TANIUM

WHITEPAPER

The Essential Eight

How the Tanium Converged Endpoint Management (XEM) Platform can help organisations implement the Australian Cyber Security Centre's Essential Eight recommendations.

Essential Eight Overview

The Essential Eight is a baseline set of mitigation strategies that the Australian Cyber Security Centre (ACSC) has recommended to make it harder for adversaries to compromise computer systems based on actual incident data. While implementation of the Essential Eight does not guarantee against a successful attack, the objective is aimed at significantly reducing the attack surface.

Before we even address the Essential Eight controls, it's worth discussing one of the greatest challenges that most organisations face – and that's visibility. You can implement a very stringent security posture against all your managed IT assets, but that posture is only as good as the weakest link. In this context, that weak link is your unknown and therefore unmanaged devices. The Tanium platform shines a light into every dark corner of your network. It will continuously expose every connected interface and quickly determine those that should be brought under management, those that are unmanageable and devices that should be immediately quarantined. Once you have a accurate, up to the minute view of your entire endpoint fleet, only then will implementing the Essential Eight make a substantive improvement to your overall security.

The Tanium Platform allows organisations to "re-platform" the endpoint, removing multiple 3rd party applications and their associated endpoint agents. With Tanium, functionality is consolidated into a single agent, maximising endpoint resources and driving down 3rd party software costs.

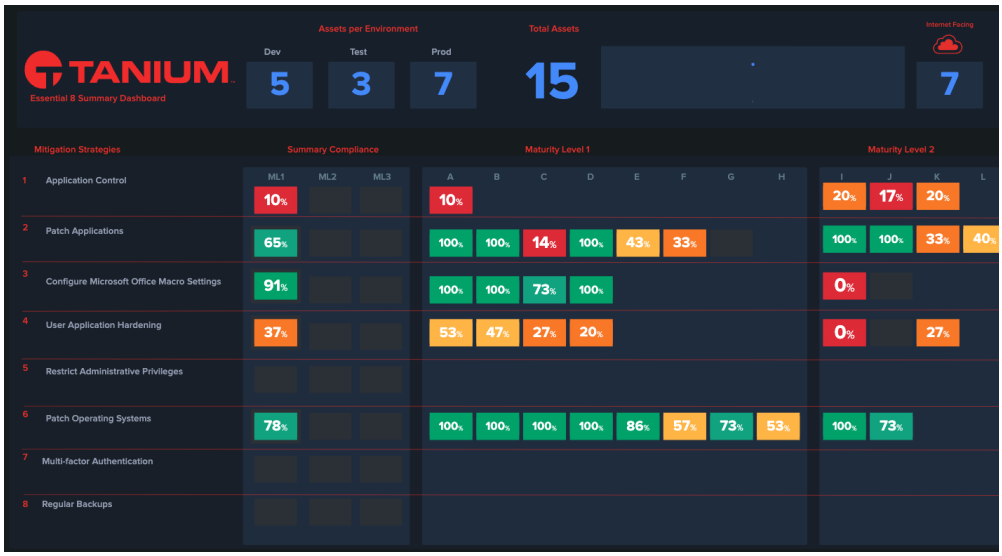
The Tanium Difference

Tanium not only gives you an immediate view of actionable data (see below for e.g.) to address exposures and pass compliance and safety checks, but can take action to enforce compliance in case you fail to pass the government mandated cyber security check. In the scenario where you've already invested in the technology required to fix the issues, but haven't configured it right, (causing you to fail the check) Tanium can help step in and either assist the outliers or take over the control entirely.

It is important to note that Essential Eight refers to 8 categories of tests, and in fact comprises 65+ individual tests in total, which, Tanium helps you address. When companies self-assess, they only perform a handful of tests, often on select machines, with paper-based Q&A. Additionally, paying a consultancy to perform this check can cost millions, and you are still left with the possibility of failing and actual audit. With Tanium, you can achieve fact based Essential 8 compliance with real-time data, and a lot more including:

- Asset discovery and reporting
- Configuration and management of Defender, AppLocker, BitLocker, and Firewalls
- Performance reporting
- Incident and threat response
- PII Data

This document details each of the Essential Eight controls exactly as described by the ACSC and then maps the capabilities of the Tanium Platform against each control. The controls below talk to the ability for Tanium to implement the control and be the tool to help you achieve Essential Eight compliance.



Application Control

Essential Eight control

To prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g., Windows Script Hosts, PowerShell and HTA) and installer.

Tanium capability

For some years, the Windows Operating System (client and server variants) has come with application and script execution control in the form of AppLocker. Organisations often choose not to use AppLocker for a variety of reasons:

1. Whitelisting applications like AppLocker require constant updates to cover the everchanging application landscape of a large enterprise
2. Administration of AppLocker via the native controls is cumbersome
3. Local admins can change policy and render AppLocker ineffective

Tanium Enforce allows administrators to set AppLocker policy (including Microsoft recommended lists) across an enterprise targeted to specific Computer Groups. The policy itself is defined via an intuitive UI and can be applied and enforced to endpoints within the corporate network or connected via the internet, whether on the VPN or not. Tanium also has some ability to audit other whitelisting tools that may be in use should AppLocker not be available.

Application Patching

Essential Eight control

Flash, web browsers, Microsoft Office, Java, and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use only the latest version of applications.

Tanium capability

Many organisations struggle to understand the state of their application assets. They have limited visibility of what's actually installed on their endpoint fleet and their CMDB is hard to keep up to date. They often rely on end users to carry out application updates, or the continuous checking of vendor websites for new updates, which results in unpatched vulnerabilities remaining in place for months or years.

Tanium Deploy provides the ability to Install, Update and Remove applications at speed and scale across the entire enterprise, with controls similar to Patching. Each endpoint constantly evaluates its application state against the published software catalogue, providing unparalleled visibility into application assets across the entire endpoint fleet. Specialised applications not within the Tanium catalogue, only need initial packaging and approval for Tanium to roll out. Tanium can also audit versions and remove software as dictated by the Essential Eight controls.

Configure Microsoft Office Macro Settings

Essential Eight control

Block macros from the internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate, as well as enable deep windows Defender functions to block threats.

Tanium capability

Setting Office Macro policy is typically achieved via Group Policy or Registry Keys. However, vendor tools lack the validation step to ensure the action is in place. Tanium Enforce works directly on the endpoint to allow policy definition targeted based on machine, groups, or users with a simple to use UI. Once in place, the configuration state can be monitored and enforces to ensure the required controls remains in place, despite user actions.

User Application Hardening

Essential Eight control

Configure web browsers to block Flash (ideally uninstall it), ads and Java on the internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers, and enable further Microsoft Defender functions.

Tanium capability

Tanium Enforce supports the most common Browser to apply specific configuration elements outside of other GPO components, as well as Defender, Firewalls, Encryption and other common configuration items. Where enforce has no predefined capability, generic control over configuration files or windows registry can achieve the same outcomes to enforce the multiple controls required by Essential Eight.

Restrict Administrative Privileges

Essential Eight control

Restrict administrative privileges to operating systems and applications based on user duties. Regularly re-validate the need for privileges. Don't use privileged accounts for reading email and web browsing.

Tanium capability

While user/admin privileges are set at a domain level, keeping track of the impact of computer groups, user-groups and nested privileges can be difficult.

Tanium Impact allows you to gain control of your administrative privileges. It provides a graphical representation of access rights and the resulting exposure if those credentials are compromised. It will detail the potential lateral movement across your enterprise and allow you to quickly remediate a security issue.

Tanium can also look into local accounts, which will not appear in central management systems. These are also subject to the Essential Eight control, and often overlooked.

Patch Operating Systems

Essential Eight control

First discover your computers and then patch/mitigate (including network devices) those with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.

Tanium capability

Patching systems in heterogeneous environments are complex. Assuming you can identify which systems need a patch, you have little feedback about whether a patch is installed successfully after it's been deployed. The borderless enterprise means that more and more company IT assets are located remotely and patching these systems can have a negative impact on VPN and WAN connectivity. This now also includes machines you may not know, making Tanium Discovery a prerequisite to finding all of your machines.

Tanium Patch solves these issues. It gives you visibility into the patching state of your entire endpoint fleet – whether or not they are on the corporate network. Monthly patching becomes a trivial exercise that can be completed in minutes or hours rather than days or weeks with current patching solutions. Any endpoints that are off the corporate network are just as visible to Tanium Patch and patch download location can be controlled when it makes more sense to download directly from Microsoft. This ensures that corporate WAN and VPN resources are protected and available for critical business functions.

Directly to the wording of the control, using Tanium Comply to discover Vulnerabilities, evaluate the nature of the exposure, and right-click to Patch make keeping on top of exploits much easier than having separate platforms.

Tanium also has the unique ability to apply vendor mitigations when a patch does not exist (typically the first 48 hours). The power of the Tanium agent to view and control files, services, network, applications, features and registries provides the proven capability to allow IT teams to act in those crucial first hours.

Multi-factor authentication

Essential Eight control

Implement multifactor authentication (MFA) for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access privilege systems or data.

Tanium capability

While the Tanium Platform doesn't provide MFA capability, it assists in monitoring and controlling end-point configuration where these tools directly interact with.

Tanium also has visibility and control over local accounts on endpoints, which can often bypass the MFA controls. Additionally Tanium itself can also interact with MFA, subject to the control itself

Daily Backups

Essential Eight control

Maintain a daily backup of important new/changed data, software, and configuration settings, stored disconnected, kept for at least three months. Test restoration initially, annually, and when IT infrastructure changes.

Tanium capability

For many organisations, daily backup of critical data has become a process that is transparent to the endpoint. Backups are taken centrally via a volume backup on a shared storage device or at the hypervisor layer. While the Tanium Platform doesn't provide backup services, there are a few uses cases where Tanium can assist.

Tanium can audit the existing roll-out of backup clients and validate they are running on the required endpoints. Tanium can also provide visibility of all files that exists to allow validation that the data is included in routing backup jobs.

In these functions above, Tanium can also "Report" on the real-time data to show if the control or policy has been applied. This means that Tanium can 'Audit' your environment to validate if your existing policy is in-place and working. Tanium has inbuilt reports and dashboards to show this data but can also export the information into other ITSM or data platforms to allow business controls to act on the outputs.

Please talk to us, to see how a full ecosystem surrounding Tanium can make Essential Eight a standard, low-overhead and real-time feature of your IT environment.

For more information on the Essential Eight, visit **https://cyber.gov.au/acsc** and speak to Tanium

Schedule a demo