



eset[®] Digital Security
Progress. Protected.

**PROTECTING YOU ON
YOUR DIGITAL JOURNEYS**

**Your Simple Path
to Essential Eight
Alignment**

Introduction

In today's business landscape, cybersecurity has quickly gone from being an afterthought to a critical consideration. To help Australian businesses identify and prioritise areas of protection, the Australian Government introduced the Essential Eight, a curated suite of eight cybersecurity risk mitigation strategies. Drawn from a larger set of 37, these strategies are deemed the most vital for businesses of all sizes.

However, if your business hopes to align with the Essential Eight, it will face a new challenge: selecting and implementing the right tools to execute each strategy. The proliferation of options, together with the continuous influx of new solutions, can make it difficult to identify reliable, cost-effective solutions that maximise your protection without blowing your budget.

ESET decisively fills this void, delivering robust, flexible solutions fully aligned with the Essential Eight framework. Regardless of where you are in your cybersecurity journey—just starting out and seeking a solution that supports as many of the strategies as possible, or already most of the way there and needing a tailored solution for the remainder—ESET offers the perfect protection for you.

This whitepaper offers an in-depth exploration of the ACSC's Essential Eight strategies and shows how ESET can help you efficiently achieve each one.

What Are the Essential Eight?

The Essential Eight was introduced by the Australian Cyber Security Centre (ACSC) in 2017. Starting with a holistic list of 37 strategies that can mitigate cybersecurity incidents, the ACSC categorised each based on its relevance to Australian businesses, ranging from 'Essential' to 'Limited'. The strategies classed as 'Essential' became the Essential Eight.

Each strategy includes a variety of prescriptive controls for technical implementation, along with stipulated timeframes for specific processes and initiation activities.

The Essential Eight cybersecurity strategies come in four Maturity Levels (numbered zero to three). Each level represents progressively robust cybersecurity defences, meeting increasing minimum criteria, and provides protection against adversaries of rising sophistication and determination.

Maturity level one is designed to safeguard your organisation from adversaries with limited skills, utilising readily accessible cyber offensive tools and committing minimal time to each attack attempt. At the opposite end of the scale, maturity level three aims to protect you from adversaries who tailor their attacks to exploit their specific targets, investing significant time and resources in their offensive efforts.

As your organisation advances through the maturity levels, the number of controls required for each mitigation strategy increases, and the criteria to meet controls fulfilled at earlier maturity stages become increasingly strict.

The ACSC encourages every business to select a target maturity level based on its unique risks and the likelihood that different types of adversaries will target it.

Achieving Maturity Levels of the Essential Eight

As noted earlier, the ACSC provides highly specific criteria and controls within each mitigation strategy at every maturity level to reach the intended outcome.

One advantage of this approach is that even organisations with limited cybersecurity expertise can implement each control as prescribed and establish robust cyber defences. On the other hand, this specificity can result in increased cost and effort if you find yourself needing to configure a multitude of different applications and procure multiple solutions. It's also possible that your organisation has already put other cybersecurity measures in place to achieve the same outcome, making the prescriptive criteria superfluous.

Acknowledging this, the ACSC allows for the use of compensatory controls. A compensatory control can be used where an organisation either cannot or choose not to meet the specific criteria set out in the Essential Eight and instead has a compensatory strategy in place that fulfils the same outcomes.

Example: Normally, to achieve maturity level three of the Essential Eight, you need to block all Office Macros. However, if your business relies on macros for operational functions, this might not be practical. Instead, you may opt to allow macros in certain circumstances and implement a toolset that scans, identifies, and blocks malicious behaviour. This would be considered a compensatory control.

This would allow you to utilise macros, while still complying with the Essential Eight strategy and maintaining a strong cybersecurity posture.



Why Use the Essential Eight?

As a framework developed by the Australian Government, the Essential Eight is quickly becoming the de-facto cybersecurity framework in Australia. Its endorsement by the ACSC gives it credibility within Australia, and in many cases, the Essential Eight has become a requirement of certain supply chains.

While not as comprehensive as other cybersecurity frameworks, the Essential Eight offers an easy and cost-effective pathway for organisations of all sizes to begin and progress their cybersecurity journey, without the need for expert cybersecurity resources.

Why Choose ESET?

ESET's solutions offer coverage across many of the Essential Eight mitigation strategies. By covering many aspects of your organisation's environment and associated Essential Eight strategies ESET's solutions can reduce both cost and complexity while also increasing the ease and speed of implementation of the Essential Eight.

ESET's solutions not only meet but frequently surpass the requirements of the Essential Eight. Where the Essential Eight requires secure configuration of specific applications or implementations of specific cybersecurity tools, ESET's solution can either support these activities or avoid the need for them entirely all while maintaining Essential Eight alignment.

	ESET Protect All Packages	ESET Protect Complete	ESET Protect Enterprise	ESET Protect Elite
Configure Microsoft Office macro settings	✓	✓	✓	✓
User Application Hardening	✓	✓	✓	✓
Patch Operating Systems	✓	✓	✓	✓
Patch Applications		✓	✓	✓
Application Control			✓	✓
Multi-factor authentication				✓
Restrict administrative privileges	Support available through our partner network			
Regular backups	Support available through our partner network			

The Eight Essential Mitigation Strategies

Configure Microsoft Office macro settings

Strategy Overview

Office macros are miniature programs that execute automatically in Word, Excel, or PowerPoint documents upon opening. For many years, macros have been a common malware target. This strategy permits Office macros only when absolutely required, as well as restricting users from changing their own Office macro settings.



The ESET Difference

The Essential Eight requires strict control over when and how Microsoft Office macros can be used and configured.

While this is a great idea, it may not be possible if your business relies on macros for its operations. Meanwhile, many organisations may require a higher level of protection against malware that enters via macros, given it is such a common threat vector.

If you're unable to restrict macro settings but still want to achieve a high level of Essential Eight maturity, ESET's Endpoint Detect and Respond (EDR) toolset provides compensatory controls you can use. It also offers additional protection if your organisation can restrict macros but desires enhanced security.

ESET's endpoint protection solutions provide multiple layers of defence to not only prevent malicious macros from running but also detect and stop malware introduced through those macros that are still allowed.

User Application Hardening

Strategy Overview

User Application Hardening looks at the configuration of user applications, concentrating on web browsers and Microsoft Office. It aims to block typical malware entry points such as Java and web advertising and stops users from changing applications' security settings.



The ESET Difference

While ESET's solutions do not alter the configuration of other applications, ESET provides a supplementary line of protection when misconfigured applications allow the introduction of malware, and blocking potentially unwanted applications (PUA).

ESET's Reporting functionality allows you to enumerate all applications installed within the environment and enables administrators to remove disallowed applications.

Additionally, ESET's Vulnerability assessment feature enables administrators quickly identify and patch all vulnerable applications, and ESET's Secure Web Browser mitigates the risks of common web browsers referenced in this strategy.

Patch Operating Systems

Strategy Overview

This strategy mirrors application patching but focuses on the operating system.

Given the urgency with which cyber criminals exploit known Windows vulnerabilities, prompting installing all updates and patches released by Microsoft is one of the best ways your organisation can protect its digital assets.



The ESET Difference

ESET Protect provides you with a holistic view of your business's operating systems and patching levels.

The ESET Identify console allows administrators to discover and remediate endpoints which have fallen behind with Windows patching quickly and easily using dynamic templates and automation.

It also lets you configure asset identification and operating system vulnerability scanning in line with your chosen maturity level, use market-leading threat intelligence to prioritise patches with known exploits, and highlight and remove unsupported versions of Windows.

Patch Applications

Strategy Overview

This strategy deals with the pace at which patches from software providers are installed and how an organisation identifies missing patches. Prompt installation of software patches, which frequently target just-discovered vulnerabilities, can form a key part of your cyber defences.



The ESET Difference

Patching applications has long been one of the hardest parts of an IT administrator's job. Identifying every application that every user uses, which vendor supports it, how it's patched, when patches are available and which vulnerabilities have known exploits can be an incredibly time-consuming exercise—not to mention the actual process of delivering patches to the endpoints.

With the latest features in the ESET Protect bundle, this headache goes away.

ESET Protect scans your entire environment, highlighting vulnerabilities and missing patches. Together with market-leading threat intelligence, administrators can easily identify missing application patches and prioritise those with known vulnerabilities.

Scanning and patch installation can even be configured to align with the timeframes required by your chosen level of the Essential Eight.



Application Control

Strategy Overview

Application Control involves restricting and limiting the location and operation of executable files and applications. By doing so, it aims to prevent unauthorised and potentially dangerous software from being installed and run, whether by the user or automatically.



The ESET Difference

ESET Endpoint Protection provides a comprehensive solution to prevent the execution and spread of malware in your environment. Supported by our global threat intelligence and machine learning, ESET EDR goes beyond the Essential Eight's requirements of simply blocking all executions from high-risk locations by examining all software executions from all locations—including fileless attacks.

By monitoring and evaluating the behaviour and reputation of applications, ESET EDR achieves all of the objectives of Application Control without the user frustrations, productivity impacts and management costs associated with application whitelisting.

If your organisation also wishes to implement more rigorous application controls, Safetica DLP, also part of the ESET family, can be used to create policies to allow and block applications based on categories and individual applications.

Multi-Factor Authentication

Strategy Overview

Multi-factor authentication (MFA) uses a range of supplemental authentication methods, including one-time passcodes and smartphone authentication apps. These strategies make password theft and account takeover significantly more challenging, greatly reducing your organisation's risk profile.



The ESET Difference

ESET's Secure Authentication helps you flexibly implement the highest level of MFA across VPNs, Remote Desktop Protocol, Microsoft 365, Outlook Web Access, operating system login and more.

Even better, Secure Authentication can be implemented with push notifications on iOS and Android devices, allowing for a low-cost, highly secure solution with a seamless user experience. If your organisation has higher security requirements, you can also integrate FIDO-compliant hardware devices with the solution.

Secure Authentication includes a full-featured API, as well as an SDK, that organisations can utilise to extend the protections of MFA to the third-party applications and platforms they use—even without a dedicated plugin.

Restrict Administrative Privileges

Strategy Overview

Restricting admin privileges means that users who don't require the ability to administer systems are not given it. It also imposes strict controls on those users with system administration rights. Since most malware needs a degree of administrative access to function, limiting these privileges can considerably lower your organisation's cyber risk.



The ESET Difference

Restricting Administration Privileges is achieved through the configuration of user permissions within each application your organisation uses.

While ESET does not reconfigure permissions within other applications, our products support implementations of restricted admin privileges by allowing the granular configuration of permissions for users who administer ESET solutions.

ESET's permission features support your organisation no matter which level of maturity it's working to achieve, supporting the principle of least privileged access and allowing true role-based access controls to be implemented within the ESET product set.

Regular Backups

Strategy Overview

Backups are essential for recovery from many types of cyber incidents. If data is lost, destroyed, or held for ransom, a recent backup—aligned with your organisation's business continuity requirements—can provide a swift, straightforward, and effective way to get back on track.



The ESET Difference

While the backing up of other systems and applications is not in the scope of ESET's objectives, ESET solutions support this strategy by allowing configuration and critical ESET data to be backed up in line with your organisation's business continuity needs and chosen Essential Eight maturity level.

If your organisation needs further support with business continuity and backup strategies, we have an extensive partner network that can guide you through the process of defining and implementing appropriate backups.

About ESET

WHEN TECHNOLOGY ENABLES PROGRESS, ESET® IS HERE TO PROTECT IT.

ESET brings over 30 years of technology-driven innovation and provides the most advanced cybersecurity solutions on the market. Our modern endpoint protection is powered by unique ESET LiveSense® multilayered security technologies, combined with the continuous use of machine learning and cloud computing.

Backed by the world's best threat intelligence and research, ESET products offer the perfect balance of prevention, detection and response capabilities. With high usability and unparalleled speed, we are dedicated to protecting the progress of our customers, ensuring maximum protection.

ESET IN NUMBERS

1bn+

protected internet users

400k+

business customers

200+

countries and territories

13

global R&D centers

SOME OF OUR CUSTOMERS



Drive your Ambition

protected by ESET since 2017, more than 9,000 endpoints



protected by ESET since 2016, more than 4,000 mailboxes



Canon Marketing Japan Group

protected by ESET since 2016, more than 32,000 endpoints



ISP security partner since 2008, 2 million customer base

COMMITTED TO THE HIGHEST INDUSTRY STANDARDS



eSET® Digital Security
Progress. Protected.