DATASHEET

Puppet helps achieve security compliance with 6.5 of the ACSC Essential Eight

The Australian Cyber Security Centre (ACSC) has developed *Strategies to Mitigate Cyber Security Incidents* to help organisations protect themselves against various cyber threats. The most effective of these mitigation strategies is the Essential Eight, which are further described below and available in detail on the ACSC's website. When all of the Essential Eight mitigation strategies are implemented, together they provide an effective baseline for cyber defence.

The ACSC has developed three maturity levels for the Essential Eight:

- **Level 1:** An organisation has implemented all eight controls to an acceptable initial standard.
- **Level 2:** An organisation has achieved implementation of more stringent controls across all eight of the mitigation strategies.
- **Level 3:** An organisation has achieved implementation of the most stringent controls across all eight of the mitigation strategies. The ACSC recommends that all non-corporate government entities should seek to achieve compliance with maturity level three.

Non-corporate government entities are required to regularly self-report against compliance with the Essential Eight, and are also subject to periodic audits undertaken by the Australian National Audit Office for compliance with the Essential Eight. These internal and external audit activities can be time-consuming and pull resources away from other priorities.

Customer benefits

- Use infrastructure as code and IT automation to simplify compliance with the Essential Eight.
- Reduce the time taken for self reporting and audit compliance with the Essential Eight.
- Reduce IT spend and the number of tools required to achieve compliance with the Essential Eight.

Expected outcomes

- Automate and simplify Essential Eight compliance.
- Pass audits for Essential Eight compliance with less fuss and effort.

puppet

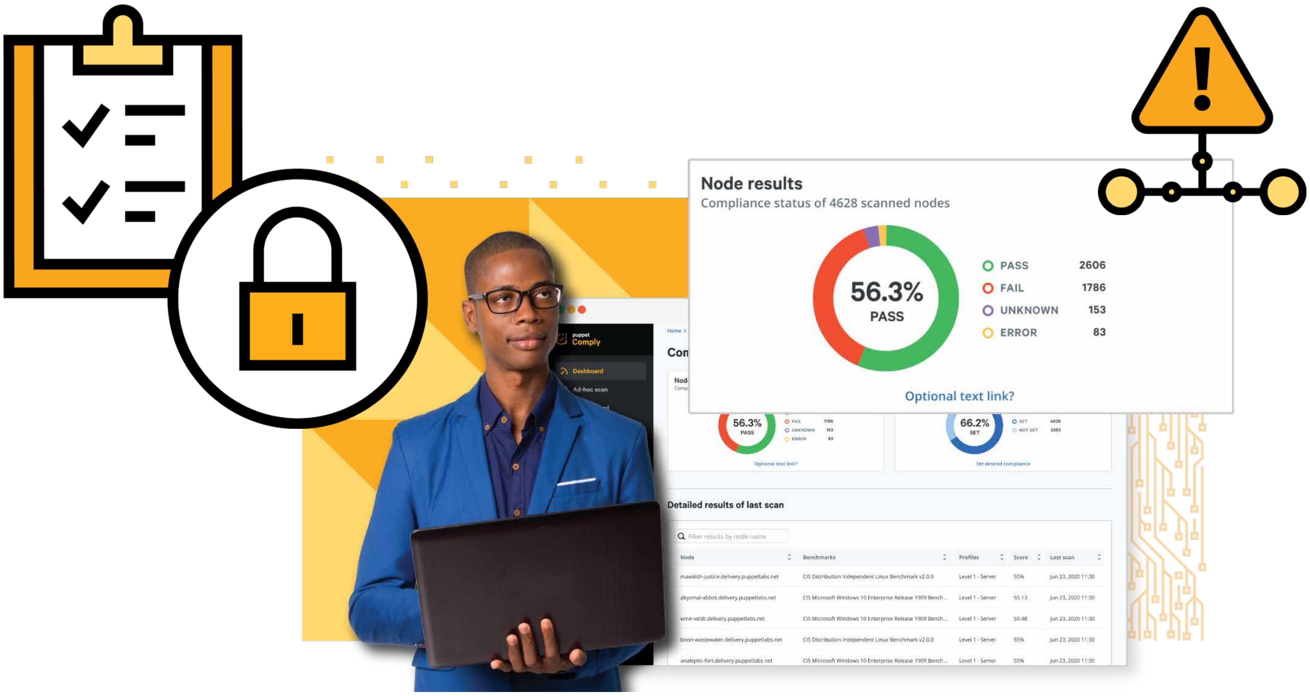
Where Puppet Fits In

There is no “one size fits all” for achieving compliance with the Essential Eight, and improving cyber resilience always requires a collection of vendor tools, specialist expertise, and a commitment to both implementing and maintaining the Essential Eight and other cyber security mitigations recommended by the ACSC. Puppet Enterprise is able to deliver a large portion of the controls and methods required to support compliance with six of the Essential Eight, and also provides a key element for a seventh mitigation (“regular backups”) as Puppet Enterprise automatically becomes the primary source of backup for configuration data once implemented.

This document provides a high-level description of how Puppet Enterprise helps to achieve compliance with each mitigation strategy, which in turn eases the burden on IT administration and operations teams in obtaining and maintaining compliance with the Essential Eight. Furthermore, proving compliance for audit purposes is simplified for IT security and IT audit teams through a centralised platform for configuration management and reporting.

Who will benefit?

- **Chief Information Officers** benefit through the knowledge that their environments are secure and have reduced the risk of a “please explain” moment due to a security breach, or at audit time.
- **Chief Information Security Officers** benefit through a significant reduction in security gaps in the environment, and a closer working relationship between IT Security and IT Operations teams as Puppet Enterprise becomes the single source of truth for configuration and patch management status.
- **IT Security teams** benefit from reduced security errors within IT infrastructure, meaning less follow-up and validation activities so that efforts can be focussed on higher value tasks.
- **IT Administrators** benefit from huge gains in efficiency of infrastructure management through automation and reduced time spent with patch management and fixing issues manually. Further, with less issues appearing in security scans for review and/or rectification means more time for higher value tasks and project delivery.



Node results

Compliance status of 4628 scanned nodes

56.3% PASS

○ PASS	2606
○ FAIL	1786
○ UNKNOWN	153
○ ERROR	83

Optional text link?

56.3% PASS

○ FAIL	1786
○ UNKNOWN	153
○ ERROR	83

Optional text link?

66.2% SET

○ SET	4628
○ NOT SET	2363

Set desired compliance

Detailed results of last scan

Filter results by node name

Node	Benchmarks	Profiles	Score	Last scan
mawkish-justice.delivery.puppetlabs.net	CIS Distribution Independent Linux Benchmark v2.0.0	Level 1 - Server	55%	Jun 23, 2020 11:30
abysmal-abbot.delivery.puppetlabs.net	CIS Microsoft Windows 10 Enterprise Release 1909 Bench...	Level 1 - Server	55.13	Jun 23, 2020 11:30
wine-veldt.delivery.puppetlabs.net	CIS Microsoft Windows 10 Enterprise Release 1909 Bench...	Level 1 - Server	59.48	Jun 23, 2020 11:30
boon-wastewater.delivery.puppetlabs.net	CIS Distribution Independent Linux Benchmark v2.0.0	Level 1 - Server	55%	Jun 23, 2020 11:30
analeptic-fort.delivery.puppetlabs.net	CIS Microsoft Windows 10 Enterprise Release 1909 Bench...	Level 1 - Server	55%	Jun 23, 2020 11:30

How can Puppet make a significant difference with 6.5 of the Essential Eight?

Here is the secret sauce: Puppet Enterprise is an infrastructure automation platform that provides infrastructure as code. When an organisation manages their infrastructure as code using Puppet Enterprise, many benefits aligned with the Essential Eight are automatically realised.

Below is ACSC's Essential Eight and how Puppet can help to achieve 6.5 of them:

Essential Eight Mitigation Strategy Description (abbreviated)	How Puppet Enterprise helps to achieve compliance with each control
1. Application control The execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets is prevented on workstations from within standard user profiles and temporary folders used by the operating system, web browsers, and email clients.	Within a Windows OS, Puppet Enterprise can manage elements of this control by restricting access to Executables and Folders via ACLs, restricting the ability to read and execute files and controlling what packages are allowed, such as installing known good and removing the rest. By only allowing users to have access to select folders, other folders will not be visible to the end user and therefore not allow the user to run anything that may have been installed. This can all be accomplished on a granular basis without the need for complex Group Policy settings.
2. Patch applications This mitigation prescribes time frames for applying patches, updates or vendor mitigations for security vulnerabilities. It also specifies the removal of software and security products that are no longer supported by vendors. Time frames and schedules for use of vulnerability scanners is also prescribed.	Patching applications is generally a time-consuming and often poorly performed operation. Applications, like Operating Systems, can be patched for configuration, executable changes or updates, and resource changes or updates. Once an application is patched, the services or the OS may need a reboot. When patching is undertaken manually, oftentimes patches are implemented but secondary phases such as service restarts are ignored, therefore leaving the application with the vulnerability. Puppet Enterprise is able to determine the difference between a regular OS patch, or application patch from a security patch, which allows security patches to be prioritised. Puppet offers patching and package management modules that drive the update process. This provides complete control of the process. If a reboot is required, it can be completed as part of the patching run.

3. Configure Microsoft Office macro settings

A variety of controls for blocking and required settings for Microsoft Office macros are described.

Puppet Enterprise offers a much simpler and repeatable way to define settings at a central location that handles a continuous compliant state. This removes the complexity of managing Group Policy and an easily auditable control is in place.

Historically, this control has been achieved via Group Policy and, while Group Policies can be effective, they can also be complex to implement. Group Policies exist on local machines as well as in the Active Directory (potentially at many levels), meaning the resultant set of policies is hard to determine.

4. User application hardening

A variety of controls around Web browsers, Microsoft Office and PDF software are described.

Puppet Enterprise can consolidate the configuration and hardening of applications into a single delivery platform. This allows administrators to deliver the required controls in an easy-to-use central location for all nodes.

Typically, control of applications on a node falls into an area that can be complex to maintain; control of application settings is accomplished using a combination of Group Policy, registry settings, configuration files, and PowerShell scripts. It is this combination approach that creates an administrative nightmare, maintaining many different approaches that have been implemented out of necessity.

5. Restrict administrative privileges

A variety of controls are stipulated for the use of privileged administrative accounts, ranging from limiting internet access for privileged accounts through to ensuring separation of privileged and unprivileged account use based on appropriate usage.

Puppet Enterprise is able to manage accounts and privileges directly on Windows, *NIX, MacOS, and other connected systems. After a node is taken under management by Puppet Enterprise, it is configured with a known set of credentials (user IDs / passwords). The credentials are sourced from Puppet Enterprise group memberships and a known set of individual permissions if necessary. The credentials for each node can be requested from a secrets vault, which creates the initial set of credentials. From there, if an administrator (human) needs to utilise the credentials, they would request them from the secrets vault.

In addition, every 30 minutes the Puppet Agent on the node reports back to the primary Puppet Server on the configuration of the node, including the administrative accounts on the node. If the configuration of the node including changes to the administrative accounts have drifted from the defined configuration, it is automatically reverted to its known good state and any unauthorised account changes are removed. These changes could include group membership, sudo rights, remote login rights, and more. Any configuration drift is captured and can be shipped to an SIEM system.

6. Patch operating systems

This mitigation prescribes time frames for the application of patches and removal of un-supported operating systems.

Time frames and schedules of use for vulnerability scanners is also prescribed.

Puppet Enterprise provides a centrally managed and controlled method for patch management. Puppet Enterprise stores FACTS about each node including OS version, packages installed, and application dependencies. Having a centralised view of all configuration data ensures that patching decisions can be made efficiently and effectively, and target the required nodes within required timeframes.

Once a patch has been approved for release, Puppet Enterprise can automatically apply the patch through all required levels (for example dev, test, prod) and can ensure that patches are only applied during approved change windows. Risk mitigations can be utilised that will automatically cancel a patch roll-out if specified failure thresholds are reached. Patches can be applied to an entire server fleet regardless of size, within minutes. If a reboot is required, it can be completed as part of the patching run.

When it comes to reporting on patch status, all nodes under management of Puppet Enterprise, whether Windows or *NIX, are visible under a single interface that allows auditors to easily identify that patching is up to date.

7. Regular backups

Backups of important data, software and configuration settings are performed and retained in a coordinated and resilient manner in accordance with business continuity requirements.

Puppet Enterprise stores a backup of the configuration settings for each node. It also holds audit information of who, when, and why a configuration change has been made. This allows nodes under management to be restored quickly in the event of a catastrophic failure. Once the nodes have been restored and configured by Puppet Enterprise, important data can then be restored to the nodes.

8. Multi-factor authentication

Puppet Enterprise supports the usage of MFA with the ability to authenticate users to the Puppet server console. This allows Puppet Enterprise to be a participant of an enterprise MFA implementation.

Using Puppet Enterprise to manage infrastructure as code enables significant gains in achieving compliance with all maturity levels of the Essential Eight for even the largest and most complex IT Infrastructures. With Puppet Enterprise as the central platform for configuration management, proving compliance for audit purposes and reporting becomes much more efficient.

More detailed technical information that maps out Puppet Enterprise's capabilities specific to each of the Essential Eight is available by contacting Puppet

Additional information about the ACSC's Essential Eight:
cyber.gov.au/acsc/view-all-content/essential-eight