A comprehensive guide to the Essential Eight Maturity Model

ManageEngine

Table of contents

The need to prioritise protection strategies

Cybercrime has been constantly evolving and is a complex issue that affects numerous sectors across the country. Though most organizations have implemented strategic policies and programs to combat security challenges, they are still struggling to keep up with threats posed by rapid advances in technology.

To make matters worse, some companies are in the dark about their levels of threat exposure. The BDO and AusCERT Cyber Security Survey 2018/2019 found that that most cyberattacks aren't caused by mere accidents or employee error, but are instead the result of targeted criminal attacks.[1]

If organisations can properly understand who is targeting them and why, it makes it easier to invest in the correct policies and solutions.

Many recent cyberattacks targeting the Australian Parliament, major universities, and corporate entities illustrate that the threat continues to be significant. A recent survey found that small businesses account for 43 percent of all cybercrime targets in Australia.[2] To combat these rising threats, the Australian government has doubled down on its efforts to secure businesses and individuals across the country, and has increased focus on its nationwide cybersecurity policies.

In a discussion paper on Australia's 2020 cybersecurity strategy, Minister for Home Affairs Peter Dutton said,

"We need to adapt our approach to improve the security of business and the community. Cyber criminals are more abundant and better resourced, state actors have become more sophisticated and emboldened, and more of our economy is connecting online. Cyber security incidents have been estimated to cost Australian businesses up to $29 billion per year and cybercrime affected almost one in three Australian adults in 2018."

Australian organizations need a clear set of policies and steps they can implement to protect their business from the most common and dangerous attack vectors. The Australian Signals Directorate's Strategies to Mitigate Cyber Security Incidents, commonly known as the Essential Eight, aims to provide a prioritised list of mitigation strategies to help organisations protect themselves from a range of cyberthreats.

This guide will detail the main requirements of the Essential Eight Maturity Model, what it means for organisations, and how organisations can ensure that they are fully protected at all times.

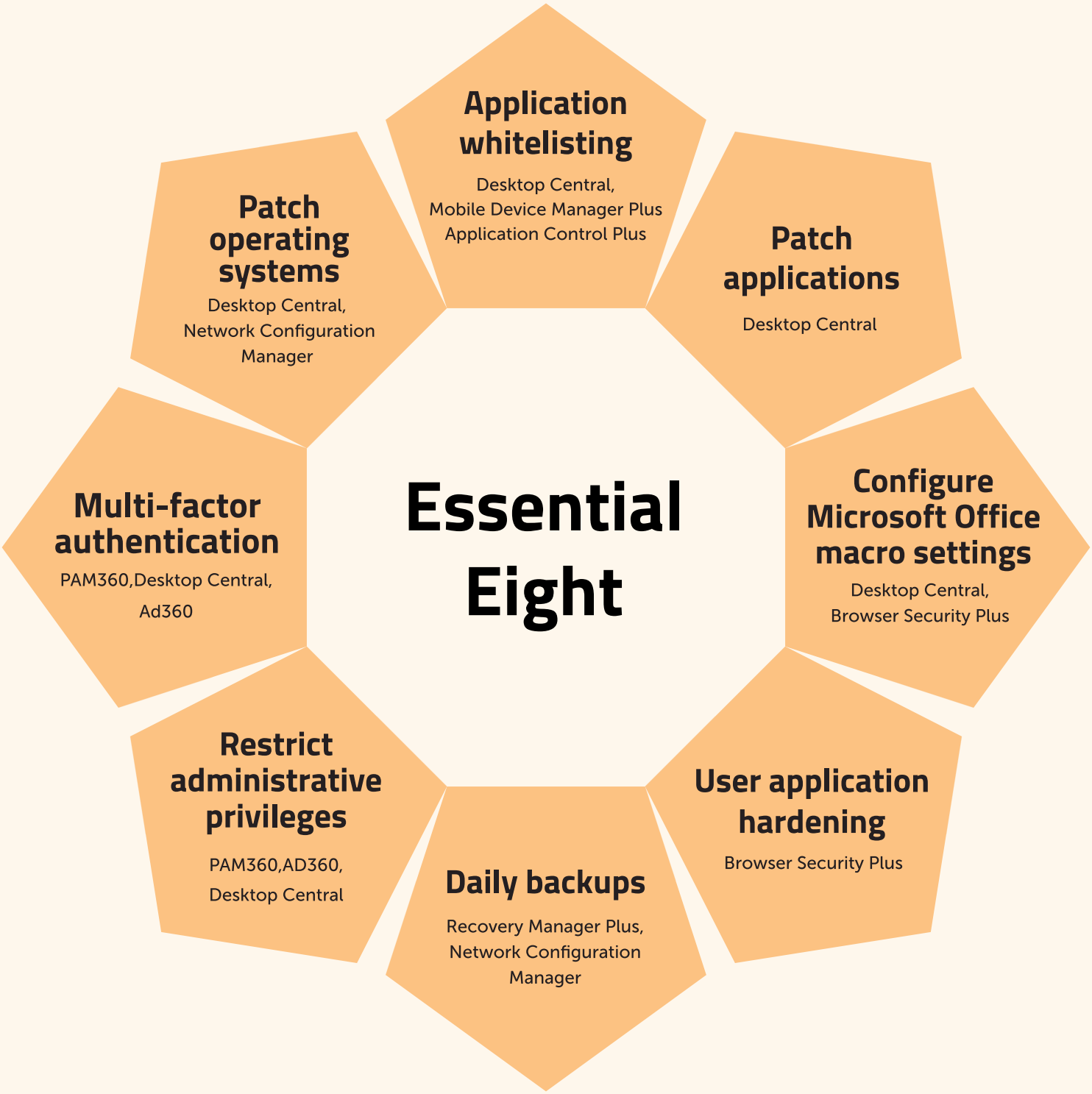
The Essential Eight explained

In 2017, The Australian Signals Directorate revised its long-standing list of protection strategies for organisations to mitigate cybersecurity threats. This list of eight strategies is known as the **Essential Eight.**

While no single strategy is guaranteed to prevent cyberattacks, it is recommended that organisations implement these eight essential mitigation strategies as a baseline. These strategies aim to make it harder for attackers to compromise systems and networks. Moreover, proactively implementing the Essential Eight can be more cost-effective than responding to a large-scale cybersecurity incident.

However, as every environment is different and the same set of actions won't apply in every situation or for every company, these mitigation strategies can be customised based on each organisation's risk exposure and the security challenges they are most concerned about.

It is important to keep in mind that applying security policies is an ongoing process. A network constantly evolves as devices are added and/or removed. New threats always appear, and new measures become necessary. Organizations need to pursue an optimal state of constant vigilance and readiness.



The Australian Signals Directorate has defined three maturity levels for the application of the strategies. Once organisations have implemented Level One mitigation strategies, they should strive to reach Maturity Level Three to ensure maximum protection for their organisational data.

The maturity levels are defined as:

1 **Maturity Level One:**
Partly aligned with the intent of the mitigation strategy

2 **Maturity Level Two:**
Mostly aligned with the intent of the mitigation strategy

3 **Maturity Level Three:**
Fully aligned with the intent of the mitigation strategy.

What does the Essential Eight mean for my organisation?

The Essential Eight strategies have three main purposes:

- **Preventing malware attacks**
- **Limiting the extent of events**
- **Recovering data and system availability**

Organizations need to implement the following strategies to protect their business-critical information from cyberattacks and data breaches.

Mitigation strategies to prevent *malware delivery* and *execution*

1. Application whitelisting

An application whitelist only allows preapproved software to run in your network.

Why?

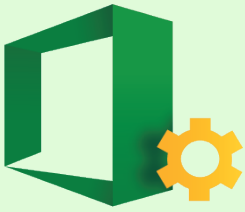
All unsanctioned, and therefore potentially harmful, software is prevented from executing.

2. Patching applications

Regular patching fixes security vulnerabilities in software applications.

Why?

Attackers can take advantage of known security vulnerabilities to target organizations.



3. Configuring Microsoft Office macro settings

Macros from the internet are blocked, and only vetted macros with limited write access or macros that are digitally signed with a trusted certificate are allowed.

Why?

Macros can be used to enable the download of malware. Cybercriminals can then access sensitive information.

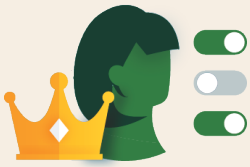
4. User application hardening

Application hardening involves disabling unsecure and unused services, such as Flash, Java, and web ads from applications, and restricting the use of applications that are known to be vulnerable.

Why?

Flash, Java, and web ads are notorious for being malware gateways to systems.

Mitigation strategies to limit the extent of *cybersecurity incidents*



5. Restricting administrative privileges

Restrict administrative privileges to operating systems and applications based on user duties. These should be restricted to only those that need them. Regularly revalidate the need for privileges.

Why?

Admin accounts are the ***"keys to the kingdom"***; attackers can use these accounts for access to critical information and systems.

6. Patching operating systems

Regular patching fixes security vulnerabilities in operating systems.

Why?

Attackers can use known security vulnerabilities to target computers.

7. Enabling multi-factor authentication (MFA)

A user is granted access only after successfully presenting multiple, separate evidences of authenticity.

Why?

Having multiple levels of authentication makes it a lot harder for attackers to access an organization's sensitive information.

Mitigation strategies to *recover data* and *system availability*

8. Performing daily data backups

Regularly back up all data and store it securely offline or at an alternate site such as a secondary data centre or in the cloud.

Why?

Daily backups ensure that your organisational data remains safe in the event of a cybersecurity incident.

The Essential Eight action plan

Organisations need to implement these eight strategies at least at a baseline level to ensure basic levels of protection. Once organisations have reached Maturity Level One for all the eight strategies, they should strive to reach a higher maturity level depending upon their business' risk exposure.

The following tools and solutions can help organisations implement the protection strategies with ease.

1. Application whitelisting

Begin by identifying the different applications used by the various departments and/or processes. These will automatically go into your whitelist. Keep in mind that not every team or department in your organisation will use the same applications. On the other end of that, there will be a core list of applications that everyone uses across departments, such as Office applications. Knowing which applications exist in your environment, whether they're necessary or unnecessary, is crucial.

Steps:

» Block applications; identify and auto-uninstall prohibited software.

» Lock a device to a single application or group of applications

» Enable application whitelisting and blacklisting.

» Block executables and script execution.

» Deploy block rules on workstations and servers.

» Allow or block apps on mobile devices running Android, iOS, or Windows.

Tools:

ManageEngine
Application Control Plus

ManageEngine
Mobile Device Manager Plus

ManageEngine
Desktop Central

2. Patching applications

Begin by making an inventory of all the applications in use. It is crucial to know what is being used in your organisation and why. Once you have an inventory of all the applications being used, you can check whether these applications have the latest releases and patches installed.

Steps:

» Patch Microsoft, non-Microsoft, macOS, and Linux applications.

» Update drivers and BIOS versions.

» Detect, approve, download, test, install, and validate patches and service packs.

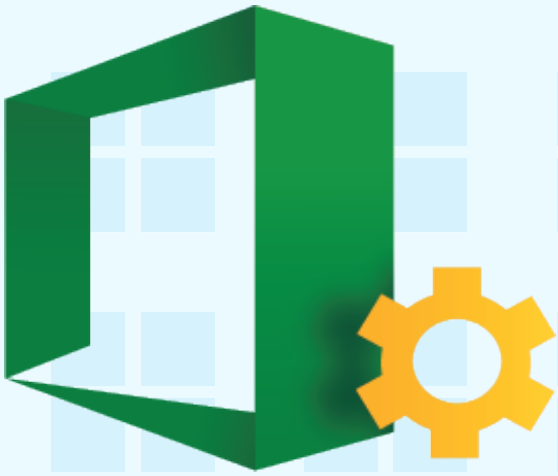
» Schedule patch scans and deployment.

» Achieve patch compliance using advanced analytics and audits.

» Manage workstations and servers on a LAN or WAN.

Tools:

ManageEngine
Desktop Central



3. Configuring Microsoft Office Macro settings

Begin by assessing what (if any) macros your organisation uses and what purpose they serve. Only trust macros selectively, and do not leave the choice up to end users. Trust only macros that are digitally signed, and then configure applications to disable all but signed macros.

Steps:

» Manage Microsoft Office settings out of the box.

» Manage Microsoft Office macro settings through execution of custom scripts.

» Control browser plug-ins, extensions, and allowed sites for Internet Explorer, Edge, Firefox, and Chrome.

Tools:

ManageEngine
Desktop Central

ManageEngine
Browser Security Plus

4. User application hardening

Begin by making a full inventory of your applications. In case, you already did that for the application whitelisting exercise, congratulations, you've got a head start! Once you have a full list of your organisation's applications, begin by changing any default usernames and passwords. It might seem like a trivial step, but it's one of the most important ones. If an application uses a service such Flash, Java, or web advertisements that are not essential, disable or uninstall these components.

Steps:

- » Control browser plug-ins, extensions, and allowed sites.
- » Leverage browser lockdown and isolation, download restrictions, and data leak prevention tools.
- » Provide or restrict access to web applications.

Tools:

ManageEngine
Browser Security Plus

5. Restricting administrative privileges

Begin by making a thorough a list of all of the administrator accounts in your organization. Include all local, domain, and enterprise admin groups as well as all accounts with elevated privileges. Once you have a list of all administrative privileges, check for the validity of these privileges and how many of these are still required.

Steps:

» Manage privileged access to systems, applications, and network devices.

» Exert granular control over users' access to resources and passwords.

» Delegate role-based access to AD, Exchange, and Office 365

» Gain visibility into and manage privileged permissions.

» Enable just-in-time privilege escalation.

» Set role-based access to computers and mobile devices running Android, iOS, or Windows.

Tools:

ManageEngine
AD360

ManageEngine
Desktop Central

ManageEngine
PAM360

6. Patching operating systems

Begin by making patch management an integral part of your security maintenance program. Implement central control over your patch management schedule and distribution so you don't have users downloading the same patch multiple times. Make sure that your organisation's patching policy clearly details what to patch, when, and how often.

Steps:

» Test and deploy OS patches for Windows, macOS, and Linux based on severity.
» Validate the status of patch deployment.
» Schedule patch scans, and identify the health status of devices.
» Identify and manage firmware vulnerabilities.
» Perform remote firmware upgrades and OS image transfers.

Tools:

ManageEngine
Desktop Central

ManageEngine
Network Configuration Manager

7. Enabling MFA

Begin by taking stock of your present situation and carefully consider everything you need to safeguard, as some systems are more critical than others. Review all the processes and systems to understand where your organisation needs to implement MFA.

Steps:

» Use one or more authentication techniques to verify users' identities during the password reset and account unlock process.

» Use a secure password vault for privileged and personal accounts.

» Enable authentication through AD/LDAP, PhoneFactor, email, RSA SecurelD, etc.

» Remotely log in to a wide range of systems and network devices on a LAN or WAN, and record privileged sessions.

Tools:

ManageEngine
AD360

ManageEngine
Desktop Central

ManageEngine
PAM360

8. Performing daily backups

Begin by determining what you need to back up, the priority of backed-up content, and how you will perform these backups. Depending upon your organisation's requirements, determine whether you will need to do full backups every day or a full backup once a week with incremental daily backups. Furthermore, you will also need to implement a regular restoration testing and disaster recovery plan.

Steps:

» Perform comprehensive, scheduled incremental object and item-level backups in AD, SharePoint online, on-premises Exchange, and Exchange Online.

» Back up the entire database of application configurations, system settings, and password share permissions through scheduled tasks or live data backup.

» Perform restart-free granular restoration.

» Automate configuration backups from over 200 multi-vendor firewalls, routers, switches, etc.

Tools:

ManageEngine
Network Configuration Manager

ManageEngine
RecoveryManager Plus

Endnotes

1. https://www.bdo.com.au/en-au/cyber-security/2018-2019-cyber-security-survey-results

2. https://itbrief.com.au/story/cyber-attacks-worsening-among-australian-businesses-costing-economy-1-billion-a-year

About ManageEngine

As the IT management division of Zoho Corporation, ManageEngine prioritizes flexible solutions that work for all businesses, regardless of size or budget.

ManageEngine crafts comprehensive IT management software with a focus on making your job easier. Our more than 90 products and free tools cover everything your IT needs at prices you can afford.

From network and device management to security and service desk software, we're bringing IT together for an integrated, overarching approach to optimizing your IT.

ManageEngine

www.manageengine.com