Essential Eight

Implementation Guide

Level 11,
160 Queen Street
Melbourne VIC 3000

Level 13
111 Elizabeth Street
Sydney NSW 2000

Level 38,
71 Eagle Street
Brisbane QLD 4000

Level 1
14 Spence Street
Cairns QLD 4870

Suite 10
17 Karp Court
Bundall QLD 4217

9A Vega Place
Albany
Auckland NZ 0632

High Level Summary

Best-practice implementation of Microsoft Defender for Business and Intune capabilities, including key Essential Eight mitigation strategies supplemented by additional tooling.

Proposed Tasks

Phase #1

Mitigation Strategy	Scope	Maturity Target	Estimated Timeline
Prerequisite: Validate or deploy Intune	Tenant	N/A	1 Day
Prerequisite: Validate or deploy Entra ID	All Windows Workstations	N/A	1 Day

Phase #2

Mitigation Strategy	Scope	Maturity Target	Estimated Timeline
#1 Application Control	All Windows devices	Level 2	4 Weeks
#2 Patch Applications	Review Policies	Level 2	2 Weeks
#3 Patch Operating Systems	Review Policies	Level 2	2 Weeks
#4 Office Macros	All Windows devices	Level 1	1 Day
#5 User Application Hardening	All Windows Devices	Level 1	1 Week
#6 Restrict Admin Privileges	All Users	Level 1	2 Weeks
#7 Regular Backups	All Environment	Level 1	3 weeks
Conditional Access Policies	All Windows Devices & Users	N/A	3 Days

Timeline

Mitigation Strategy	Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7
Prerequisite Tasks	Validate or deploy Intune Validate or deploy Entra ID						
Conditional Access Policies / Multi-factor authentication			Configure Baseline & Review Policies		Review & Configure Device/ Strict Policies	Reporting	
Application Control		Airlock agent deployed in audit mode	Monitoring	Monitoring	Policy review & Enforcement Mode	OTP self-service disabled	Reporting
Patch OS / Applications			Review & Configure Policies	Monitoring	Reporting		
Office Macros		Configure Policies					
User Application Hardening			Configure Policies				
Restrict Admin Privileges			Configure Policies				
Backups			Validate Backups		DR Testing	Reporting	

Application Control

What? An approved list or “whitelist” of applications is compiled and maintained, and only applications on that list can run on computers.

Why? Malicious applications, even those cleverly looking legitimate are blocked from running. This protects users from themselves and is an incredibly powerful way of securing your environment.

How? During a 2-4 week audit phase we install Airlock Digital on all endpoints and configure whitelist policies for SOE applications. After the audit phase endpoints are switched to enforced mode, blocking executables and files that are not approved or whitelisted. OTP mode can be configured to enabled temporary bypass of this policy when required.

Maturity Target
Level 2 (workstations only)

Description
Application control is implemented on workstations to restrict the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications, and control panel applets to an organisation-approved set.
Allowed and blocked executions on workstations are logged.

Patch Operating Systems & Applications

What? A patch management and threat vulnerability management solution provides automation and protection for patching and threat vulnerability management in your tenant.

Why? Devices should be kept up to date with the latest patches and security configurations to ensure and protection from security threats and vulnerabilities.

How? Microsoft Defender for Business is implemented for visibility and threat vulnerability management for all endpoints. Manage Engine Patch Manager Plus is implemented for patching of Operating Systems and third-party applications on all endpoints.

Maturity Target
Patch Operating Systems - Level 2
Patch Applications - Level 2

Description
An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.
A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.
A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services.
A vulnerability scanner is used at least weekly to identify missing patches or updates for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.
Patches, updates or other vendor mitigations for security vulnerabilities in online services are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors and no working exploits exist.
Patches, updates or other vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release.
Patches, updates or other vendor mitigations for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within one month of release.
Online services that are no longer supported by vendors are removed.
Office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products that are no longer supported by vendors are removed.

Office Macro Settings / User Application Hardening / Restricting Administrative Privileges

What? These are three separate Essential Eight controls that we combine together as “Policy Controls”. Together, they prevent unsafe Office macro execution, unsafe and unwanted web browser behaviour, and limit what actions administrators can do.

Why? Office macros allow code to be executed invisibly, potentially causing serious damage. As they are hidden inside innocent documents, they are a common attack vector. Similarly, certain web browser behaviour allows for remote code to be executed. Finally, administrative access should not be unchecked, and its use should be limited to when it is actually required.

How? We group these as Policy Controls because we define them all (and often other things like screen lock time) in a device policy that is then applied to all your devices. We can centrally validate that the policy has been applied, and Conditional Access policies mean that any non-compliant devices cannot access company resources.

Maturity Targets:
Configure Office Macro Settings - Level 1
User Application Hardening - Level 1
Restrict Administrative Privileges - Level 1

Configure Microsoft Office macro settings

Description
Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.
Microsoft Office macros in files originating from the internet are blocked.
Microsoft Office macro antivirus scanning is enabled.
Microsoft Office macro security settings cannot be changed by users.

User application hardening

Description
Web browsers do not process Java from the internet.
Web browsers do not process web advertisements from the internet.
Internet Explorer 11 is disabled or removed.
Web browser security settings cannot be changed by users.

Restrict administrative privileges

Description
Requests for privileged access to systems, applications and data repositories are validated when first requested.
Privileged users are assigned a dedicated privileged account to be used solely for duties requiring privileged access.
Privileged accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services.
Privileged accounts explicitly authorised to access online services are strictly limited to only what is required for users and services to undertake their duties.
Privileged users use separate privileged and unprivileged operating environments.
Unprivileged accounts cannot logon to privileged operating environments.
Privileged accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.

Regular Backups

What? The framework requires regular backups of all your data, and mature processes for storing, protecting and testing those backups.

Why? A solid backup regime is an absolutely essential part of any IT environment. It protects against malicious data loss (a hack, or a malicious insider), accidental loss (such as saving over a file), infrastructure failure, and more. Taking the backups is not enough though – they need to be thoroughly and regularly tested, and there need to be controls in place restricting who can access these backups and how they are retained.

How? Many highly capable backup solutions exist, and we do not prescribe any particular one. Rather, we map out the different locations your store data and ensure that there is a compliant backup in place for each of those, and we align that with your business requirements. We provide best-practice advise on how backups are stored and secured, and we build out policy controls to secure the backups from unauthorised access.

Maturity Targets:
Regular Backups - Level 1

Description
Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements.
Backups of data, applications and settings are synchronised to enable restoration to a common point in time.
Backups of data, applications and settings are retained in a secure and resilient manner.
Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises.
Unprivileged accounts cannot access backups belonging to other accounts.
Unprivileged accounts are prevented from modifying and deleting backups.