TANIUM

PERSPECTIVE

Decoding Essential 8 Compliance: Tanium's Unique Path To Success

CONTENTS

Introduction

From Tanium's Australian bureau, we dive into the Essential 8 baseline mitigation strategies and reveal how Tanium's unique architecture goes beyond the traditional approach of other vendors and enables organisations to overcome key challenges to help them successfully achieve automated continuous compliance

Globalisation is nothing new. It's become the norm for corporations to have significant transnational business dealings. That could take the form of providing goods or services to customers abroad or relying on global supply chains for key inputs such as labour or manufactured parts.

This poses a serious concern for IT risk and compliance professionals. Government regulations on things like data privacy and cybersecurity vary from one jurisdiction to another, and it's up to these compliance experts to ensure that their organisation operates within the legal frameworks for every jurisdiction in which they operate.

Fortunately, Tanium's Converged Endpoint Management (XEM) platform is designed to ease the burden of compliance across a wide array of regimes and use cases.

In this post, we'll address one such cybersecurity compliance framework, Australia's Essential Eight, and show how Tanium's "Compliance by Design" solution helps organisations achieve their compliance objectives as an outcome of managing the network effectively rather than treating it as a separate exercise.

What is The Essential Eight?

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 that all attacks will fail, the objective is aimed at significantly reducing the attack surface.

As its name suggests, the ACSC Essential Eight is composed of eight pillars:

- **Application control:** To prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g., Windows Script Hosts, PowerShell, HTA, and installer)
- **Application patching:** 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.
- **Configure Microsoft Office macro settings:** 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.
- **User application hardening:** 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.
- **Restrict administrative privileges:** 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.
- **Patch operating systems:** Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.
- **Multifactor authentication[1]:** Implement multifactor authentication (MFA) for VPNs, RDP, SSH, and other remote access and for all users when they perform a privileged action or access privileged systems or data.
- **Daily backups:** Maintain a daily backup of important new/changed data, software, and configuration settings, stored disconnected, and kept for at least three months. Test restoration initially, annually, and when IT infrastructure changes.

Leveraging Tanium to manage and secure IT environments provides significant advantages when addressing the challenge of Essential Eight compliance. We'll explore those advantages by comparing Tanium's modern, "Compliance by Design" solution to traditional approaches. We'll point out the shortcomings of these legacy compliance methods and demonstrate how organisations operating fully or only partially in Australia can achieve their compliance objectives as an outcome of managing the network effectively rather than treating compliance as a separate exercise.

Please note that this document forms part of a documentation set which also includes specific details on how Tanium applies Essential Controls and other more generalised rationale behind the Tanium approach to Essential Eight.

References:

1. https://www.tanium.com/blog/what-is-multifactor-authentication-mfa/

How does Tanium help maintain ACSC Essential Eight compliance?

Given the difficulties organisations have encountered building an approach to Essential Eight compliance since its inception, one could be forgiven for thinking that there is a lack of available detail on what it is that should be measured, and that this detail has been left to external commercial entities to conjure and regard as their intellectual property.

The reality is however that the ACSC have produced detailed documentation and guidance on each of the 8 mitigation strategies and their associated controls right through the maturity levels. This not only includes information about the intent ofs each control to help with interpretation but also tools and specific details on what it is that should be measured. So, if what we need to measure against is well-known and understood, then what is the problem?

There are four key areas to consider that have traditionally impeded organisations from understanding a true representation of their compliance level (let alone improving it).

- **Coverage:** Can you account for all of your assets and have them under management?
- **Currency:** How old is the data in your latest report?
- **Completeness:** Does testing occur on *all* your endpoints or just a subset?
- **Corrective Action:** How do remediation activities fit into your regime?

Tanium is underpinned by a unique and innovative architecture that provides real-time access to endpoints. This architecture allows Tanium to function in a way that inherently addresses the four challenges above. The goal of this document is to work through each of these areas, describe the challenge in more detail, and show how Tanium's unique design ensures these challenges do not obstruct compliance objectives.

Coverage

Asset coverage is a fundamental part of endpoint management. The adage "what gets measured gets managed" is undeniable. To this point, most reasonable folk would agree that applying advanced security products and practices to only a percentage of assets is an obviously flawed approach. Yet organisations regularly do (often unknowingly).

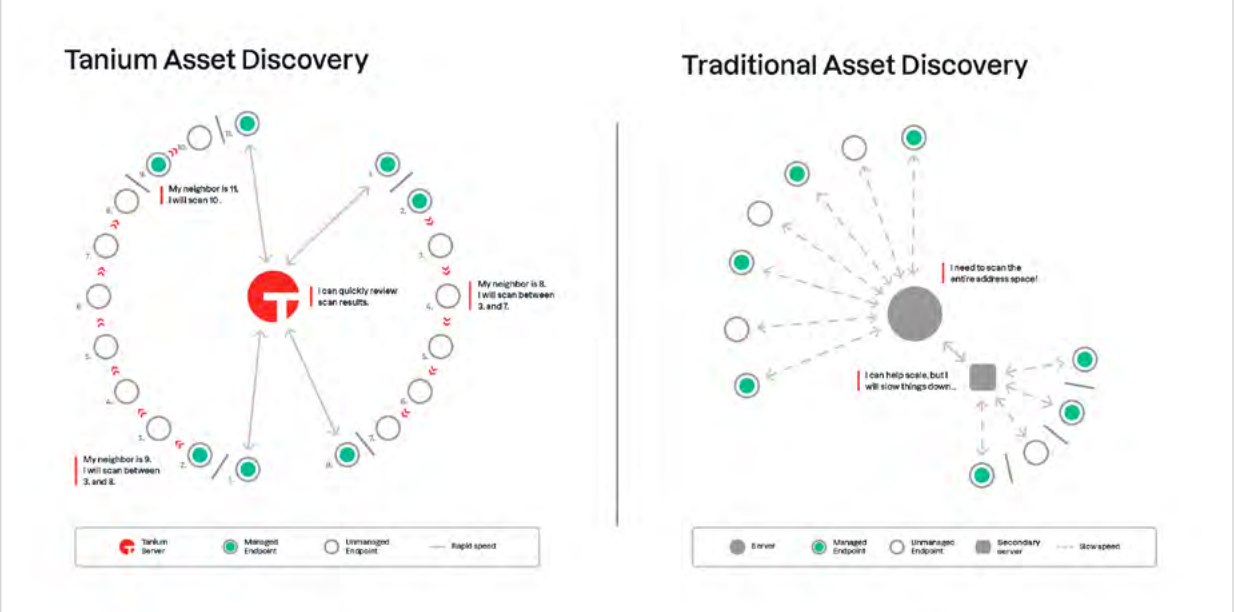
This poses several questions:

- Are you truly aware of every asset that joins the network?
- Do you have a current and complete CMDB?
- Do all management and security tools leverage the CMDB as a source of record?
- How do you ensure endpoint tools remain in a healthy state?

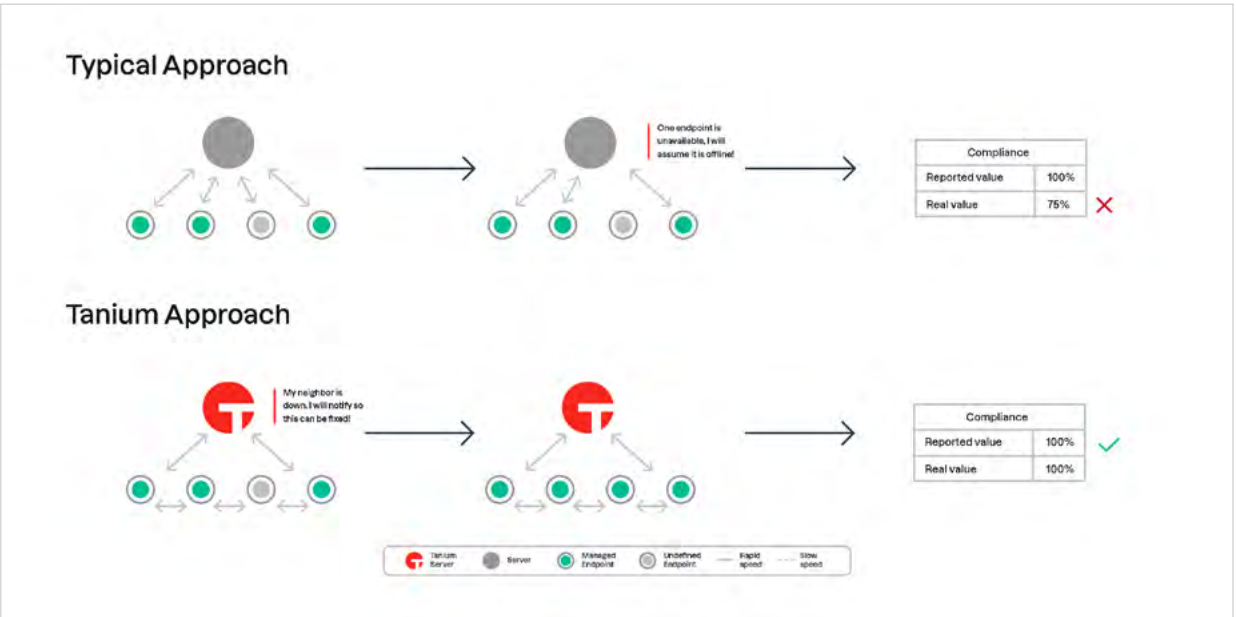
A recent amendment to the Essential Eight added an explicit asset discovery control into both the Application Patching and Operating Patching mitigation strategies. For prior versions, this was an assumed or implicit prerequisite.

Fortunately, Tanium includes an asset discovery function. This capability leverages the Tanium architecture by performing distributed scanning. That is, endpoints discover their neighbouring assets themselves, rather than via a centralised scanning point. This allows knowledge of what is on the network to be gained much faster as the load is spread and allows scanning to reach into areas of the network that a centralised point may not be able to. The primary goals of Tanium's asset discovery are to:

1. Identify manageable assets that are not currently under management and have them brought under management.



2. Identify assets that were under management, and for some reason, they are currently not, and have them investigated and remediated.



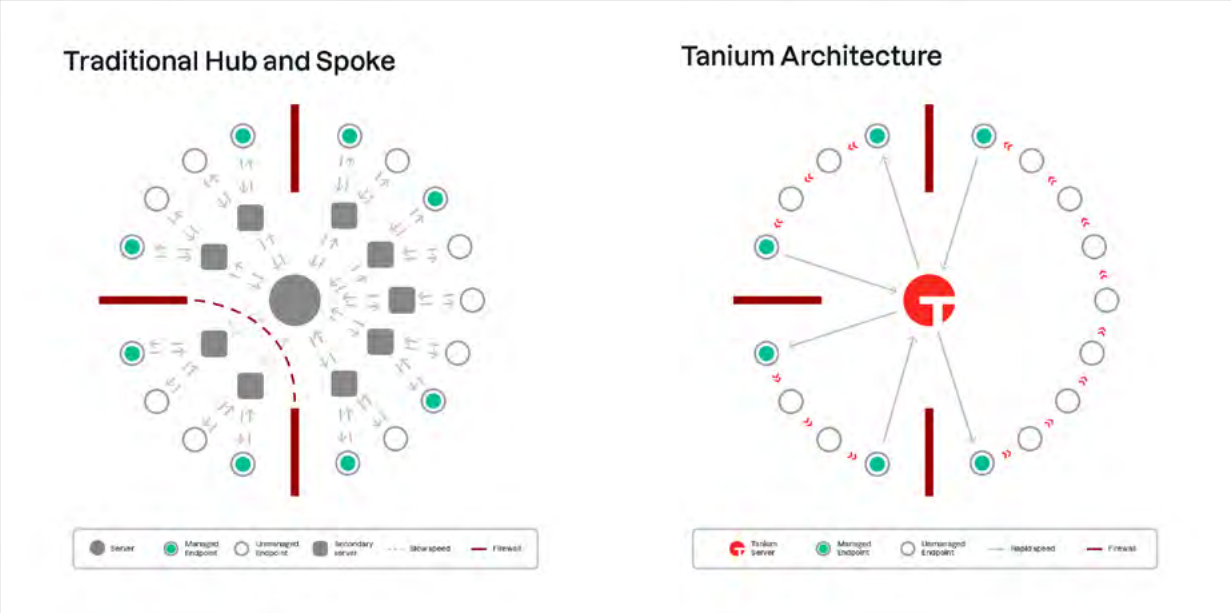
Tanium ensures that all endpoints for an organisation within the Essential Eight scope are being managed and that there are no gaps skewing compliance percentage levels up or down. Ultimately the intent of the Essential Eight is to provide a starting point for organisations to understand and improve their security posture – if you do not get the coverage aspect right then the whole effort is failing that intent.

Currency

The data currency challenge is applicable right across the endpoint management realm. Traditional tools and architectures have struggled to scale with ever-increasing network sizes while ensuring visibility and control of that network is available at a speed to satisfy today's security and operational needs.v

Traditional tools utilise the classic hub and spoke style architecture. That is, point-to-point connections from the management server to every endpoint. The only way for this architecture to scale is to add middle tiers of infrastructure to spread the load from a single centralised point, however, this slows down data retrieval and introduces more break points.

Tanium leverages a patented linear chain architecture. Endpoints connect to and transmit data between neighbours allowing communications from a single management server to be minimised. The result is a highly efficient, immensely scalable communications platform that can access endpoints to both retrieve data and perform actions at speeds measured in seconds.



How do these architectures have an impact on Essential Eight compliance?

First, traditional approaches to measuring Essential Eight compliance are often performed via an audit-style approach. This involves the services of either internal or external resources to connect to endpoints that they have access to, run scripts to assess compliance, return the results and then correlate/curate for reporting. This can be a timely and costly exercise, so it is generally not performed regularly. The resulting compliance report reflects a **point in time** and is relied on until another audit can be performed.

In contrast, when Tanium is managing an environment, it is already collecting a wide variety of data in real time – the specific data points required for Essential Eight reporting are simply another use case. When viewing reporting data of this nature it reflects the **current state** of the environment. This is important not only for the validity of the results at any given time but when introducing the notion of taking action to remediate and improve security posture as discussed in the 'Corrective Action' section of this document. As each remediation effort is undertaken, an old point-in-time report becomes less reflective of the environment and consequently less useful.

Completeness

There are several ways in which organisations are challenged to gain completeness of data for Essential Eight compliance monitoring.

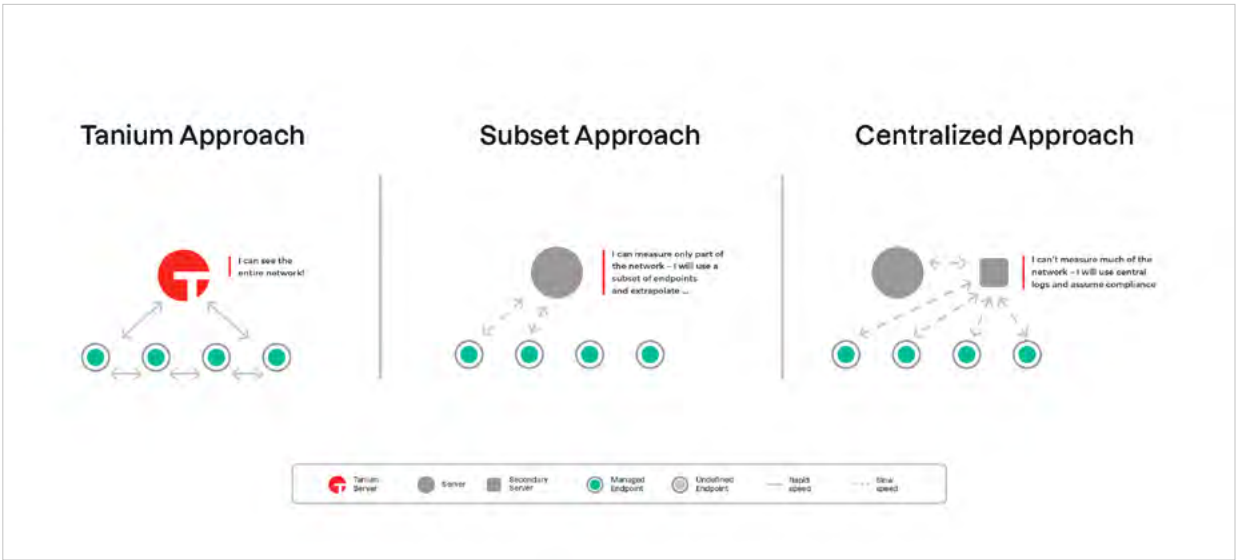
- **Resource/cost constraints:** Audit style approaches to collect data consume limited resources.
- **Technical constraints:** Traditional data retrieval methods have limitations on their scale, speed, access to the entirety of endpoints (e.g. remote and non-domain joined endpoints) and ultimately breadth and depth of visibility at the endpoint.

To work around these constraints the following approaches are typically employed:

- Measure a small subset of endpoints for compliance and then extrapolate across the network.
- Consult centralised configuration and logs and derive/assume that this is reflective of the actual state of endpoints.

Tanium is designed natively to manage very large and complex network environments in their entirety. Numerous architectural features ensure this is achieved and those features naturally flow into the Essential Eight compliance monitoring use case. Advantages include:

- Tanium manages endpoints running multiple disparate operating systems such as Windows, macOS, and Linux in a consistent, normalised manner.
- Tanium is not domain-bound. Endpoints simply need network connectivity to the Tanium server. This allows endpoints to be managed as part of a global fleet across the internet, VPN, or when located in secured enclaves of the network.
- Tanium scales massively while maintaining near real-time management capabilities.
- The breadth and depth of visibility at the endpoint is extensive. Any data retrieval or task that can be accomplished from a command line (via native utility or script) at the endpoint can be achieved estate-wide with Tanium.



Once complete estate-wide Essential Eight compliance monitoring has been established using Tanium, it may be beneficial to construct sub-views of this data. Tanium provides mechanisms to categorise endpoint data in various ways, so that views may be presented on a geographical, business unit, sub-network basis or any other logical distinction that makes sense.

Corrective Action

The ability to improve security posture via some form of corrective action or remediation activity is ultimately the end goal of Essential Eight compliance.

However, as outlined in the sections above, typical audit style Essential Eight reporting delivers a set of derived percentage compliance numbers, but you are then left to work out how to resolve areas of non-compliance. Without detailed and attributable endpoint data being made available this becomes a very difficult task indeed.

Tanium's Essential Eight monitoring surfaces gaps in compliance showing not only summarised percentages but the relevant underlying endpoints, the specific controls that have failed, and the data that constituted this result against each maturity level. From there, either Tanium may be used to remediate, or an existing tool can be utilised as desired. Given reporting's current state, new results will be reflected soon after in the reports.

Tanium inherently provides the ability to improve security posture and consequently Essential Eight compliance. Standard hygiene reporting and enforcement activities using Tanium can be leveraged to positively impact compliance across most controls. The reporting of those activities simply becomes an outcome of that management rather than a separate or disparate exercise. This closed feedback loop of compliance is what we refer to as "Compliance by Design".

Learn more about the ACSC Essential Eight and how Tanium can help your organisation[2] maintain compliance.

References:

2. https://site.tanium.com/Essential-8.html