Compliance Enforcement

The Compliance + Security Struggle.

Many organizations must comply with multiple security policies and regulations to protect critical data, control system access, and enforce security baselines. At the same time, an increase in regulations to meet secured infrastructure standards has made becoming compliant and staying there challenging.

Why Puppet?

Puppet's Compliance Enforcement solution provides a turnkey method to enforce system-wide compliance with security policy baselines at any scale. It reduces the risk of misconfiguration and drift within your Linux and Windows estate by utilizing Puppet policy-as-code (PaC) to automatically remediate and harden system configurations aligned to CIS Benchmarks, DISA STIGs, and more.

Security and compliance are hard at any scale. Benchmarks are updated frequently and even basic frameworks can contain hundreds of settings, meaning security is a moving target no matter what industry you're in; DIY security takes a huge amount of time and still leaves your infrastructure at risk; and manual configuration stifles business innovation by diverting precious hours to urgent, one-off tasks and firefighting.

Key Benefits

- **Harden system configurations to align with CIS Benchmarks and DISA STIGs to comply with PCI DSS, HIPAA, and more***
- **Improve system security to protect critical data, safeguard sensitive information, and pass audits**
- **Continuously enforce a hardened, compliant state at any scale, from small estates to enterprises**
- **Available for all Puppet instances, including Open Source Puppet****
- **Automate exceptions to dial in your ideal compliance**
- **Enforce Windows and Linux* configurations across hybrid infrastructure**

Turning secured infrastructure compliance policies into automation scripts or playbooks saves time and helps IT stay audit-ready, especially when those scripts are already **pre-configured to enforce continuous compliance** with the most demanding security frameworks.

Continuously Enforce Compliance — Automatically, Everywhere

aws Azure Google Cloud ORACLE CLOUD vmware kubernetes docker

*For a complete list of OS and benchmark support, visit the Puppet website.

**Minimum supported versions: Puppet Enterprise 2019.8.x, Puppet 6.23.0. For full information on supported versions, visit the readme for the Windows and Linux modules.

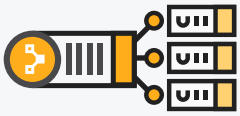
How Puppet Compliance Enforcement Works

BEFORE

Misconfiguration, drift, and lack of state enforcement limits security hardening and continuous compliance across deployments.

Manual configuration, remediation, documentation, reporting, and audit preparation can take hundreds of hours each year.

+ PUPPET COMPLIANCE ENFORCEMENT



Puppet policy-as-code maintains configurations across hundreds of thousands of servers to enforce common security and compliance frameworks.

Puppet agents continually check with the primary Puppet server to enforce the latest coded configurations.

AFTER

Continuous compliance is enforced across cloud, on-prem, and hybrid.

Puppet automatically remediates troublesome drift, prevents dangerous misconfigurations, and automatically generates documentation to streamline audit preparation.

Stay Secure

Enforce desired state configurations and automatically remediate drift.

Reclaim Time

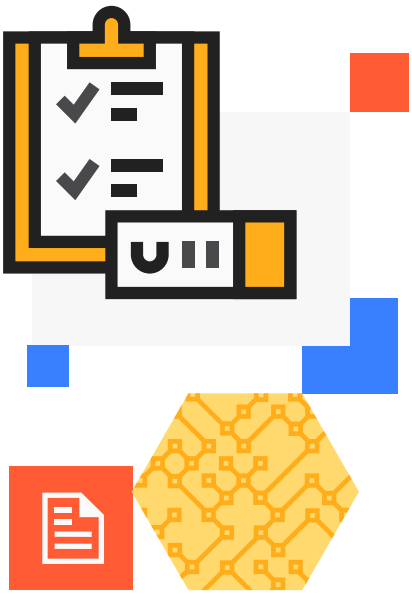
Give your team more time to tackle the work that drives business value by automatically configuring and updating baselines.

Stay Up to Date

Supported and maintained by Puppet, Compliance Enforcement is updated as new recommendations become available.

Enforce Your Ideal Compliance

Customize controls and apply policies to groups by geography, business use, and more.



For more on Puppet Compliance Enforcement, visit the Puppet website or request a demo today.