

Self-Healing, Policy-Based, Continuous Compliance for Federal Agencies

Maintaining a continuously secure state across devices is complex and resource-consuming for federal agencies. Configuration standards include various controls and settings and are constantly changing. Last quarter's secure configuration may suddenly be vulnerable to a newly discovered exploit. Security configuration setup and management on the scale of a federal agency requires automation, simplicity, agility, and high confidence.

Puppet Enterprise: A better way to deliver continuous compliance and security

Puppet is the leader in automated information technology management solutions for the public sector. Our solution is proven in the federal government as highly adaptable to any IT development, test, and production environment, whether on-prem or in the cloud.

A US Government energy sector agency leveraged Puppet to take Linux servers from 30% to 98% STIG compliance. This reduced fines considerably while providing complete visibility over infrastructure.

Leveraging the strengths of open source Puppet, Puppet Enterprise enables agencies to define their infrastructure as code and then automate it. As a result, agencies can build compliance and security policies directly into their IT configurations, knowing they will be deployed efficiently, continuously monitored, and enforced as intended.

Our platform is built to support compliance on the scale required by federal agencies. It supports a multitude of checks on each agency IT asset, including everything from passwords and default settings to access rules and audit trail requirements.

Puppet offers a mature, intelligent enterprise platform that:

- Continuously checks for and enforces desired state every 30 minutes
- Escalates conflicting rule sets
- Dynamically discovers, filters, prioritises, and remediates at scale
- Operates in air-gapped environments
- Offers agent-based and agentless options
- Is complemented by the industry's largest ecosystem

Puppet Enterprise makes it easy for agencies to automate the tasks related to maintaining a continuously secure state and compliance with mandates. This allows agencies to rapidly discover, prioritise, and remediate new security vulnerabilities. Manage it and write it once; Puppet Enterprise makes sure it stays true.

Best-in-class, truly intelligent, continuous compliance enforcement

Puppet provides automated, real-time control and reporting capabilities to satisfy the Australian National Audit Office and internal security team audits. Once Puppet Enterprise brings an IT environment into compliance, it continuously monitors and verifies that all changes comply with pre-defined organisational policies. The platform dramatically improves agency compliance rates by:

- Checking every 30 minutes for compliance and drift
- Monitoring and verifying that any changes made comply with pre-defined organisational policies
- Intelligently escalating conflicting rules sets for proper visibility and correction
- Automatically remediating vulnerabilities, quickly adjusting systems back to their compliant state

Government-proven security and scalability

A central dashboard delivers rich, interactive graphical reporting. This provides a single source of truth to let security teams and auditors know exactly how infrastructure and applications are configured, their relationships, and their dependencies. In addition, Puppet Enterprise maintains agency IT environments at any scale, continuously enforcing, maintaining, and documenting security compliance with:

- Role-based access control (RBAC) to handle any agency configuration
- Continuous monitoring of system changes against the defined baseline
- Enforcement of security policies and desired states as defined by the Essential 8, ISM and CIS benchmarks
- Proven expertise in secure, mission-critical programs and large-scale environments

Enterprise-grade automation platform designed for the way governments work

Puppet delivers agency-wide team collaboration, orchestration, vulnerability remediation, support, and services. DevSecOps teams can test proposed changes for impact before implementation, modeling security-compliant IT environments in the cloud and on-prem. Puppet gives IT teams a common language to support version control, code review, continuous integration, and automated testing and deployment. The solution automates the tasks required to keep heterogeneous, enterprise-scale IT environments properly configured, with:

- Centralised compliance reporting across the entire agency
- Integration with well-known cloud platforms, operating systems, and network resources to automate and control the most common agency hybrid infrastructures
- Easy setup and implementation using over 6,600 reusable automation modules
- Real-time reporting to ensure quicker, less costly audits and faster remediation of configuration change issues

Puppet Enterprise streamlines compliance, infrastructure administration, and software delivery processes, freeing staff to focus on innovation. This translates into more efficient IT staff resources and far less time and cost dedicated to compliance, fines, and penalties.



The shortest path to better software.

Learn more at puppet.com/government