perforce Puppet

SOLUTION BRIEF

Security Compliance Enforcement

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

Why Puppet?

Security Compliance Enforcement provides a turnkey method to enforce system-wide compliance with security policy baselines in infrastructure managed by Puppet Core or Puppet Enterprise Advanced. 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 and DISA STIGs.

Security and compliance are hard at any scale. Benchmarks are updated frequently, and even basic frameworks can contain hundreds of settings. Manual configuration and DIY security takes a huge amount of time, wastes resources on firefighting, and still leaves your infrastructure at risk.

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.

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 Puppet Core and Puppet Enterprise Advanced**
- Automate exceptions to dial in your ideal compliance.
- Enforce Windows and Linux* configurations across hybrid infrastructure.

*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 Security Compliance Enforcement Works

Before

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

With Puppet

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

After

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

Stay Secure

Enforce desired state configurations and automatically remediate drift. 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.

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, Security 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.

Continuously Enforce Compliance — Automatically, Everywhere

aws · ORACLE · vmware by Broadcom · kubernetes · docker

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