CleanStart

# STIG Hardening by Design

**An Infrastructure-native approach to compliance, enforcement, & drift protection.**

## Executive Summary

Traditional STIG implementation often occurs after deployment, leading to configuration drift, operational friction, and long remediation cycles. Modern container environments demand a foundational approach where government-grade security is enforced before applications run.

This document explains how CleanStart enables infrastructure-native STIG enforcement through pre-hardened operating system baselines, automated configuration control, and continuous validation across build and runtime environments. Security is embedded into the foundation so teams can build and deploy without manual hardening or compliance delays.

As of 2025, nearly 500 DISA STIGs apply across operating systems, platforms, and application components. Manual hardening often takes weeks or months and must be repeated as STIGs are updated quarterly. Organizations that adopt automated hardening consistently report major reductions in remediation effort and audit overhead.

## The Hardening Problem

Manual STIG application is difficult to scale across cloud-native environments. Common challenges include:

- STIG checklists applied inconsistently
- Configuration drift after deployment
- Runtime environments fail to match baseline expectations
- Developers face friction while navigating hardening requirements
- Security teams spend time remediating and documenting issues instead of preventing them

STIG updates occur every 90 days to address newly discovered vulnerabilities and vendor changes. Each update resets the hardening lifecycle. In large container estates, this creates a continuous loop of manual configuration, regression risk, and audit pressure.

This results in compliance bottlenecks and reduced deployment velocity.

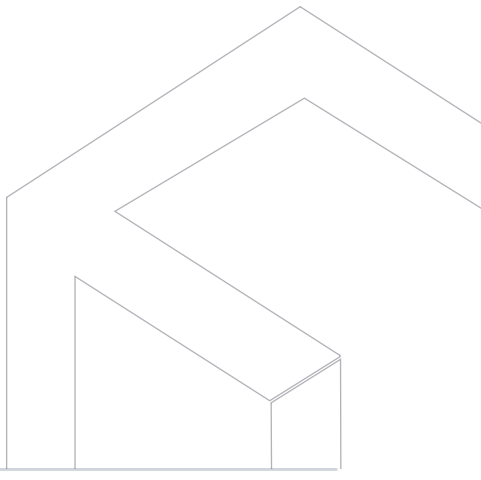
## A Foundational Approach to STIG Compliance

CleanStart shifts STIG implementation from a manual and reactive process to an embedded security layer built into the operating system itself. Compliance becomes an attribute of the platform, not an application-level responsibility.

CleanStart provides:

- Pre-hardened STIG-compliant base images
- System-wide enforcement of configuration policies
- Runtime controls preventing deviation from STIG requirements
- Automated remediation workflows
- Built-in validation to ensure consistency across environments

Unlike traditional hardened images that inherit legacy risk, CleanStart is purpose-built for secure container execution. It minimizes inherited attack surface, applies security configurations at build time, and integrates continuous validation as part of normal platform operation.



# Core Capabilities

| | |
|---|---|
| **Pre-Hardened STIG Baselines** | Built with validated configurations and locked policies |
| **Policy Enforcement** | Prevents modification of critical security parameters |
| **Runtime Protection** | Blocks configuration drift and unauthorized changes |
| **Automated Remediation** | Restores compliance states when drift occurs |
| **Compliance Assurance** | Continuous verification across CI/CD and Kubernetes environments |

# CleanStart STIG Hardening Workflow

- Start from hardened CleanStart image
- CI/CD pipeline verifies STIG configurations
- OpenSCAP validation runs automatically
- Runtime policy enforcement prevents drift
- Compliance attestation generated for reporting

STEP 01 **Start from hardened CleanStart image**

STEP 02 **CI/CD pipeline verifies STIG configurations**

STEP 03 **OpenSCAP Validation runs automatically**

STEP 04 **Runtime policy enforcement prevents drift**

STEP 05 **Compliance Attestation generated for reporting**

Compliance becomes part of the infrastructure & does not depend on developer intervention

Fig 1: Security enforced at the foundation, with compliance validated automatically across build and runtime environments

# Why CleanStart

The evolution of STIG compliance from a manual burden to an automated capability represents more than operational efficiency. It reflects a fundamental shift in how organizations approach infrastructure security. When compliance operates continuously and transparently, security no longer constrains innovation and instead becomes its enabler.

Organizations deploying cloud-native applications no longer need to trade security rigor for development speed or choose between government-grade protection and commercial agility. Modern secure infrastructure delivers both. STIG controls are embedded deeply into the operating system foundation so that compliance becomes invisible to the teams building and operating on top of it.

This is the infrastructure architecture CleanStart provides. CleanStart OS delivers container images where STIG hardening is foundational rather than applied later, where validation is continuous rather than periodic, and where security supports mission outcomes rather than slowing them. The platform transforms DISA security guidance from extensive manual configuration into a purpose-built operating environment that organizations deploy and operate with confidence.

As cyber threats against government and enterprise infrastructure continue to increase in complexity and scale, security requirements will only intensify. Organizations building on CleanStart's pre-hardened and continuously validated container foundation will not need to react to these escalating demands. They will already be operating at the security standard the future requires.

Organizations adopting automation for STIG hardening report up to 90 percent reduction in initial hardening time and nearly 70 percent reduction in ongoing security policy maintenance. This shifts hardening from a quarterly remediation exercise into a continuous, low-friction security control.

For defense contractors and regulated enterprises, this transformation moves STIG from a deployment blocker into a built-in security assurance layer.

## Cleanstart Benefit

| Benefit | Outcome |
|---|---|
| Built-in compliance | No upfront configuration effort |
| Reduced audit workload | Evidence generated during runtime |
| Developer efficiency | No delays due to STIG research |
| Higher security posture | Drift detection and policy enforcement |
| Government readiness | FedRAMP, DoD, and STIG baseline alignment |

## Integration and Availability

- **Integrates with:** Kubernetes, GitHub Actions, OpenShift, Terraform, OpenSCAP
- **Supported Standards:** DISA STIG, FedRAMP ConMon, NIST SP 800-53, SCAP 1.3

# References


Compliance Requirements for DISA's Security Technical Implementation Guides (STIGs)

Overview of STIG applicability across Department of Defense environments:

Automated STIG Hardening Finally Comes to Government IT.

STIG update frequency and vendor-driven security revisions

Impact of automation on STIG hardening timelines and operational efficiency