# The Essential Eight

How the Tanium Platform can assist with the implementation of the Australian Cyber Security Centre's Essential Eight recommendations.

## Essential Eight Overview

The Essential Eight is a baseline set of mitigation strategies that have been recommended by the Australian Cyber Security Centre (ACSC) to make it harder for adversaries to compromise computer systems. 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 start to 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 is designed to shine 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 an 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 "replatform" 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.

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.

### 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) have 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 ever-changing 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 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.

### 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 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 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. Each endpoint constantly evaluates its application state against the published software catalogue, providing unparalleled visibility into application assets across the entire endpoint fleet. Application updates can be enforce based on policy and update packages distributed very efficiently using the power of the Tanium Linear Chain architecture.

### 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.*

**TANIUM CAPABILITY** - Setting Office Macro policy is achieved via Group Policy or Registry Keys. Tanium makes either approach very easy. Tanium Enforce offers integration into GPO to allow policy definition targeted based on machine, groups or users. In addition, Tanium can update Registry Keys at speed and scale across the entire endpoint fleet, targeted by Computer Group using an Action Package. Once in place, the configuration state can be monitored to ensure the enforced state remains in place.

### 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.*

**TANIUM CAPABILITY** - Depending on the application, hardening can be accomplished via GPO and Registry Keys. For some applications, it is also possible to update settings via an application specific configuration file. Again, Tanium Enforce offers integration into GPO to allow policy definition targeted based on machine, groups or users. Registry Keys and configuration files can be modified at speed and scale via an Action Package. The required state can be monitored and re-enforced if local changes over-write the desired state.

### Restrict Administrative Privileges

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

**TANIUM CAPABILITY** - Keeping track of administrative privileges can be challenging. In general, permissions become too permissive over time as it's easier to grant access than to remove it. In larger organisations, permissions become nested as permission groups get included in others.

Tanium Impact allows you to gain control of your administrative privileges. It provides a graphical representation of access rights and more importantly, 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.

More importantly, Tanium Impact gives you the tools required to be able to lock down administrative access rights to only those accounts where they are actually required – limiting the possibility of privileged credential exposure and the resulting lateral movement during an attack.

### Patch Operating Systems

**ESSENTIAL EIGHT CONTROL** - *Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.*

**TANIUM CAPABILITY** - Patching systems in a heterogeneous environment is complex. Assuming you can identify which systems need a patch, you have little feedback about whether a patch actually 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.

Tanium Patch solves these issues. It gives you visibility into the patching state of your entire endpoint fleet – whether they are on the corporate network or not. 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.

For major Operating System updates - for example Windows 10 1909 and 2004 - Tanium Deploy can be used to manage deployment.

### Multi-factor authentication

**ESSENTIAL EIGHT CONTROL** - *Implement multi-factor authentication (MFA) for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive/high-availability) data repository.*

**TANIUM CAPABILITY** - While the Tanium Platform doesn't provide MFA capability, it will fully support integration with the most common MFA providers. Indeed, it is strongly recommended that MFA is in place for the Tanium platform and is mandatory for TaaS (Tanium as a Service).

However, Tanium can be used to audit your endpoint fleet to ensure that MFA is correctly enabled and provide visibility into configuration gaps. This information is very useful to ensure comprehensive MFA coverage and eliminate any weak spots in your security posture. When issues are found, Tanium can also be used to push required MFA software to an endpoint as well as modify any configurations across your entire endpoint fleet.

### Daily Backups

**ESSENTIAL EIGHT CONTROL** - *Maintain a daily backup of important new/changed data, software and configuration settings, stored disconnected, retained 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.

If an adversary has made changes to critical files and built in persistence via modified registry keys, these changes are typically included as part of the regular backup. This means that following the discovery of an attack, it can be very difficult to find a restore point that isn't going to keep the door open for the attacker. Of course, the further back you go, the further you move from your Recovery Point Objective.

Understanding when unauthorised changes are being made to critical system files is essential to ensuring that the data you are backing up is indeed in a restorable condition. Tanium Integrity Monitor enables you to monitor those critical files and alert on any changes that occur, giving you confidence in the integrity of your backup.

There are times when a machine-initiated backup is required. Given the prevalence of centralised backup technology, this can expose some management challenges. The Tanium Platform can be used in both an auditing and scheduling capacity. It can monitor critical systems to ensure that backups have been completed correctly. Tanium can also be used to copy and export critical files to an external system.

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

## About Us

Tanium is a unified endpoint management and security platform proven in the world's most technically demanding organizations. Providing unparalleled speed, visibility, and scale, we serve half of the Fortune 100, top retailers and financial institutions, and four branches of the US Armed Forces, which rely on Tanium to make confident decisions, operate efficiently, and reduce risk. Tanium recently ranked 7th on the Forbes list of "Top 100 Private Companies In Cloud Computing For 2019," 10th on FORTUNE's list of the "100 Best Medium Workplaces" in the U.S., and 18th on the UK's Best Workplaces list. Visit us at www.tanium.com or follow us on LinkedIn and Twitter.

TANIUM