportunity for cost savings and uniformity. This is the key to the leverage that ConfigOS provides - a simple signature that can be easily developed once and then used securely across enterprises, in all networks and domains, with little training and no changes to security, networks, or infrastructure.

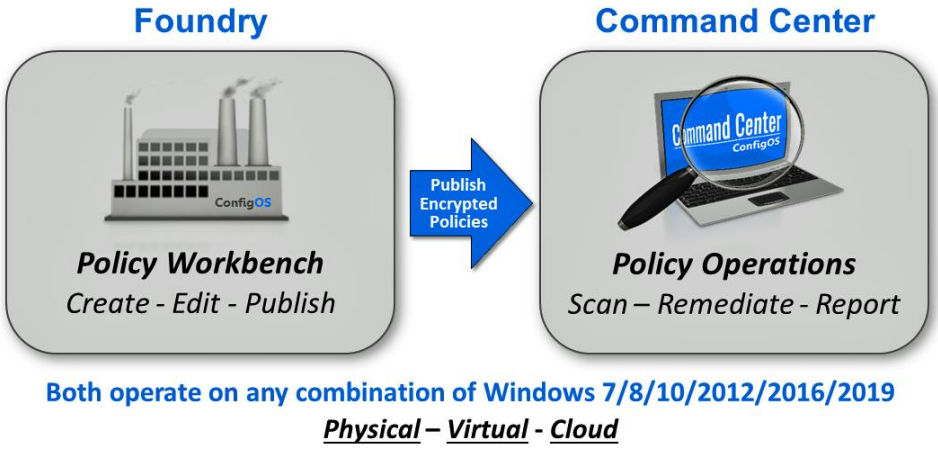
C. Enterprise Solution

To define an enterprise solution, one needs first to define an enterprise. For example, in the DoD, an enterprise might represent an individual program, a component, or merely a single base, network, or domain. Or, does "enterprise" refer to the entirety of the DoD? Assuming that the definition stands as the entirety of the DoD creates issues with typical enterprise solutions. Commercial enterprise solutions were developed around the corporate model of computing, including a single or a few domains, data centers, or networks. In contrast, the DoD's infrastructure is significantly more fractured, decentralized, and complex—including security domains.

Enterprise technologies do not need to be installed centrally with ubiquitous access to endpoints to enforce standards and provide consistency across the enterprise. ConfigOS was developed to provide "enterprise" capabilities across complex organizations, such as the DoD, without requiring unnatural changes to the enterprise's infrastructure. ConfigOS provides for security and capability consistency that can be controlled at any level within an enterprise (no matter how it is defined), without the requirement for connectivity or access.

D. ConfigOS – Security Overview

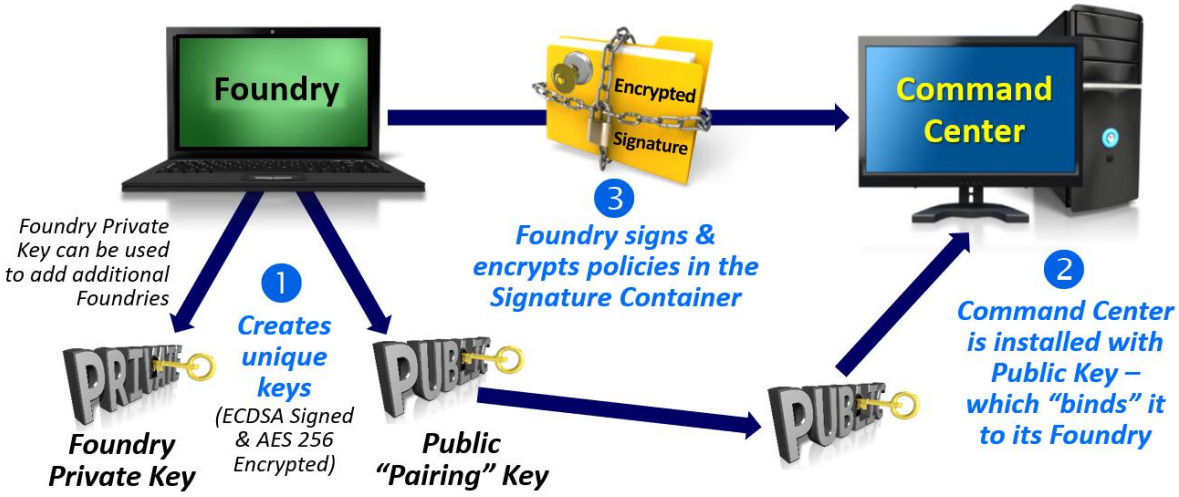
The ConfigOS solution incorporates two distinct pieces of software—Foundry and Command Center. Command Center performs all of the production functions of ConfigOS, including scanning, remediation, and reporting. Foundry is an information assurance (IA) workbench that allows organizations to tailor policies to their applications and environments and then publish secure policy containers incorporating those policies. Therefore, an organization may have dozens of Command Center installations supporting hundreds or thousands of endpoints, all supported by just one or a handful of ConfigOS Foundries. The number of Foundry instances are determined by the desired publishing control points within the enterprise rather than by capacity or throughput.



The security mechanisms within the ConfigOS solution ensure that a set of Command Centers can use only policy content from its prescribed Foundry instance(s). Upon its installation, the ConfigOS Foundry utilizes a FIPS-compliant random number generator, along with a user passphrase, to create an Elliptic Curve Digital Signature Algorithm (ECDSA) key pair for data signing, and a 256-bit key for AES encryption. The Foundry Private Key is used to install one or more Foundry instances, and the private key's corresponding public key is used to bind installed ConfigOS Command Center instances to that Foundry. The binding process occurs on installation of the Command Center.

Because the public key cannot be used to derive its private key, this approach ensures that the data installed with the Command Center cannot be used to create "rogue" Foundries or unverified policy content. The binding process binds to the installation of the Command Center rather than the machine where Command Center is installed. This allows ConfigOS to be preinstalled as part of an image that can be copied to systems at a later date.

The ConfigOS Policy Encryption Process



As an option when installing a new or additional Foundry, the user can choose to implement a Foundry Key that has already been generated by an existing Foundry. This allows the user to set up more than one Foundry to service a set of ConfigOS Command Centers for volume considerations as well as for backup and COOP considerations. The ConfigOS Foundry signs and encrypts the policy files in its generated Signature Containers, which may then be used by the bound Command Center(s).

E. Secure Signatures and Signature Containers

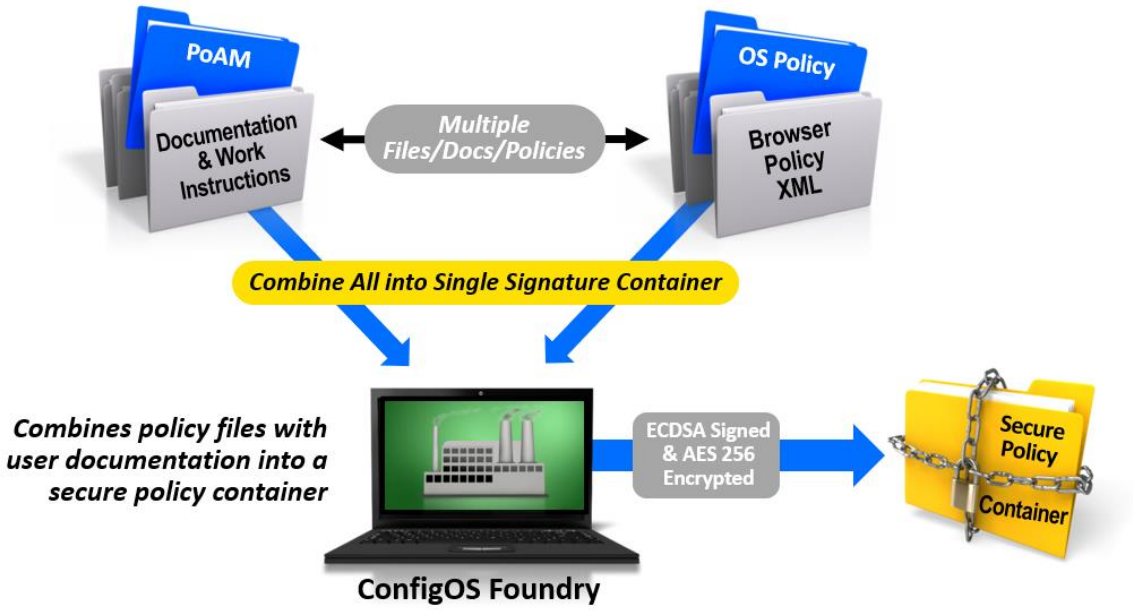
When discussing ConfigOS signatures, the terms "signature" and "Signature Container" are sometimes used interchangeably. To be precise, a signature is an individual XML file that addresses the policy or the configuration of a specific operating system or pieces of support

software, such as IE or Chrome. There is a one-for-one relationship between a ConfigOS signature and a DISA STIG document. For example, there would be a signature for Windows Server 2019 and a separate Internet Explorer signature. You might even desire to have a signature of, say, only the STIG CAT1 items. A ConfigOS Signature Container is a single file that may contain multiple policy/configuration XML files (signatures) along with other user documents, such as POAMs and work instructions. Individual XML policy signatures are not operational. Only encrypted and signed Signature Containers are used to scan and/or remediate systems.

SteelCloud's rationale for developing the Signature Container concept was to provide a facility to those responsible for creating/approving policy whereby they can communicate everything that a system administrator might need to manage a system into a single file. A Signature Container is simply a single file that incorporates multiple encrypted and signed XML policy signatures as well as other unencrypted user documents.

For example, a signature container might include the following:

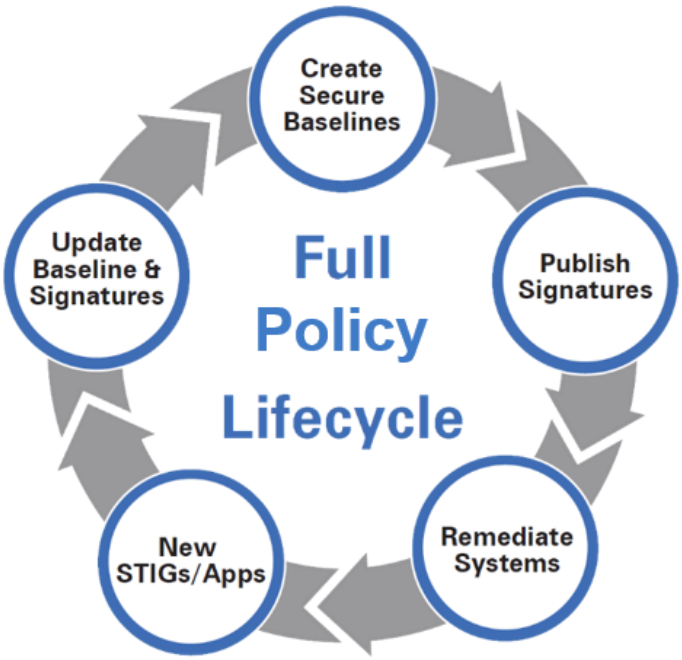
- the application-specific policy signature for Server 2019
- IE 11 STIG policy signature
- the text of the latest Server 2019 STIG
- waiver and POAM information
- other documentation, such as work and/or installation instructions



The ConfigOS Foundry allows the user to simply select the appropriate XML policy and user files. The Foundry will use its Foundry encryption key to encrypt and sign the XML policies and will combine them with any user files into a Signature Container file. Using the container concept, ConfigOS supports both customers' policy requirements and their operational user documentation requirements.

F. Policy 360

Understanding 'Policy 360' is the key to leveraging the power of ConfigOS, which was designed to be used by systems administrators to harden the STIG environment around an application. Policy 360 is SteelCloud's concept for monitoring and maintaining security policy throughout the lifecycle of an application. ConfigOS has a unique 'builder' function that allows a user to build a signature from scratch, or more likely, from existing SteelCloud STIG or CIS policy content. Using a simple point-and-click process, individual policy controls (i.e., STIG V-IDs) can be included or excluded, ignored, or modified in a signature. Additionally, the Foundry provides the user with the ability to "accept" non-compliant controls and document waiver reasons in the signature content for reporting and interfacing with 3rd-party products like STIG Viewer. The policy waiver information embedded in the ConfigOS policy content created by the user in the Foundry can be transferred to the STIG Viewer product through ConfigOS's checklist integration capability. This feature provides far more comprehensive information integration than simple XCCDF. Checklist Integration provides both detailed control-level finding information as well as waiver documentation. Automating both pieces of information virtually eliminates the need to manually enter data into STIG Viewer. Besides Checklist Integration, findings and waiver information are used throughout the ConfigOS workflow and reporting.



On a single screen, users can easily monitor and compare the changes/differences between the 'source' signature and the 'master' signature. This capability also allows ConfigOS to automate the task of bringing in a newly published STIG, compare it to an existing STIG, filter the control differences, and test the new controls. Control differences are shown using simple color-coding. With the ConfigOS Foundry signature builder function, users can create new signatures without ever touching the underlying XML. In addition, ConfigOS validates the syntax.

"Builder" and "rollback" are the key ConfigOS functionalities that support the concept of STIG 360. The ConfigOS signature builder and rollback functions allow the user to implement and reverse hundreds of STIG controls within minutes. Typically, complete STIG hardening is reduced from hours/days/weeks to only 30-60 minutes. Most importantly, in addition to

having created the first "good" image, the policy environment is fully documented with a ConfigOS XML signature as a byproduct of the hardening process.

So, not only does ConfigOS reduce the effort and expense of hardening systems by more than 90%, but it also creates the signature artifact that can automatically remediate like systems anywhere, on any network, in any domain.

G. ConfigOS Foundry Implementation Strategy

SteelCloud has separated the policy creation/tailoring functionality provided by the Foundry from the operational scanning/remediation/reporting capabilities found in Command Center. This separation allows the customer to create an audit break between those responsible for creating and approving policy and those using the approved policy. The ConfigOS Foundry creates secure policy files (containers). Therefore, it does not need to be on the same network or domain as Command Center. The Foundry signature content can easily be moved (physically or electronically) from an unclassified infrastructure to a classified one, as one would move other files from the low side (unclassified) to the high side (classified).

The number of Foundry instances deployed depends on the number of concurrent staff members that will be doing the job of hardening around applications and creating or publishing policy. Determining the optimal number of Foundries deployed depends more on the organizational complexity and number of unique policies supported rather than on the number of endpoints. For small implementations with shared responsibilities, the Foundry and Command Center can easily reside on the same laptop, server, or virtualized instance. Typically, however, the Foundry and Command Center are deployed on different systems.

The ConfigOS Foundry logs each user policy creation activity for auditing and tracking purposes.

H. ConfigOS Command Center Overview

Command Center is the workhorse of the ConfigOS product set. Command Center uses the secure policy containers created/published by ConfigOS Foundry and scans, remediates, and provides reporting for endpoint processing. Command Center provides the following capabilities:

- flexible endpoint and group set-up
- automated network population from AD and DNS sweeps
- comprehensive scanning and remediation for Windows and Linux and additional components within these environments (e.g., Microsoft Office, SQL Server, IIS, IE, Apache)
- rollback support with sequential history processing to a known "good" state
- permanent scan/remediation results archive

- flexible reporting at the policy, endpoint, and job levels
- special functionality for GPO conflict reporting, XCCDF output, and STIG Viewer Checklist integration

Flexible Group/Endpoint Set-up – Command Center uses a familiar "tree" structure to organize groups and endpoints. Optionally, credentials and policies can be managed at the group level to simplify managing these elements for a large endpoint population. Command Center allows the user to determine which endpoints are managed as a group and which are managed individually, irrespective of how they are grouped. The Command Center tree can be bulk loaded by a DNS and/or an AD sweep and categorized by its OS type. The Command Center tree can be reorganized by simply dragging and dropping items into new locations. Groups can traverse networks.

Scanning and Remediation – Scanning and remediation jobs can be set up by selecting groups of endpoints or individual endpoints. Scans and/or remediations can be combined into a single job across Windows and Linux. The system running Command Center will "attach" to the maximum concurrent processes identified in Command Center Preferences and will "crawl" through the selected population at that maximum number of concurrent processes specified. For example, if the concurrent processes ("throttling") in Preferences are set at 50, and you want to scan/remediate 500 endpoints, Command Center will initially attach to 50 endpoints. As the first endpoint is done processing, Command Center will attach to the 51st endpoint and roll through the 500 endpoints, keeping 50 processes active. The scanning process involves scanning and producing reports and XCCDF files (if selected). The remediation process is a little more involved and includes the following steps for each endpoint selected for remediation:

1. Scan
2. Create a rollback file
3. Remediate
4. Re-scan
5. Conduct an additional scan to produce GPO conflict results (optional)
6. Create a results archive
7. Create compliance reports
8. Create XCCDF output (optional)

NOTE: Setting the maximum processes within ConfigOS allows the user to "throttle" the system to the capacity of the hardware running ConfigOS (i.e., number of cores) and/or the available network bandwidth.

Rollback – Any time Command Center updates any control on a system, it produces an encrypted synchronous rollback file that is keyed/encrypted to its associated system. Command Center manages rollback files over time and allows the user to sequentially step through rollbacks. Rollback files are only as big as the controls that are being updated—typically 5k-100k.

Results Archive – ConfigOS stores detailed results of its scanning and remediation activities in a permanent data store. Results are organized by endpoint and activity/date. The results archive is accessible by selecting an endpoint and a scan/remediation activity/date. Reports, logs (JSON format), and STIG Viewer Checklists are available by accessing the results archive. This facility is useful in researching/auditing detailed, time-specific control information at the policy/endpoint level.

Reporting – Report generation is determined on the Command Center Preferences screen. Reports can be produced by individual policy, by endpoint, by container (all policies), by endpoint, and by job. XCCDF and GPO conflicts (remediation only) can also be produced when running reports. Preferences can be overridden when a scan/remediation job is run. Policy and endpoint reports are produced in a highly flexible, searchable HTML format. Consolidated job reports are produced in a PDF format and include special functionality to project endpoint compliance if/when remediation is selected.

XCCDF and STIG Viewer Checklists – XCCDF output is automatically produced by ConfigOS. XCCDF output is set up in ConfigOS Preferences and can be initiated/overridden when a scan/remediation job is started. The XCCDF output can be easily imported into STIG Viewer to close findings. ConfigOS Checklist integration is a more comprehensive interface to STIG Viewer. It not only closes findings but also integrates detailed finding results and waiver information. In practice, a user would start with a reusable checklist with static (manual) information pre-entered, and ConfigOS would fill in all of the details regarding controls and waivers (i.e., dynamic information) for the endpoint. This process eliminates virtually all manual STIG Viewer data entry, further streamlining STIG Viewer maintenance.

I. ConfigOS Command Center Implementation Strategy

Command Center is a flexible, lightweight tool that can easily be installed where it makes the most sense for the client use case. Command Center is not tied to a Microsoft or security domain and can operate on workgroups and stand-alone systems. As a high-performance tool, Command Center is typically implemented according to operational and/or security boundary considerations rather than volume. Since only endpoints are licensed and not Command Center itself, the client is licensed to install instances of ConfigOS anywhere a Windows endpoint has been licensed.

Volume Considerations – Several factors will determine the number of deployed instances of Command Center. While the number of endpoints is a major factor, other factors are also important, including the following.

- *Total Policies* – This refers to the total number of policies to be applied to the endpoints. For example, an infrastructure with 500 server endpoints might only have two policies applied to each endpoint. This would mean that 1,000 total policies would be applied when scanning/remediating the infrastructure. Conversely, 200 workstations with a dozen policies each would generate 2,400 total policies. Note that both endpoints and total policies are important.

- *Frequency* – Scan/remediation frequency is another major factor. The frequency of processing is based on business and security requirements determined by an organization. The processing frequency will impact the capacity at higher endpoint counts, especially when it comes to the frequency of remediation versus the frequency of scanning.
- *Time Constraints* – If the scanning and remediation are required to be completed within hours, then an instance of ConfigOS will be implemented with higher endpoint counts. If, however, scan/remediation jobs are required to be processed within minutes, then larger hardware and/or additional instances of ConfigOS would be implemented.
- *Hardware* – Network traffic is typically not a consideration in determining the appropriate number of instances of Command Center to implement. The user can easily determine the number of concurrent processes executed by Command Center. A concurrent process is an individual endpoint policy scan/remediation. The robustness of the platform running Command Center is the primary factor in determining concurrent processes, and therefore capacity. The maximum number of concurrent processes is primarily based on the number of CPU cores available to Command Center on the system running it. A rule of thumb is that each core can effectively handle 10-20 concurrent processes. The variation in the number of processes includes the number of threads per core and the speed of the cores.
- *Available Bandwidth* – Very low bandwidth availability will potentially blunt the processing capacity of ConfigOS, primarily when addressing very high endpoint processing.

Security Boundaries – ConfigOS Command Center does not require domain services and does not need the Internet. Licensing does not dictate the number of instances of Command Center that a customer can deploy. Typically, clients will not have an economic incentive to 'pierce' protected networks in order to reduce the number of Command Center instances. Policies are published as secure file containers that can easily be moved around an organization (physically or electronically) to the instance of Command Center where they are to be used.

Stand-alone Systems – ConfigOS Command Center can be loaded/run directly on stand-alone Windows workstation and server endpoints. Additionally, users can run Command Center on a laptop and directly scan and remediate stand-alone Windows/Linux systems by connecting a standard network cable.

AD/GPO Best Practices – Active Directory (AD) is a ubiquitous tool for Microsoft infrastructures. Although AD/GPO (Group Policy) is a great tool for its intended purpose, many organizations have attempted, with varying success, to extend GPO as the primary mechanism for initiating and maintaining STIG compliance. Even with the STIG GPO content provided by DISA, GPO's inherent complexity and lack of functionality, such as rollback and Linux support, make GPO a challenging solution for comprehensive enterprise STIG

compliance – especially across the DevOps lifecycle. Additionally, many enterprises organizationally separate the AD/GPO and systems administration functions, which adds significantly to the time, complexity, and expense of finding, solving, and correcting GPO/STIG conflicts. The distance created by this organizational setup places additional burdens on GPO as an effective tool for adequately responding to STIG compliance demands. ConfigOS is by no means a replacement for AD/GPO, but rather a synergistic technology that allows an organization to significantly flatten and simplify its implementation of AD/GPO.

As described throughout this document, ConfigOS is the most efficient means to harden controls around an application – typically in ~60 minutes. The byproduct of this hardening process is a transportable policy signature that can be used to automate STIG compliance in each step of the DevOps process, from development to production/sustainment. Therefore, when implemented in conjunction with ConfigOS, best practices dictate that organizations use GPO for the top-level controls that are common across all applications (e.g., password length, bad logon attempts, legal banner).

The exact line of demarcation for GPO will vary from organization to organization. Appropriate GPO control candidates will include those high-level controls universally applied across all application stacks that typically do not break applications. With AD/GPO relegated only to top-level controls, ConfigOS would overlay the complete control stack with its agile approach to reporting and interfaces to STIG Viewer. Typically, the quarterly DISA STIG changes will be implemented below the GPO control threshold, exclusively by ConfigOS. The result will be an implementation of AD/GPO that is far less complex, with improved availability and reduced administrative burden on the organization.

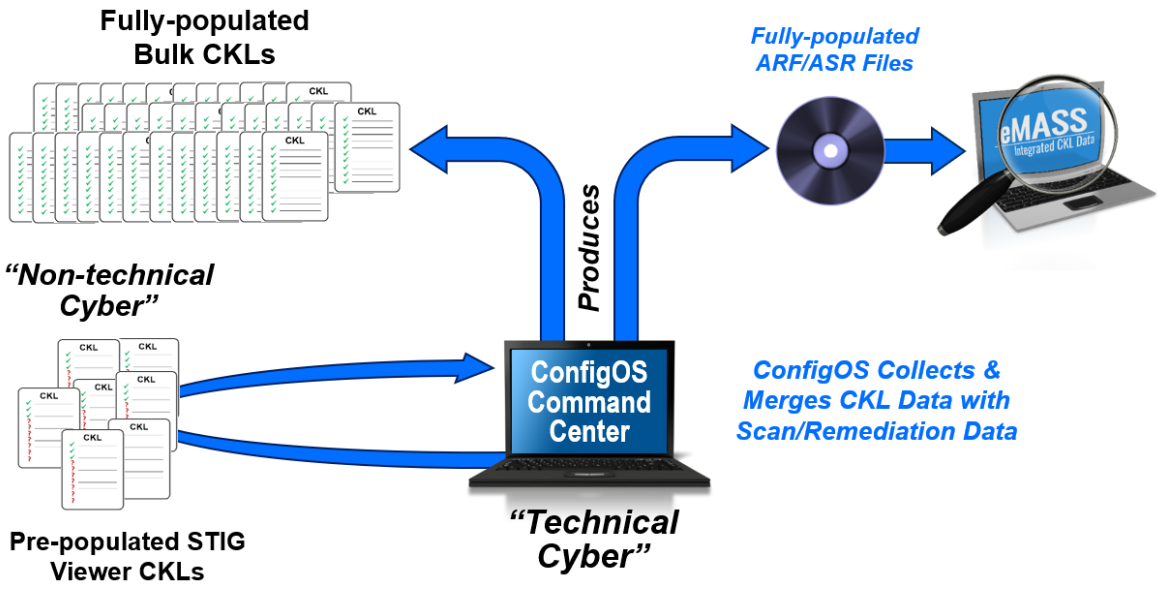
To keep GPO and ConfigOS properly aligned, ConfigOS specialized GPO conflict reporting will identify each control on each endpoint, where GPO is taking the endpoint out of compliance.

Frequency – The recommended frequency for scanning and remediation will vary based on factors specific to the customer environment. ConfigOS has enough capacity to scan or remediate every endpoint, every day in most infrastructures. ConfigOS automation with low operational overhead allows organizations to increase the frequency of remediation.

Policy Publishing – SteelCloud has spent a good deal of effort designing ConfigOS to allow organizations to safely publish policies. Client-specific ECDSA signed and AES 256 encrypted keys are used to encrypt policy containers. With this protection, clients can publish and use these policies in any environment (e.g., classified, tactical, weapon systems), anywhere in the world, with the assurance that their approved policies are intact and have not been altered.

J. Integrated STIG Viewer Checklists with eMASS Automation

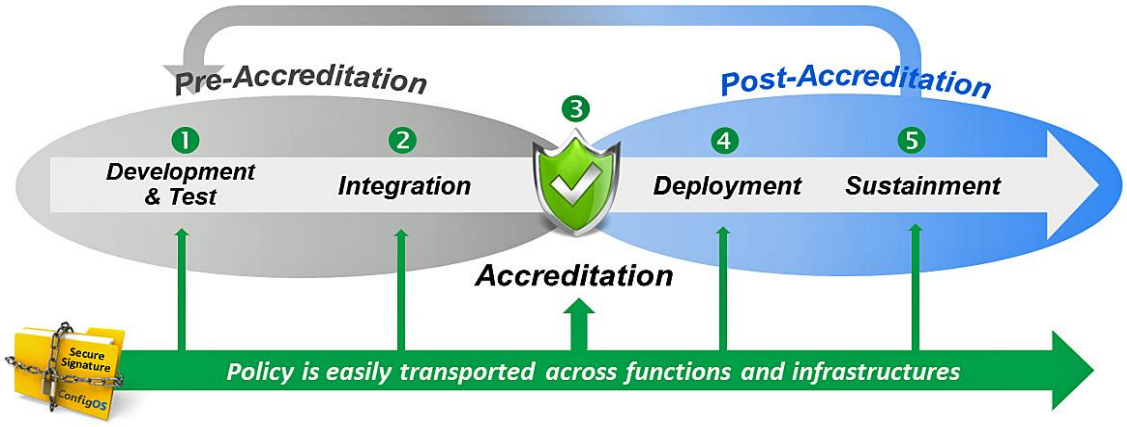
ConfigOS has the capability to create integrated STIG Viewer checklists and eMASS ARF/ASR files that include both ConfigOS scan/remediation data along with manual checklist data. This is accomplished by simply linking checklists that have been pre-populated with documentation/manual controls with policies for specific endpoints/groups of endpoints within Command Center.



To create integrated checklists, the user would simply select the individual or groups of endpoints to process and Command Center will merge its data with the pre-populated checklist data and create a completed checklist for each policy, for each endpoint that has been selected. Similarly, to create integrated eMASS ASR/ARF files, the user would select the individual or groups of endpoints to process, and Command Center will merge the data and create eMASS files that include both ConfigOS and manual checklist data. The user has an option to create an ARF file for each policy or produce an ARF that combines policies – taking advantage of a new DISA eMASS enhancement

K. DevSecOps – *Driving Compliance Throughout DevOps*

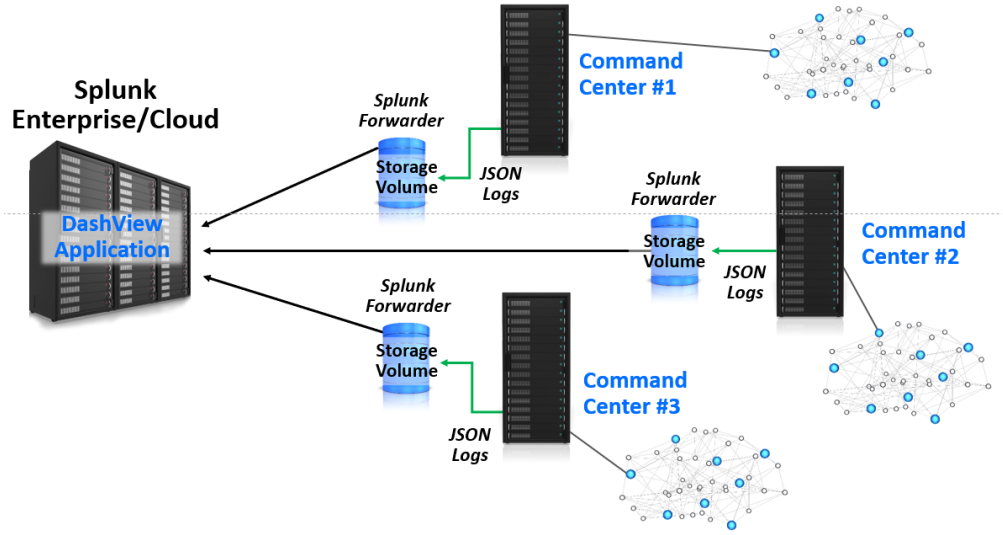
DevSecOps is the concept of driving compliance and security elements into and throughout the application lifecycle. ConfigOS provides a range of functionality that makes it an attractive vehicle to drive compliance throughout every stage in the DevOps process. The user can easily stand up a specific application-oriented policy within minutes, perform application testing, and then reverse the hardening and revert back to the original development state. Additionally, ConfigOS policy containers can easily be transported across discrete infrastructures.



Policy transportability provides the real-world opportunity to inject policy testing anywhere in the DevOps process, no matter where the process is executed. This capability also allows the user to ensure the consistent application of policy from development to production sustainment.

L. DashView – The ConfigOS Advanced Compliance Dashboard

ConfigOS DashView is an advanced compliance dashboard built on the Splunk platform. SteelCloud delivers DashView as a simple to implement COTS application that can be installed in any Splunk infrastructure – Enterprise or Cloud. DashView provides a detailed hierarchical view of data including enterprise, location, system, policy, and control. Dashboards are also provided for "horizontal" view of data across operating systems and application stacks. Additionally, users can view waiver information across their enterprises. Naturally, all data can be viewed across time and compliance "heat maps" are included.



Splunk's standard forwarders consolidate data from multiple locations into Dashview. DashView is set up to parse and ingests Command Center's standard JSON output.

M. ConfigOS – Major Use Cases

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

- RMF Accreditation and ATO Acceleration – Risk Management Framework (RMF) accreditation leading to an Authorization to Operate (ATO) requires multiple tasks that include significant documentation and system hardening. Traditionally, system hardening has been a highly specialized manual process requiring significant knowledge of OS policy and the idiosyncrasies of the installed application. Frequently, this activity takes weeks to accomplish. ConfigOS reduces the application policy hardening process to about an hour. Using ConfigOS not only accelerates the hardening process but also documents the results in a signature that can then be used to automate consistent replication of the results across infrastructures. ConfigOS allows the user to easily transfer policies approved in the accreditation process to the deployment/production environment for ongoing assessment, remediation, and reporting. ConfigOS can reduce accreditation timelines by as much as one to two months.
- Gold Disk Support – "Gold Disks" have been great accelerators for implementing new systems. However, they typically do not mitigate the cost and effort of keeping the systems built with them up to date with the latest policies. ConfigOS is a perfect complement to a gold disk program. Simple signatures can be published to keep systems built with gold disks up to date with the latest policies. Over time, policy compliance using ConfigOS will have a more significant impact on costs and manpower than the initial gold disk implementation.
- Mission Partner Support – It can be a significant challenge to coordinate testing and deployment when activities span multiple environments. ConfigOS signatures can easily be included with applications as they are transferred to disparate infrastructures from one mission partner to another. With ConfigOS, it is easy to replicate and maintain policies and configurations as systems move through the process from development, through accreditation, to production. In addition, since ConfigOS is inexpensive and lightweight, requiring little infrastructure of its own, it is easy to implement across mission and technology partners. ConfigOS secure policy signatures can be transported with applications so that compliance application-specific environments can be quickly and consistently implemented.
- CMMC/NIST 800-171 Compliance – SteelCloud provides a simple tool that lets DoD contractors harden and keep their internal infrastructures in compliance as required by the DFARS. SteelCloud's patented ConfigOS automated STIG/CIS compliance software reduces the time, effort, and complexity of addressing the CMMC control mandate. ConfigOS scans and remediates with compliance reporting to fix the non-compliances and hardens STIG/CIS controls around an application baseline in 60 minutes.
- Software/Technology Product Delivery – COTS software vendors can easily ingest the compliance policies with a simple ConfigOS signature. Not only can vendors then test

(and develop) their products to government standards, but they can document back to their customers any waiver requirements that their products may require using a simple signature. Then the customer can use this signature to automate the installation and testing of the vendor's products. ConfigOS helps vendors prepare both their company and their products to be "STIG ready."

- Cloud STIG Implementation and Maintenance – The commercial cloud is a great facility to quickly stand up and test applications. While it is extremely flexible, commercial cloud environments naturally lack some of the tools that organizations have available in their private infrastructures. Because ConfigOS is simple and lightweight, it is a great solution for even the smallest cloud prototypes. SteelCloud has used the same ConfigOS signatures across private infrastructures (hardware and virtualized) and commercial cloud environments, such as MilCloud, GovCloud, AWS, and Azure.
- Critical Infrastructure – Implementing government recommendations of best practices for hardening systems within the country's commercial critical infrastructures has proven cumbersome and expensive. ConfigOS is an excellent solution for implementing and maintaining compliance in non-traditional computing environments.
- Weapon and Tactical Systems – Like critical infrastructure, weapon systems incorporate many IT resources that are out of the mainstream of traditional enterprise IT. Increasingly, organizations 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.

N. About ConfigOS

ConfigOS is currently implemented in classified and unclassified environments, tactical and weapon system programs, disconnected labs, and the commercial cloud. ConfigOS is client-less technology, requiring no software agents. ConfigOS scans endpoint systems and remediates hundreds of STIG controls in under 2 minutes. Automated remediation rollback as well as comprehensive compliance reporting and STIG Viewer Checklist and XCCDF output, are provided. ConfigOS was designed to harden every CAT 1/2/3 STIG control around an application baseline in about 60 minutes—typically eliminating weeks or months from the RMF accreditation timeline. ConfigOS addresses Microsoft Windows workstations and server operating systems, SQL Server, IIS, IE, Chrome, and all of the Microsoft Office components. The same instance of ConfigOS addresses Linux environments, such as Apache, Red Hat 5/6/7, SUSE, Ubuntu, and Oracle Linux. ConfigOS content includes over 10,000 STIG and CIS controls. New patent-pending functionality has been added to Command Center to resolve AD/GPO policy conflicts.

O. 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.