SteelCloud®

Simplifying Cyber Assurance

ConfigOS™

Concept of Operations

Automated STIG Remediation

Making Software Work in Secure Environments

Version 1.7

February 31, 2015

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

SteelCloud
Simplifying Cyber Assurance

ConfigOS Concept of Operations

Contents

A. Background

The Department of Defense (DoD) protects its 15,000 networks by defining, implementing, and auditing "best practices" for installation and maintenance of its information technology resources. The Defense Information Systems Agency (DISA) develops and publishes policy, 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, little progress has been made in automating the arduous tasks of implementing and maintaining STIG policy on the hundreds of thousands of systems operated by the DoD.

SteelCloud has been automating STIG compliance in the DoD for over six years. Having delivered and supported STIG-compliant technologies across the DoD, in major agencies and each of the Services, SteelCloud has seen the operational issues involved in creating and supporting secure environments that support mission goals. Over this time SteelCloud has developed a set of easy to implement tools that mitigate risk and reduce the cost of supporting applications in DoD-mandated secure environments.

B. Defining the Problem

It is widely recognized that supporting STIG-compliant environments is expensive and negatively impacts mission effectiveness. It is expensive because system STIG maintenance is tedious and time consuming for systems administrators. STIG compliance is typically done on a system by system, application by application, and site by site basis thousands of times a day throughout the DoD. STIG maintenance also requires a high level of Operating System knowledge and experience.

STIG compliance is not really the problem. If the same policies and configurations could be implemented on all systems, STIG compliance would be a rather easy exercise. Unfortunately, commercial and government developed applications react to security policy differently, and therefore, each system must be uniquely “tuned”. In addition to fine-tuning policy changes, many applications require configuration beyond the scope of what is adjusted by the policy. Also, many applications require somewhat unique configurations, beyond just security policy.

The problem is not creating and maintaining secure compliant environments, the problem is creating and maintaining secure compliant environments where application software products will actually run reliably. Making software work in secure environments defines the intersection of operations/mission and security. Automating this intersection is the problem that SteelCloud has developed ConfigOS to address - creating and maintaining secure, compliant “application-specific” environments.

An effective solution really comes down to “leverage.” How can something be done right once, and then be replicated across an enterprise (the DoD) dozens, hundreds, or 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; where a simple signature can easily be developed once and then securely used across the DoD, 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 to first define an enterprise. In the DoD, is an enterprise an individual agency or Service? - A location or department? – A network or domain? – Or is it the entirety of the DoD? Assuming 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 which includes single/few security domains, data centers, or networks. In contrast, the DoD's infrastructure is significantly more fractured, decentralized, and complex.

HBSS and ACAS are two examples of "enterprise" technologies within the DoD. Neither need be installed centrally, but both provide a level of consistency across the DoD by helping to enforce standards of computing/security. ConfigOS was developed with a similar "enterprise" solution paradigm; software that can be implemented ubiquity across the DoD without requiring unnatural changes to the infrastructure. ConfigOS provides for security and capability consistency that can be controlled at any level within the DoD without the required connectivity or access.

D. ConfigOS – Security Overview

The ConfigOS solution incorporates two distinct pieces of software – the Foundry and the Client. The ConfigOS Client performs all of the production functions of ConfigOS, while the Foundry was developed to allow organizations to secure, control, and manage the production of signatures. Therefore an organization may have hundreds or thousands of ConfigOS Clients which are supported by secure signature production of one or a just few Foundries. The number of Foundries are determined by desired "publishing" control points within the enterprise rather than capacity or throughput.

The security mechanisms within the ConfigOS solution ensures that a set of Clients can only use signatures from their prescribed Foundry(s). Upon its installation, the ConfigOS Foundry utilized a FIPS-compliant random number generator to create a unique 256-bit key that is encrypted into two key files. The Foundry Key is used to install one or more Foundries and the Client Key is used to install the ConfigOS Clients. SteelCloud separated the Foundry and Client Keys so that the key that is distributed with the Client for installation cannot be used to set up a rogue Foundry. When the ConfigOS Client is first installed it is "bound" to the Foundry(s) using the Client Key produced by the Foundry. As part of the Client installation, the Client re-encrypts the Client Key produced by the Foundry. This process utilizes protection mechanisms so the Client Key cannot be

exchanged after installation. Based on specific DoD input, the key mechanism is "bound" to the installation of ConfigOS rather than the machine where the ConfigOS Client is installed. This allows ConfigOS to be preinstalled as part of an image that can be copied to machines at a later date.

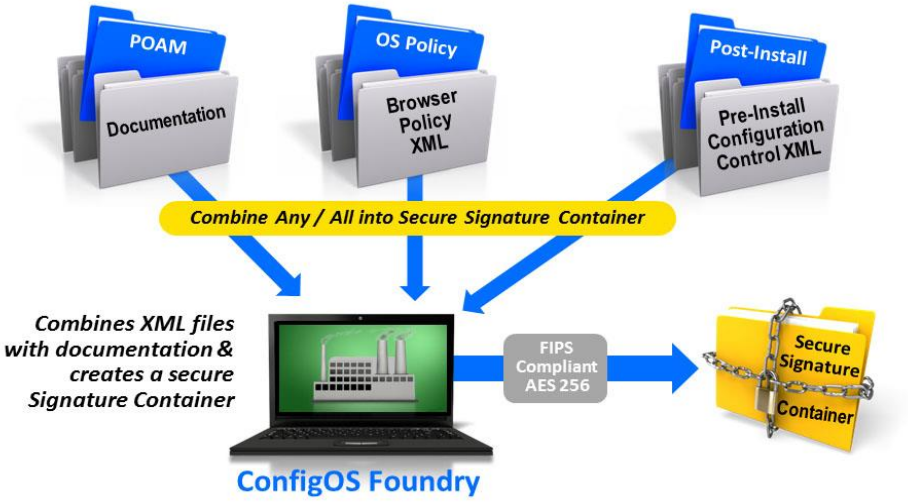
As an option when installing a new/additional Foundry, the user can choose to implement a Foundry Key that has already been generated by an existing foundry. This allows the user to set up more than one Foundry to service a set of ConfigOS Clients for volume considerations as well as backup and COOP.

E. Secure Signatures and Signature Containers

Sometimes in discussing ConfigOS Signatures the terms "Signature" and "Signature Container" are sometimes used interchangeably. But, to be precise, a signature is an individual XML file that addresses policy or the configuration of a specific operating system or piece of software. For example, there would be a signature for Windows 2008 R2 and a separate signature for Internet Explorer. You might even desire to have a signature of only the STIG CAT1 items. Also, you might have a configuration file signature for a specific implementation on an application. A ConfigOS Signature Container is a single file that may contain multiple policy and configuration XML files (Signatures) along with other documents. Only Signature Containers are used to remediate systems.

SteelCloud's concept in developing ConfigOS was to provide a facility to communicate everything that a system administrator might need to manage a system into a single file hence a "Signature Container." A Signature Container is simply a single file that incorporates multiple Signatures as well as other documentation. For example, a signature container might include:

- The standard STIG signature for 2008 R2
- The application-specific policy signature for 2008 R2
- IE 10 & 11 STIG signatures
- The text of the latest 2008 R2 STIG
- Waiver and POAM information
- Other documentation such as work and/or installation instructions



It is the ConfigOS Foundry that allows the user to simply select the appropriate files which the Foundry will encrypt with the Foundry's Key and incorporate them into a single hashed zip file – the *Signature Container*. Utilizing the container concept, ConfigOS supports both a customer's security requirements as well their operational requirements.

F. Remediation Alternatives

Traditionally, most STIG remediation work has been done manually. For Windows-based systems, the STIG work has to be augmented by Active Directory (AD). Typically, a client might build about half of the STIG controls into AD Group Policy. The half implemented in AD are typically those policies for which applications are insensitive, thus requiring little AD tuning or maintenance. While AD is fabulous for its intended purpose, it is too cumbersome to implement the hundreds of Windows STIG policies. And, most importantly, AD does not address Linux policy requirements.

Imaging (copying an entire machine image) is also a viable technique for implementing STIGs for some environments or applications. The problem with imaging is that, for it to work well, it assumes that application updates, OS updates, support software updates, and STIG policies can be managed on a single installation schedule. We know this is almost never the case. Also, some more secure applications are "bound" to the machine for which they are installed and, therefore, cannot be imaged. Furthermore, some systems store unique data that cannot be maintained when overwriting its image. The sheer bandwidth requirement of imaging creates issues in some environments. Imaging is a great alternative, where it fits.

A number of expensive boutique management solutions can make sense in some DoD environments. These, primarily commercial systems, best address single infrastructures because of their inability to transport policy across networks/domains. Because of their cost and complexity, these boutique management solutions are reasonable alternatives for a small subset of DoD environments.

ConfigOS Windows 2008 R2 STIG Coverage

Tool	Validate *(Items)*	Remediate *(Items)*	Application-specific	Configuration Validation	Cross-Domain	Infrastructure Validation
SCAP	~263	0	No	Partial	Yes	No
ConfigOS	313	296	Yes	Most	Yes	Yes

(as of February 2015)

ConfigOS Windows 2012 STIG Coverage

Tool	Validate *(Items)*	Remediate *(Items)*	Application-specific	Configuration Validation	Cross-Domain	Infrastructure Validation
SCAP	~286	0	No	Partial	Yes	No
ConfigOS	314	297	Yes	Most	Yes	Yes

(as of February 2015)

ConfigOS Red Hat Linux 6.5 STIG Coverage

Tool	Validate *(Items)*	Remediate *(Items)*	Application-specific	Configuration Validation	Cross-Domain
SCAP	~173	0	No	Partial	Yes
ConfigOS	233	229	Yes	Most	Yes

(as of February 2015)

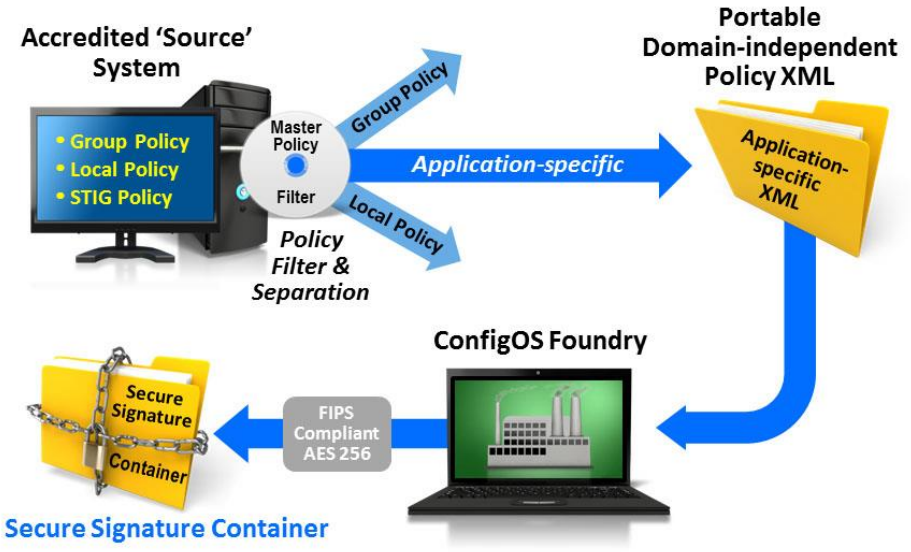
SteelCloud developed ConfigOS to address the widest range of DoD use cases. It is inexpensive, easy to install and support, while requiring no new infrastructure or changes to DoD's security or networks. It can effectively be used in large or small, classified or unclassified environments. ConfigOS remediates more STIG controls than either SCAP or ACAS currently validate. Most importantly, ConfigOS automatically creates policy signatures from operating accredited/baseline systems in a matter of seconds. Then, within minutes, the ConfigOS Foundry packages those signature up into secure Signature Containers that can be safely published for use across the DoD.

G. ConfigOS – *In Operation*

ConfigOS is a patent-pending solution that is built on the concept of simplicity. In this case, the simplicity to create application-specific policy signatures and the simplicity to remediate systems. The core to its simplicity is ConfigOS' ability to create XML signatures

from operational accredited 'source' systems. It accomplishes this by translating a system's security policies into machine-actionable XML.

ConfigOS uses the concept of a Master Policy to determine which individual policies/controls to extract from the source (accredited) system. A Master Policy is simply a standard ConfigOS Signature that contains all of the policies that need to be extracted/translated from the source system. For the DoD, the Master Policy is typically the DISA STIG policy, including much of the STIG text and the acceptable policy entries and ranges. A Master Policy can be created by any customer, but for convenience, SteelCloud provides customers with a STIG Master Policy as a standard part of our ConfigOS DoD offering.



When the user performs a policy export (which can be done from any system running the ConfigOS Client), ConfigOS extracts the policies and controls from the source system and translates these policy/controls into a machine-actionable XML signature. This signature can then be combined, when appropriate, with additional signatures and documents through the ConfigOS Foundry to create a secure Signature Container with the specific policies/controls of the original source system. The entire policy export process to create the secure Signature Container can take as little as two minutes.

Once the Signature Container is created it is ready to use on a target system. The basic workflow on updating an endpoint system is as follows:

- Compare the target system's policies to the ConfigOS signature published by the user (<30 seconds)
- Review the results
- Remediate (update) to target system with the published signature (<60 seconds)
- Reboot the system

- Compare the target system to the published signature to review any changes made by AD Group policy
- Scan and review using an approved IA tool (i.e. ACAS)
- Place back into production

This entire process can take as little as 5 minutes. The key to the success of this process is the confidence that the signature, produced from an operational 'source' system, will not introduce any errors in updating a target system.

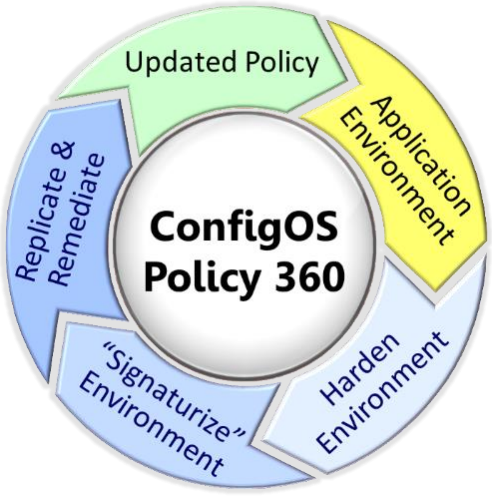
☑ ***Key Concept*** *– Over the last six years, SteelCloud has validated that STIG policy is application sensitive, rather than environment/infrastructure sensitive. Therefore, once a signature has been developed for an application, it should work without issue, in every environment from a single server, to a virtualized environment, to the commercial cloud.*

H. STIG 360

In addition to being able to create a Signature for a source accredited system, ConfigOS has a unique 'Builder' function that allows a user to build a Signature manually from scratch, or more likely, from an existing Signature. Using a simple point & click process, individual policies can be included/excluded or modified in the new Signature.

On a single screen, a user can easily monitor/compare the changes that they make against the Source Signature and the Master Signature (STIG). Differences are shown using, simple to visualize, color coding. With the ConfigOS Signature "Builder," users can create new Signatures without ever touching XML. And, ConfigOS validates the syntax.

Builder and Rollback are the key ConfigOS functionalities that support the concept of "STIG 360." Understanding STIG 360 is a key to leveraging the power of ConfigOS. ConfigOS was designed as a tool to be used by systems administrators to harden the STIG environment around an application. ConfigOS Signature Builder and Rollback allow the user to implement and reverse hundreds of STIG controls within minutes. Typical complete STIG hardening is reduced from hours/days/weeks to only 30-60 minutes. But, most importantly, in addition to having created the first "good" image, the environment is fully documented with a ConfigOS XML signature as a byproduct of the hardening process.



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

I. ConfigOS – Other *Use Cases*

The following are examples of additional ConfigOS use cases beyond the enterprise implementation for which it was designed.

1) **First Good Image** – The DoD, its suppliers, and mission partners spent considerable time to harden environments around installed applications. Traditionally, system hardening has be a highly specialized manual process requiring significant knowledge of OS policy and the idiosyncrasies of the installed application. Many times this activity takes days/weeks to accomplish thereby increasing the expense and delaying the implementation of important systems. When using ConfigOS' ability to implement new Signatures through the builder and rollback policy changes in seconds, hardening the policy environment around an application usually takes less than an hour - with little application expertise. 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 the enterprise.

2) **Unified Gold Disk Support** – "Gold Disks" have be 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 STIGs. 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 DISA STIG policies. Over time, STIG maintenance, utilizing ConfigOS, will have a greater positive impact on costs and manpower than the initial Gold Disk implementation.

3) **WorkStation Policy Automation** – ConfigOS can dramatically reduce costs and effort while increasing consistency of deploying and maintaining secure workstation environments. SteelCloud provides signatures for Windows 7, Windows 8, Microsoft Office, Internet Explorer 10 and Internet Explorer 11. Additionally, SteelCloud provides configuration control signatures to validate other non-policy STIG items. All of these signatures can be modified in minutes to meet the needs of any DoD organization.

4) **Mission Partner Support** – Coordination of testing and deployment when the activities span multiple environments can be a significant challenge. 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 to test to pilot to production. And, since ConfigOS is inexpensive and lightweight, requiring no infrastructure, it is easy to implement across mission and technology partners. For example, a DoD component can give a program SI the policy/configuration for which they want their system to be delivered. The SI, upon development and delivery, can document and transfer the policy/configuration for the system back to the DoD component. The DoD component can then populate their lab and production environment with the appropriate policy/configuration. Tremendous amounts of error correction and testing are completely eliminated.

5) **Software/Technology Product Delivery** – COTS software vendors can easily ingest the DoD STIG policies with a simple ConfigOS signature. Not only can the vendor then test (and develop) their products to DoD STIG standards, but they can document back to their DoD customers any waiver requirements that their products may require using a simple signature. The DoD can use this signature to automate installation and testing of the vendors products.

6) **Cloud STIG Implementation & Maintenance** – The commercial cloud is a great facility to quickly stand up and test applications. While it is extremely flexible, it naturally lacks some of the tools that organizations use to maintain their private infrastructures. ConfigOS has been successfully implemented within AWS to address STIG compliancy. 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 AWS.

7) **Critical Infrastructure** – Implementing government recommendations of best practices for hardening systems within the Country's commercial critical infrastructure has been cumbersome and expensive. ConfigOS is a great solution for the government to transfer security policy information to industry in a form that can easily be implemented and maintained.

J. About SteelCloud

SteelCloud is located in Northern, VA (metro Wash. DC area). Across the DoD, we have been making "hard things, simple" by "turning projects into products." SteelCloud has implemented STIG-compliant technologies in every DoD Service, both in the U.S. and around the world. We have years of experience in automating STIG and policy compliance. More information, including links to product demonstrations is available at our web site www.steelcloud.com.