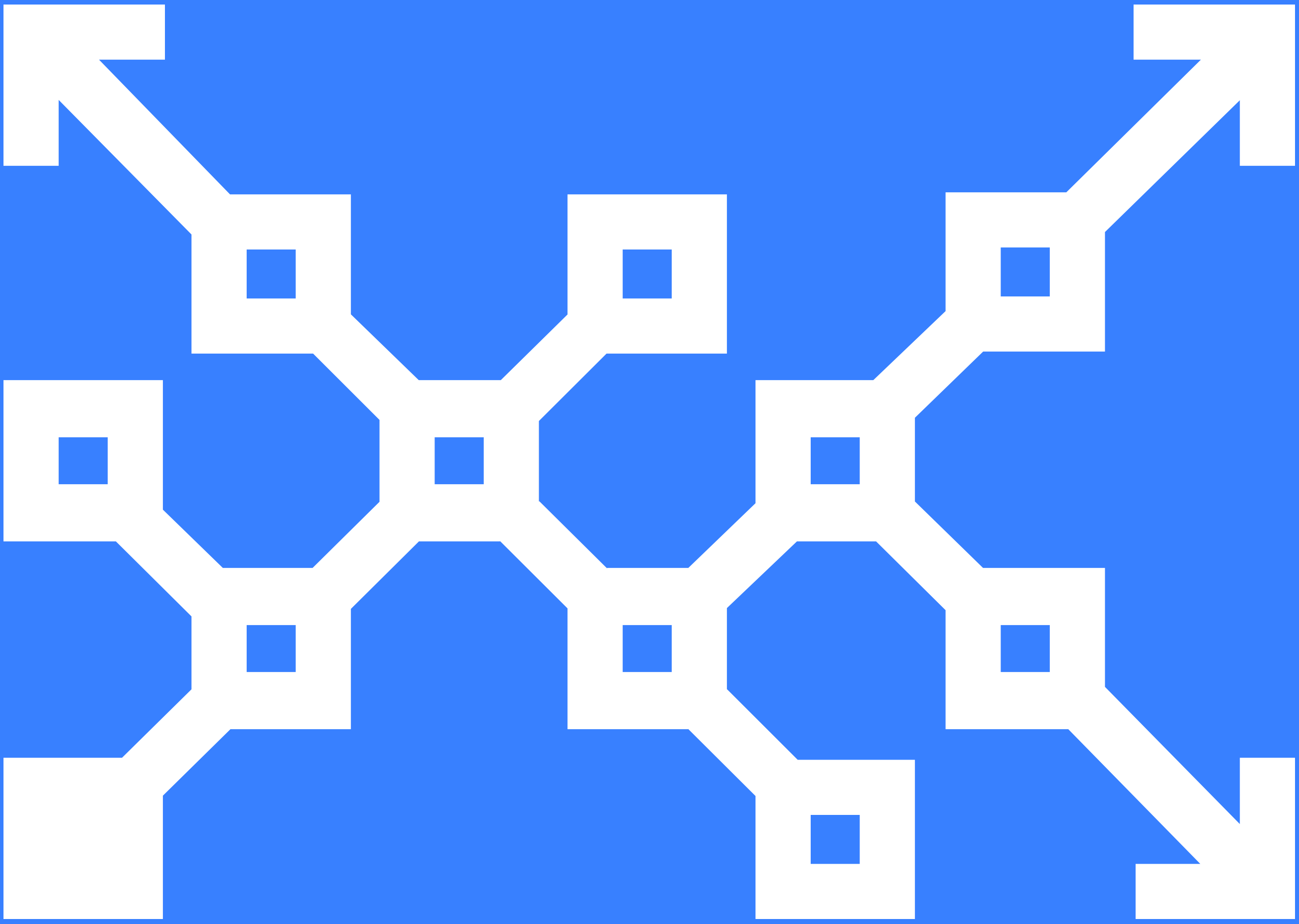
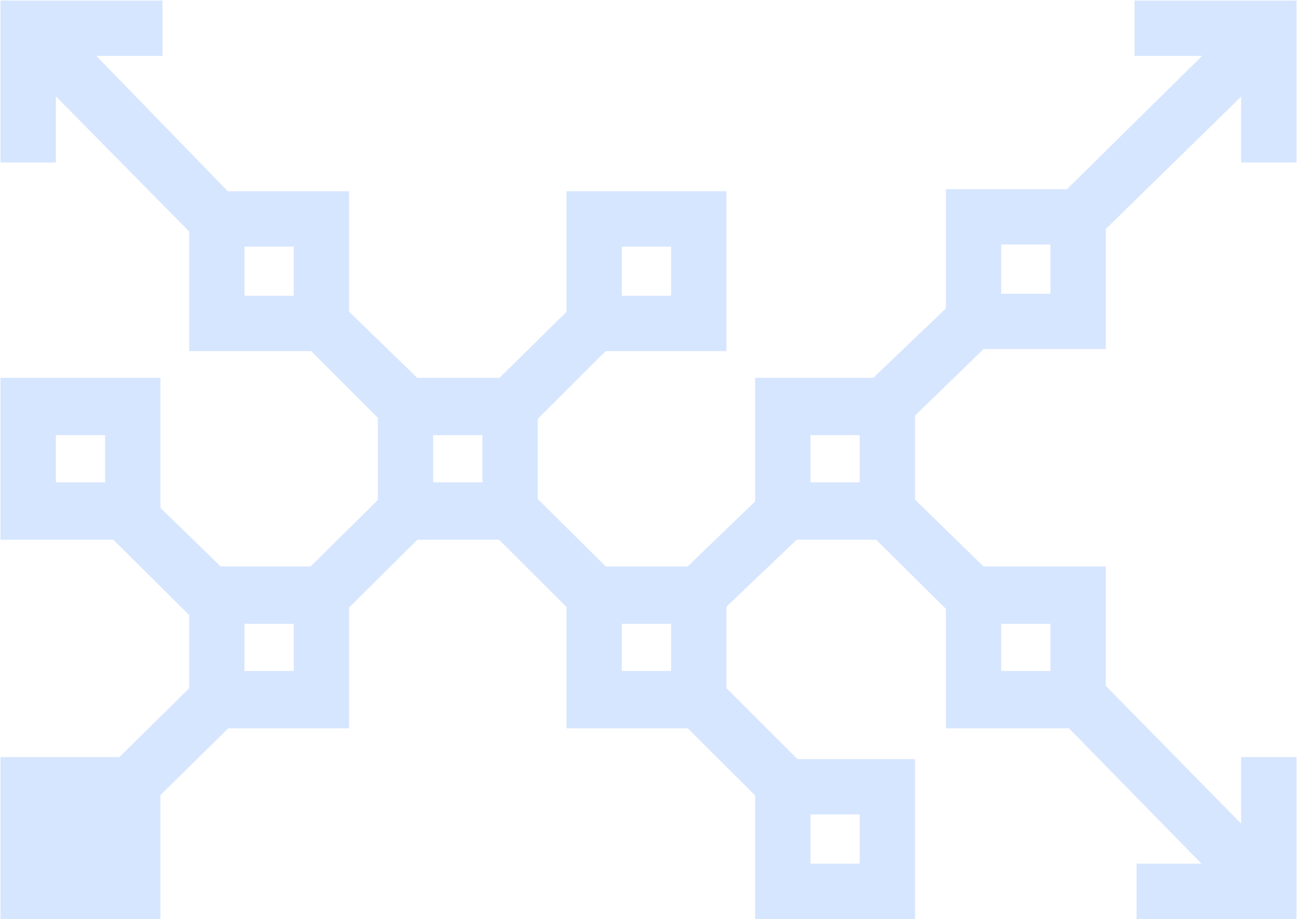
WHITE PAPER

Maximizing IT Security with Configuration Management



puppet

Contents



Overview

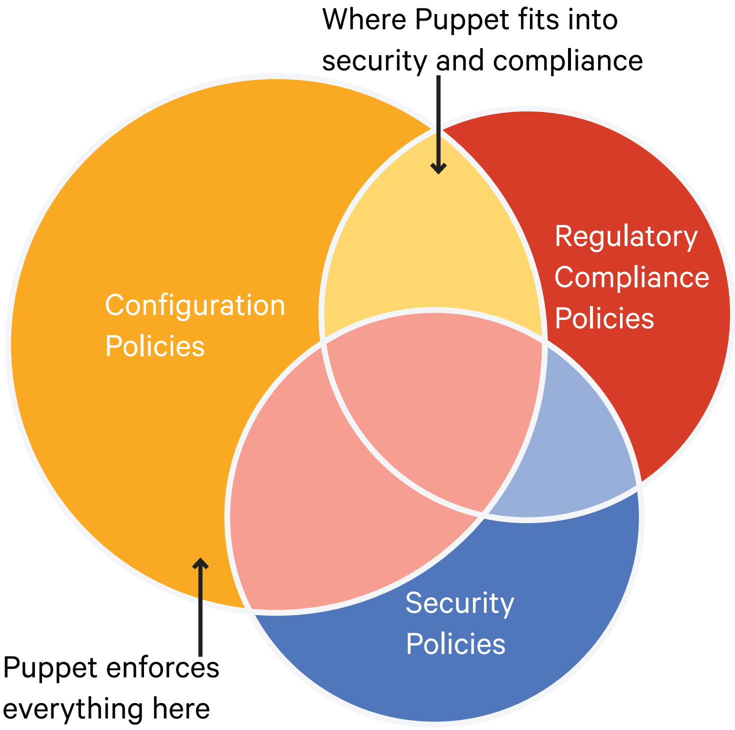
Despite large investments in technology and employee expertise, IT security remains a persistent headache with organizations across a spectrum of industries falling victim to attacks. Security spending reflects this increasingly costly threat. Market research firm Gartner says the world will spend $101 billion on information security by 2018.

While security encompasses a wide spectrum of technologies and specific organizational requirements, any best practice security plan incorporates some form of configuration management process and technology. The basis of configuration management concerns itself with establishing and maintaining a known and consistent state of the physical and software elements on any given IT resource. When it comes to IT security, configuration management can play many roles including playing an important part in the following elements of an Information Security architecture:

- Establishing a Standard Operating Environment (SOE) and meeting IT security standards.
- Reporting on or controlling configuration drift and providing change remediation.
- Supporting audit requirements and forensic analysis.
- Providing configuration knowledge and insight to assist with security patch management.

This paper examines the key security benefits of configuration management and touches on how Puppet Enterprise can help maximize these benefits.

Configuration, security, and compliance policies


Where Puppet fits into security and compliance
Configuration Policies
Regulatory Compliance Policies
Security Policies
Puppet enforces everything here

With Puppet Enterprise you define your security configuration policies as the ideal state every configuration should be in. Then, Puppet enterprise will continually compare the actual infrastructure configurations to the desired state defined in your policies. Differences are detected and automatically remediated to continually converge infrastructure to the policies.

This approach unifies configuration policy deployment, monitoring, and remediation, eliminating the need for separate tools, processes, and scripts for each step. To Puppet Enterprise, it's all the same thing and it all derives from the desired state defined in the security policies. For newly provisioned operating systems, most configurations will out be out compliance since the operating system hasn't been configured yet. Puppet Enterprise determines which configurations are out of compliance and works to remediate each one. To ensure systems stay compliant over time, Puppet Enterprise performs the same comparison and automatic remediation process regularly, every 30 minutes by default.

Each time Puppet Enterprise compares and remediates compliance with the policies, a report is sent showing what remediations, if any, took place, allowing you to be confident your infrastructure is compliant and prove it at any time.

Establishing a Standard Operating Environment (SOE) and meeting security standards

One of the first places that configuration management contributes to an organization's overall Information Security architecture and policy adherence is in establishing an SOE. This term is used to describe a standard implementation of an operating system and its associated software. A SOE helps IT Ops and security teams set consistent, automated and managed IT security standards across the organization. Establishing a manageable number of SOEs across your various platforms provides several key benefits:

- Provides a key element of a successful vulnerability management program.
- Reduces the time and cost of deploying and managing your systems and applications.
- Accelerates patch distribution by reducing the variety of computer configurations and automating patch deployment.
- Accelerates IT security incident response.

Using configuration management tools like Puppet Enterprise to support an SOE is an important element in meeting many security standards. A good example of this is the Payment Card Industry Data Security Standard (PCI DSS) requirement to Maintain a Vulnerability Management Program. In Requirement 6 of this Standard, you are required to "develop and maintain secure systems and applications. This requirement covers a wide variety of IT security measures but specifically addresses change control, patch management and vulnerability assessment. All elements that are supported by configuration management processes and the maintenance of an SOE.

The PCI DSS requirements are not the only standard that calls for establishing a secure environment. Maintaining a known configuration across your systems and defining the processes for handling change on those systems is an IT security best practice and shows up in most IT security guidelines. This is what Puppet Enterprise does best.

Puppet Enterprise allows you to define a desired state for your systems and quickly deploy that state across thousands of systems. Puppet Enterprise supports change control by allowing you to define and update the desired state of your systems in the form of reusable modules that can predictably maintain and update computing resources. In fact, Puppet offers over 3,800+ modules to help you meet security requirements, available on the Puppet Forge.

Managing, reporting on and remediating configuration drift

Closely linked to SOEs and change control is the threat of drift. Simply put, configuration drift is the change that occurs to software and hardware configurations that take them out of a supported SOE configuration. With the sheer size of today's data centers and enterprise computing environments, changes are inevitable and occur as a matter of course in running and supporting a computing environment.

The danger of configuration drift is that changes can take systems out of a known secure and updated state and undermine other requirements like high availability and disaster recovery. The reason that drift is so prevalent is that most organizations don't recognize that system configurations have changed until they cause a problem.

Organizations looking to establish configuration management procedures and prevent configuration drift should ensure they meet the following objectives:

- **Establish and ensure a standard baseline configuration.** This is the starting SOE and should be defined by the requirements of each SOE group. The configuration should guarantee a homogeneous environment across these systems and should update only under known and approved circumstances.
- **Identify and report on configuration drift.** You should have tools in place that can identify systems that no longer adhere to their intended SOE and report that to the appropriate administrator.
- **Provide a change remediation capability.** Identified changes in SOE should be able to be reverted back to the approved SOE.

Configuration management automation tools like Puppet Enterprise play an important role in minimizing the impact of configuration drift and maintaining a known SOE on computing resources.

Gaining configuration knowledge and simplifying patch management

One of the more resource intensive aspects of managing IT assets is security patch management. The pace of botnet and malware infection is at an all time high and the requirement to identify and patch vulnerabilities has never been more important.

In Q1 of 2015 alone, Kaspersky Labs detected 2,205,858,791 malicious attacks on computers, including mobile devices, and 93,473,068 unique URLS were identified as malicious. As a result, every major security standard and regulation contains requirements for combating malware through patch management.

Often times IT security patches are distributed in response to a time sensitive threat and the resulting fire drill consumes significant IT resources. Many times the source of the headache is simply determining which resources must be patched. Configuration management solutions combined with a known SOE can make this process significantly easier.

When it comes to IT security patch distribution, your configuration management solution should be able to facilitate the following processes:

- **Establish and monitor SOEs.** Effective patch management begins with knowing the state of your configuration on your IT assets in real time. SOEs reduce the variety of configurations to be dealt with and configuration management oversight can report on and remediate drift from these baseline configurations.
- **Identify priorities for patch distribution.** IT security patch distribution then begins by identifying the appropriate SOEs and assets that are impacted by the new patch. IT administrators will immediately know which resources need the update instead of having to query each endpoint.
- **Test patch on SOE.** Often the real time killer with IT security patching is testing. Because of the reactive nature and rapid distribution of IT security patches, it is essential to test the patch to ensure that it doesn't negatively impact critical hardware or software or open new security vulnerabilities. Without a reduced set of known SOEs this is an almost impossible task. Known configurations allow IT groups to test on the affected configurations quickly and efficiently to ensure rapid distribution.
- **Distribute patches as part of change control process.** Once the targets for patching are identified and the patch is tested, the patch can be distributed to the appropriate hosts. As a part of the standard change control process, the SOEs are updated and your configuration management software should immediately reflect the updated configurations.
- **Validate and log successful patch outcome.** The results of the patching should be immediately available via reports and come with a complete audit trail of the actions taken on an endpoint. This audit trail proves that patching has occurred and is important in satisfying the audit and regulatory requirements for maintaining a vulnerability management process.

Configuration management compliance relevance

As we have mentioned in several of the sections above, configuration management plays an important role in many IT security standards and is called out in individual requirements. It is important to separate claims from unfortunate hype that can often be found around tools satisfying regulatory requirements. There is no single tool that can magically satisfy the requirements of a given regulation. Regulatory standards, by their nature encompass a wide variety of IT security processes and technology. Configuration management solutions like Puppet Enterprise can be used to satisfy components of IT security regulations. Typically these requirements fall in one of the following categories:

- **Change control.** Many regulations specify implementing a change control process. One example of this is the PCI DSS standard. Requirement 6.4 calls for the organization to "follow change control processes and procedures for all changes to system components." Requirements for change control can also be found in NIST 800-53 requirement CM-3 configuration Change Control and a variety of other regulations.
- **Auditing requirements.** Auditing is also required by the vast majority of IT security standards. The specific requirements vary by standard but maintaining a log of IT security patching and changes to an organization's SOE is common across many of them. Configuration management tools like Puppet Enterprise record changes to endpoint configurations and log the user that made the change.
- **Vulnerability management.** Vulnerability management and anti-malware readiness are uniformly included in IT security standards. The requirement to defend computers against attack and keep them updated with the latest patches is a cornerstone of IT security regulations. Whether an organization is working to meet PCI DSS, NIST 800-53, Sarbanes-Oxley, HIPAA, GLBA or other IT security standards, configuration management process and tools often play an important role in that process. Puppet Enterprise has helped numerous customers meet IT security requirements and provide simple audit trails and reports to demonstrate adherence to specific guidelines.

Puppet Enterprise configuration management

When one is looking at the IT security capabilities of a specific configuration management tool, it is often helpful to review its specific IT security relevant features. The Puppet community and team is extremely well versed in IT security issues and Puppet Enterprise was built to facilitate a scalable, predictable and secure required remediation and all the things that didn't require remediation. Since Puppet Enterprise runs every 30 minutes by default, you know your systems are always in the desired state configuration and can prove it at any time.

Conclusion

Configuration management tools and processes play an important role in supporting a secure enterprise. Whether your goal is to establish a SOE, control configuration drift, manage and audit a change control process, or support vulnerability management and patch distribution, configuration management tools like Puppet Enterprise are an essential element of the solution.

Give Puppet Enterprise a try:

Download Puppet Enterprise

Download our Learning VM

Questions?

Contact sales