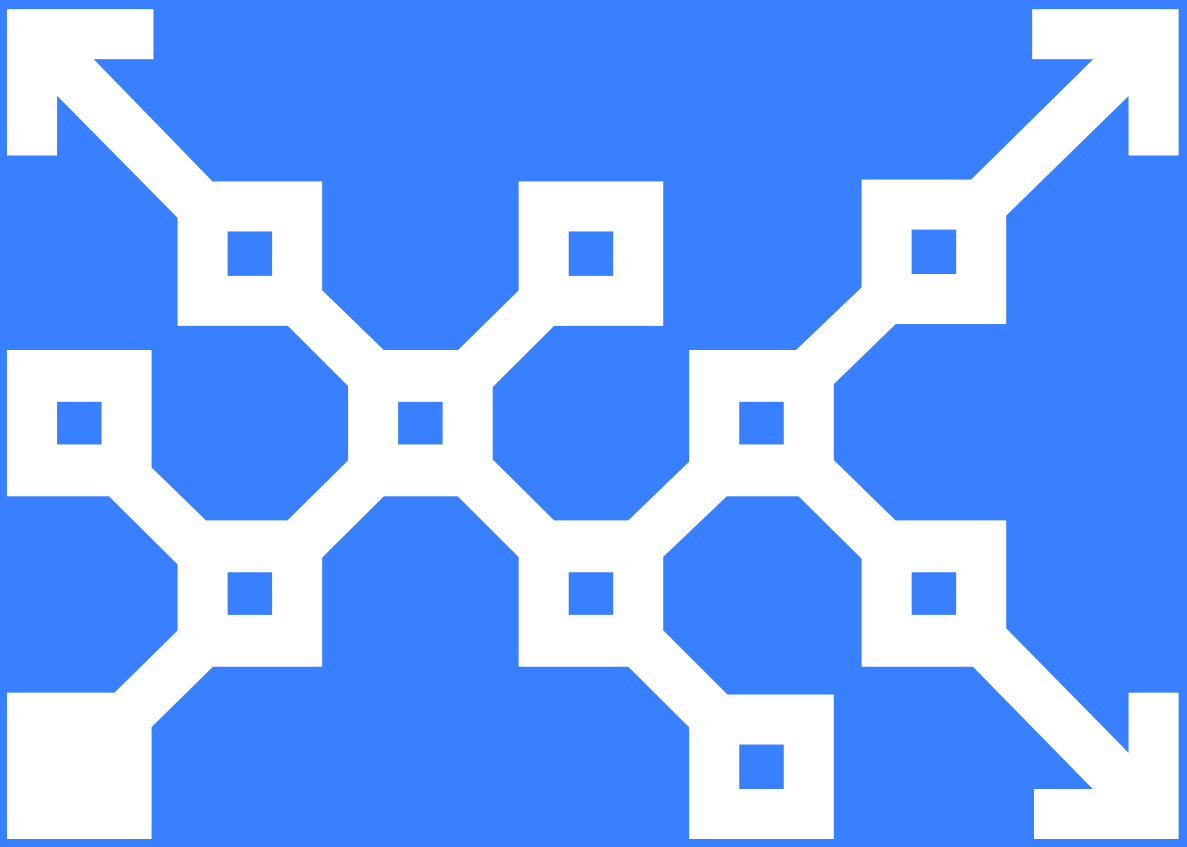
puppet

WHITE PAPER

How Automation Helps You Harden Your Systems and Become Compliant



Contents

Introduction

Compliance may not be the top line item in your IT budget, but with new regulatory requirements and security standards presenting themselves at an accelerated rate, it soon might be. A recent Ponemon Institute report found that in the United States, organizations with fewer than 5,000 employees commit 14.3% of their IT budgets to compliance. That figure is expected to keep increasing for organizations of every size.

IT automation can help you buck this trend. Automation lets IT operations teams proactively deal with inevitable compliance-related work. IT automation can be eyes and hands for your security — providing complete, real-time visibility into your IT state and ensuring security protocols can be consistently enforced.

In this white paper, we will establish the critical role of automation in meeting security requirements and demonstrate how Puppet solutions help you sustain compliance at scale, more easily prepare for audits, and integrate better with your security team.

The hard reality of always-on compliance and security

Whether protecting transaction data, securing sensitive patient health records, or attempting to clearly demonstrate the accuracy of your corporate disclosures to auditors, your IT operations are always addressing security vulnerabilities and meeting the demands of regulatory compliance.

In addition to meeting regulatory demands, many industries and organizations adopt mission critical security standards. Deployment falls to the IT team, be it initiatives to adopt cyber security best practices as laid out by the Center for Internet Security (CIS), adhere to guidelines put forth by the National Institute of Standards and Technology (NIST), or meet industry data security guidelines like PCI-DSS.

How your team handles tasks associated with compliance-related work directly impacts how much time and effort goes into meeting common requirements.

- What tool or tools are in use to ensure data at rest is encrypted using an acceptable encryption method such as Advanced Encryption Standard (AES) with strong enough keys?
- How do you address unauthorized changes to system configuration or prevent configuration drift?
- Do your transport layer security (TLS) best practices make certain your systems consistently use the latest, strongest TLS version and cipher configuration for secure communication?
- How do you verify network time protocol (NTP) clients are always properly configured to synchronize all critical system clocks and times?
- Are password policies and file permissions consistently enforced across all systems and services?
- Are your systems consistently updated with the latest security patches and hardened against the latest exploits and vulnerabilities?
- What level of automation is in place for removal of unneeded packages, unneeded default user/guest accounts, and unneeded services?

How your team handles tasks associated with compliance-related work directly impacts how much time and effort goes into meeting common requirements.

No one wants to see one of these questions in an email from the compliance officer, because it likely means a vulnerability has been revealed. Nothing diverts or distracts the IT team like the resulting scramble to determine what department is using which encryption tool or how the new guy was able to set his password as password and get away with it.

The critical question lurking behind all of these functions: Are you addressing security and compliance needs proactively or reactively?

Continuous security and manual tasks are like oil and water

They just don't mix. Synchronized enforcement of policy over time, at scale, relies on automation. Doing it all manually is painful and isn't really an option anyway. Presumably no IT operation would attempt something like manually configuring hundreds of security settings on thousands of Windows servers.

With new threats and regulations presenting themselves almost daily, even the most disciplined organizations have difficulty predicting how much resource will be devoted to security and compliance. A recent Forrester study demonstrated that most IT operations could only estimate their security spend in wide ranges (21-30% of total IT budget) and would need to build in "room to surge" at any time.

The right process and technology should be put in place to ensure the people in every corner of the organization always adhere to all of your security protocols — even as they adapt and expand to meet changing needs.

Just understanding the needs of the compliance department and keeping a strong security posture is not enough. It takes more than just recognizing the need to harden the default Windows 10 password policy. The right process and technology should be put in place to ensure the people in every corner of the organization always adhere to all of your security protocols — even as they adapt and expand to meet changing needs.

- **Sound process** allows your teams to adhere to standards and have systematic, prescriptive methods that make it easier to adopt and repeat them. It is built on infrastructure as code and compliance as code, helping simplify audits, because the documentation of steps and configurations is integrated in the code.
- **The right technology solution** provides more effective and consistent use of technology stacks that allow your organization to minimize overall risk and realize faster response times.
- **Your people** become more efficient and able to focus on value-driven initiatives — freed from mundane and error-prone tasks, relying on repeatable and consistent automation.

The Puppet approach to IT automation

We promote a proactive approach to vulnerability remediation — one that helps reduce the entire organization's exposure to external attacks. Reducing risk through continuous enforcement of regulatory and security policies across the whole infrastructure maintains high compliance standards, everywhere.

At scale, automation is a must have

You can only perform tasks manually up to a certain point. Sure, it is possible to configure a new server, maybe even a couple, to pass muster with configuration/security audits, but 50 servers? 100?

Automation of configuration management offers you significant advantages when it comes to security, not the least of which is the ability to rapidly scale. Automated configuration management means you describe the configuration in a manifest once, then those settings are applied to your entire ecosystem and maintained until you change them. Once considered an annual chore, policy reviews happen more frequently and for a variety of reasons such as accelerated growth, new technology adoption, or additional compliance requirements.

We cannot adequately stress the continuous nature of working to address ever expanding regulatory standards. One minute it is high fives all around after successfully making your entire tech stack General Data Protection Regulations (GDPR) compliant, then someone emails you specs for the California Consumer Privacy Act (CCPA) — legislation with a completely different set of rules regarding data deletion and the definition of personal data, as well as requirements for unique, secure, and exclusive communications channels for California residents.

There are plenty more states and countries out there, many of which are considering similar, yet different, legislation. Who wants to apply new settings server by server or department by department, every time a new regional privacy regulation emerges? Even if some business units have deployed automation tools, this activity can bust your budget, distract from important technology initiatives, and leave your systems at risk for too long.

A better approach is to protect your organization by continuously enforcing security and regulatory policies across your entire infrastructure with a tool that works in hybrid environments and at scale.

A better approach is to protect your organization by continuously enforcing security and regulatory policies across your entire infrastructure with a tool that works in hybrid environments and at scale.

Automation ensures consistency, compliance, and security — at scale

This means you need to define your infrastructure and policies as code. A key DevOps practice used in conjunction with continuous delivery, infrastructure as code can remove the burden of compliance from individual teams who would otherwise be responsible for maintaining security and compliance settings in their individual deployment environments.

Automation lets you set your defined compliant state across your entire IT state via infrastructure as code. No more manually searching for new servers improperly configured or changes to individual deployments.

As long as automation software is installed on the host, it can identify changes to your configuration that do not adhere to established policies, so they can be secured and managed properly moving forward. Think of automated compliance as a Roomba for your technology stack. Whenever manual change is made to an individual system, the automated configuration manager makes a corrective change and reports it immediately.

Continuously monitor, enforce, and remediate using automation, so you know all deployments will stay in their compliant state.

Automation can make preparing for audits easier and faster

Prepping for an audit can be a grueling time, spent confirming that every machine, VM and container is in a compliant state. Are standards being enforced, everywhere, always? Can users be prevented from developing workarounds or shortcuts to bypass annoying or cumbersome security procedures?

With automation including compliance as code, you rest easy because you know the answer to those and any other auditor questions before they are asked.

When you can demonstrate compliance by showing auditors code that applies to and enforces specific requirements, everyone's job becomes easier.

Automated reports make audits quicker and less costly. They can clearly demonstrate compliance — easily showing auditors your infrastructure, how systems are configured, and that you have fulfilled security requirements.

Automation frees you from the hassle of compliance

The traditional relationship where IT reacts each time the security team discovers a compliance issue can create both delay and friction. Automation, or in this case compliance as code, builds policy into systems configuration. Once both security and IT operations begin speaking to compliance in a common language, the teams become better aligned.

This cohesiveness is born from IT automation, not a Kumbaya moment. It creates a seamless flow of data and accelerates remediation. Both IT and security rest easy knowing the organization is in compliance because the systems were configured to be just that. This reduces compliance overhead and focuses IT operations on strategic initiatives that drive innovation and growth.

Automation should reduce friction between compliance and IT, because the paradigm shifts from "How can we help you?" to "Here is how we are already helping you."

Automation should reduce friction between compliance and IT, because the paradigm shifts from "How can we help you?" to "Here is how we are already helping you."

Puppet Enterprise

Compliance automation is just one element of an enterprise-wide, model-driven, and task-based approach to software automation. Puppet Enterprise delivers a unified platform enabling you to both enforce the desired state of your configurations and automatically remediate any unexpected changes to it. It is a single platform that allows you to automate on demand and achieve ongoing compliance.

Puppet Enterprise integrates with the monitoring tool Splunk and interfaces with cloud providers like Azure and AWS. We also make it easy to use secrets from stores like Hashicorp Vault, Azure Key Vault, and AWS Secrets Manager. Puppet Enterprise makes automation easier across all platforms including Windows clients, and it integrates with PowerShell.

Fervid, a DevOps consulting firm located in Pontiac, Michigan, needed a compliant solution for hardening Windows servers and eliminating cumbersome manual provisioning tasks at the United States Forest Services (USFS). Upon deploying Puppet Enterprise, Fervid was able to:

- Develop a Windows-hardening module to ensure compliance
- Merge multiple data centers
- Accelerate changes to applications on infrastructure services with better quality and less downtime

The Dutch permissions marketing leader ResponseConcepts turned to Puppet for help with continuous IT automation during a time of rapid expansion. Compliance was at the forefront of discussion because of GDPR compliance requirements. “When it comes to GDPR, you need to prove that a system is the way you say it is. Any changes made are reverted back to the environment you define within Puppet Enterprise,” said Jacco van Koll, systems administrator.

With the help of Puppet, ResponseConcepts achieved the following:

- Less time spent configuring and maintaining systems
- Faster deployments taking minutes versus hours
- Higher productivity rates
- More focus on innovation and the development of new services

Puppet Enterprise gives you a full set of capabilities to manage IT infrastructure and applications across your entire software delivery pipeline.

Bolt

Bolt is an open source, agentless orchestration tool. It runs on-demand, ad hoc and one-time automation tasks across all of your systems using SSH or WinRM. Run scripts in any language or write them using the Puppet framework, collaborate with your compliance team on benchmark sets, run compliance tests on Bolt or Puppet Enterprise, and integrate with any reporting platform you choose.

"Bolt makes this company more profitable, more automated, with less engineers working overtime."

Nick Maludy
DevOps Manager
Encore Technologies

Conclusion

IT operations and security compliance teams work in tandem to reduce risk and make organizations more secure. Configuration automation solutions like Puppet make it easier to implement and be compliant to standards — sustaining compliance at scale and maintaining continuous compliance to achieve the required level of security.

Puppet is driving the movement to a world of unconstrained software change. Its revolutionary platform is the industry standard for automating the delivery and operation of the software that powers everything around us. More than 40,000 companies — including more than 75 percent of the Fortune 100 — use Puppet's open source and commercial solutions to adopt DevOps practices, achieve situational awareness and drive software change with confidence. Headquartered in Portland, Oregon, Puppet is a privately held company with more than 500 employees around the world.

Learn more at puppet.com

linkedin.com/company/puppet

twitter.com/puppetize

facebook.com/puppetsoftware