Assured Security Compliance for Federal Agencies

A critical component of any federal cybersecurity program is ensuring that operating systems, applications, network devices, and other assets are properly configured to be secure. But the task of security configuration management for a government organization is complex, highly laborious and time consuming, and notoriously difficult to get right.

Each IT asset may require a multitude — in some cases, many hundreds — of checks on everything from passwords and default settings to user access rules and audit trail requirements to determine if current configurations are meeting government standards. These configuration policies include the Defense Information Systems Agency's Security Technical Implementation Guides (STIGs), Federal Information Security Management Act (FISMA), and the National Institute of Standards and Technology's Security Content Automation Protocol (SCAP).

IT security teams may spend days or weeks inspecting an exhaustive checklist of settings and correcting any that are out of compliance. Moreover, these configuration standards change constantly because new vulnerabilities are constantly discovered, new threats and angles of attack emerge, security practices continue evolving, and organizational risk management profiles are re-calibrated to meet shifting mission needs. A configuration deemed as secure last quarter may suddenly be vulnerable to a newly discovered exploit today. This means agencies must continually monitor and audit their IT assets against federal configuration standards to keep pace with the threat landscape.

The bottom line is that security configuration management on the scale of a federal agency requires automation, simplicity, agility, and high confidence.

Puppet: A better way to deliver assured security compliance

Puppet, the recognized industry leader in automated security configuration management solutions for enterprise-scale organizations, enables agencies to define their infrastructure as code so they can build security policies directly into their IT configurations and know they will be deployed, continuously monitored, and enforced as intended. A proven open source solution that is highly scalable, Puppet is adaptable to any IT development, test, and production environment, whether on premises or in the cloud. And it is supported by a robust global community of experts and developers.

Many federal and government agencies rely on Puppet for enforcement of security and compliance standards and to enable them to adopt DevOps best practices like infrastructure as code. Puppet Enterprise offers support for FIPS, IPv6 and 508 compliance to ensure federal government customers can adopt DevOps best practices, like infrastructure as code.

Puppet offers a single solution that:

- Ensures your security policies are enforced across all your systems and devicesconsistent security compliance throughout the IT infrastructure
- Generates reports automatically to document compliance
- Supports the most robust DevSecOps processes

Puppet delivers the following value to federal agency security programs:

Improved security compliance and configuration consistency. Puppet helps federal agencies dramatically improve compliance rates by automating the tedious work of keeping heterogenous, enterprise-scale IT environments properly configured and patched. Once Puppet brings an IT environment into compliance, it continuously monitors the infrastructure and verifies that any changes made are correctly enforcing organizational policies. When differences are detected, Puppet automatically remediates systems back to their compliant state. Being able to bring IT environments into compliance with accepted configuration standards — and then to continuously monitor, maintain, and document that compliance — enables Puppet to serve as an important security control for Risk Management Framework (RMF) programs.

Accelerate time to value for STIG and other compliance activities. STIG and other compliance activities are reduced from weeks or days down to minutes. Puppet's ability to automate the laborious processes of bringing sprawling IT infrastructures into compliance with security configuration policies, keeping them in compliance, and producing audit trails to demonstrate compliance translates into more efficient use of IT staff resources, less time and cost dedicated to compliance activities, and the avoidance of penalties for noncompliance.

Satisfy Cyber Readiness Inspections with real-time reporting and compliance documentation for audits. Puppet provides agencies the robust, automated, real-time reporting capabilities they will need to satisfy Command Cyber Readiness Inspections (CCRIs), inspector general's audits, or internal security team audits. With Puppet, agencies can easily push out new security configurations and document those steps. Puppet provides rich, interactive graphical reporting so security teams and auditors know exactly how infrastructures and applications are configured, the relationships between them, and their dependencies. Reporting functions track changes in real time, including who made changes and why — and that translates into quicker, less costly audits and faster remediation of any issues that arise due to configuration changes.

Adopt DevSecOps practices with ease. Puppet enables agencies' DevSecOps teams to model security-compliant IT environments — whether cloud-based or on premises — in an automated fashion to develop and test software so new applications run, operate, and are as secure as expected. Moreover, Puppet gives IT teams a common language to successfully adopt DevSecOps practices, such as version control, code review, automated testing, continuous integration and automated deployment.

Better use of IT staff resources. Automate the siloed processes involved in managing security compliance, IT infrastructure administration, and software delivery so agencies' IT staff can focus more on innovation, not maintenance.

For more on how Puppet can help federal agencies, visit puppet.com/government.