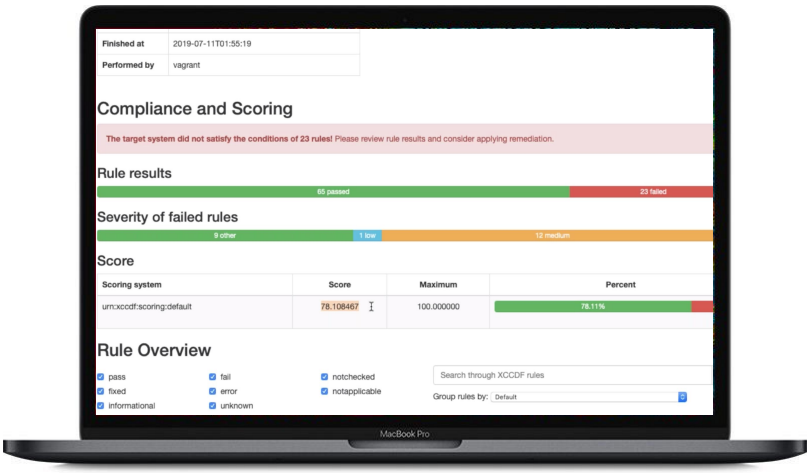
lockdown ENTERPRISE

# 3 REASONS WHY SECURITY BASELINES ARE BETTER WITH ANSIBLE

Cyber attacks are increasing, and even one misconfigured system could become the source of a catastrophic breach. Security baselines such as STIG and CIS can prevent these attacks, but adopting these baselines is no trivial task.

Security baselines are lengthy and highly complex. Thus, they are expensive to implement, and difficult to maintain. As a result, Enterprise IT is making every effort to proactively automate these security practices and outsource the maintenance whenever possible.

Ansible is the de facto choice for configuration management. It's widely deployed across organizations of all sizes, and is the perfect tool for validating, applying, and managing ongoing security baseline operations.




## A common language for security

Ansible is technology security teams need, and operations already have. With Ansible, it's possible to translate complex security policies into simple, human-readable automation which can be easily interpreted by technical and non-technical staff alike. It empowers security teams to understand what is happening "under the hood", and ultimately eases collaboration between operations and security personnel.

Lockdown Enterprise combines the simplicity of Ansible with MindPoint Group's cybersecurity expertise to further ease the application of security baselines. Lockdown Enterprise Roles are based upon the open source Ansible Lockdown community, and have been designed to secure operating systems, middleware, database, and cloud environnements to CIS and STIG standards. Every Lockdown Enterprise Role is self-documenting, certified, and supported by experts—providing businesses the confidence and reassurance that your systems are, in fact, secured to your policy.

## Ongoing baseline validation and remediation

Ansible's task-based approach to automation is perfectly suited to automating the complex configuration checklists that constitute a security baseline. Ansible enforces desired state configuration, so the baseline controls can be run repeatedly to validate and enforce compliance, correct configuration drift, and report findings throughout the entire application lifecycle. From an auditor's perspective, these features are ideal as every security control is clearly documented, repeatedly tested, and continuously validated internally and with external third-party scoring tools such as SCAP and Nessus.

Lockdown Enterprise represents yet another powerful step forward in automated baseline management. Certified content from Lockdown Enterprise can be integrated into any existing deployment and systems management tooling, or CI/CD workflows. And Lockdown Enterprise Roles are effective in any mode of deployment, including physical, virtual, cloud, or even in container builds.

*"Lockdown has literally saved us over 2000 staff-hours a year in a single environment."*

**-Education User**

*"Lockdown Enterprise delivers on the promise of rapid and highly configurable software baselining."*

**-Major Software Vendor**

*"We loved Ansible as a toolset, but struggled with the 'How'. Lockdown Enterprise is our new 'how.'*

**-US Government**

## Easily adapted to work in any environment

It's often difficult to implement any security policy in a dynamic IT environment. To apply every control within a baseline without breaking existing applications is very challenging. For practical use, baseline automation must be capable of adapting to existing configurations, application settings, and additional security policies. Using Ansible best practices, Lockdown Enterprise adds flexibility to any deployment by:

- Using variables and tags to categorize controls (CAT I and II category guidelines for instance).
- Excluding individual rules or categories of highly disruptive rules that might break things .
- Per-host overrides and configurations.
- Building your own custom controls on top of a local copy of Lockdown Enterprise.

Together with the power of Ansible, these capabilities make Lockdown Enterprise the most powerful, flexible, and straightforward method for the application and management of security baselines.