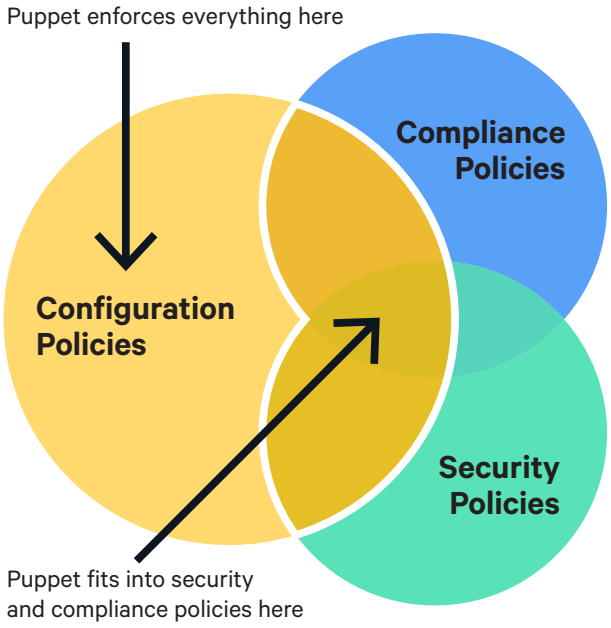
The shortest path to better security and compliance

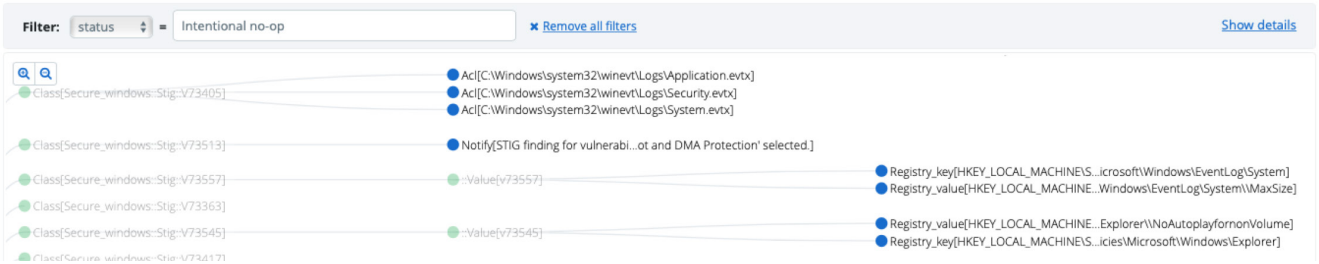
With the proliferation of high-profile hacks, data breaches and ransomware, it's easy to feel insecure about your organization's security these days. The not-if-but-when prognostications are, sadly, true. You have to protect your organization and its reputation like never before — particularly as your infrastructure grows and diversifies, presenting a broader front for attackers.

Not all security issues have to do with purposeful hacks and attacks. For many IT teams, the challenge is maintaining strict rules and regulatory requirements for everything from credit card data to health information privacy. Failing to maintain compliance can put your organization at risk of everything from lost business to substantial fines — or worse.

With Puppet, you can create and enforce better processes that can help safeguard against tampering by both internal and external sources, with automated corrective action. It all begins by establishing a baseline.

Establishing a common baseline is a great way to improve security, because it forces you to define what you want and need. Many teams don't do this, even though security experts tell us the surest way to detect a problem is to know what you have in the first place. If the baseline is not written down anywhere, how does your team distinguish between a policy and a security hole?





The key to Puppet's powerful capabilities is the Puppet language (DSL), which is easy to read, understand and share. Puppet code is executable documentation that describes the desired state of a resource.

Want all your Active Directory domain controllers to run on best practice security policies?

Grab the secure_windows module from the Puppet Forge and have direct access to enterprise-level compliance.

Want to test your servers against CIS compliance?

With the secure_linux_cis and harden_windows_server modules you will have all the CIS rules translated into enforceable Puppet code, ready to go.

Want to test for compliance first, without actually making any changes?

Use Puppet's no-op mode to quickly find out which changes would be needed to bring a system into full compliance.

Puppet can also help you catch up and keep up with routine tasks like patching.

Outdated or missing security patches are a common source of breaches, but Puppet can automatically keep everything up to date — even on different platforms. It can also remember to change passwords, and make sure they meet modern requirements.

If you'd like to learn more about Puppet's capabilities for security and compliance, contact us.