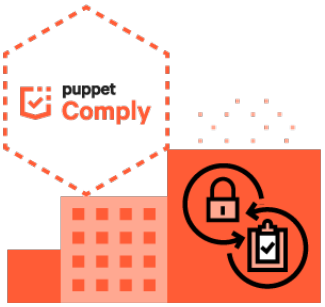
Compliance Enforcement Modules

Many organizations must comply with multiple regulations, and an increase in regulations has made being compliant and staying there challenging. Though several security frameworks are available to leverage for compliance best practices, the CIS (Center for Internet Security) benchmarks have become increasingly popular and trusted.



Organizations can make CIS benchmarks actionable to improve infrastructure security and compliance while increasing staff efficiency by utilizing automation technology and converting compliance policies into code.

But turning compliance policies into enforceable code can be complex and requires translating benchmarks into scripts or playbooks. Keeping up with updating ever-evolving benchmarks manually and managing exceptions with security teams can be daunting for any ITOps team.

Set and preserve compliant infrastructure configurations by automating the continuous enforcement of the desired state that aligns with your policies and security best practices.

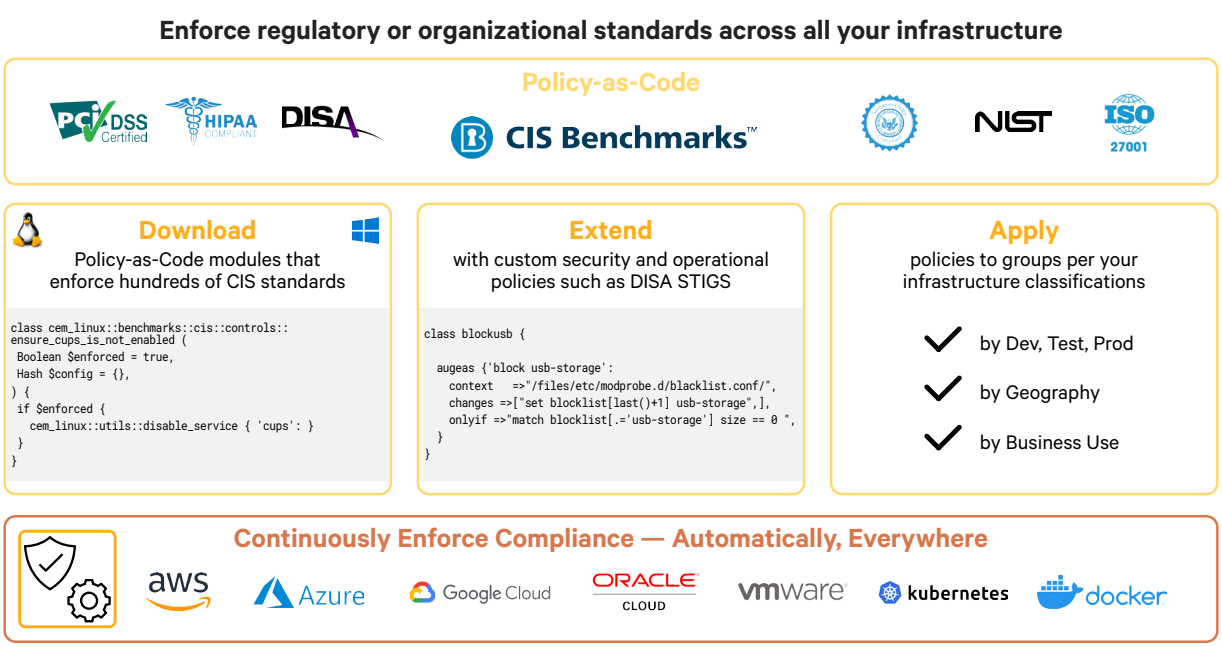
The Puppet Compliance Enforcement Modules (CEM) provides turnkey compliance remediation and enforcement policy-as-code directly aligned to the Center for the Internet Security (CIS) benchmarks for Windows and Linux, accelerating your time-to-value for the Puppet Comply solution.

CIS Level 1 benchmarks have hundreds of operating system settings contained in the benchmarks. Bridge the skill and resource gap by utilizing Puppet's ready-made Compliance Enforcement Modules subscription to achieve automation quickly. Puppet creates, maintains, and continually updates the CEM to stay up-to-date with the CIS latest recommendations, so you can trust you are reducing your compliance risk by remaining in a compliant state.

- Eliminate the pain of implementing and updating hundreds of configurations manually.
- Effectively automate the enforcement of compliance configurations based on the CIS benchmarks with turnkey enforcement code.
- Monitor and scan for infrastructure compliance policy violations and push into adherence with regularly updated policy-as-code enforcement modules to trust you are in a compliant state.
- Utilize comprehensive configuration options to tailor the content to fit your environment.

The Puppet Compliance Enforcement Modules support the below CIS operating system benchmarks:

OS	Framework	Details
CentOS 7	CIS	Profile Level 1 Server
RHEL 7	CIS	Profile Level 1 Server
Windows 10 Enterprise Release 202H	CIS	Profile Level 1 Corp. Enterprise
Windows Server 2016	CIS	Profile Level 1 Member Server
Windows Server 2019	CIS	Profile Level 1 Member Server
RHEL 8	CIS	Profile Level 1 Server



Additional Resources

Get continuous compliance with Puppet

https://puppet.com/products/puppet-comply/