“We have MFA, so we’re covered.” It is a common answer in cyber insurance forms and supplier questionnaires. It is also incomplete. Multi-factor authentication is an important safeguard, but it does not fix vulnerable software that attackers can exploit.

If your business has MFA but rarely installs security updates, the obvious Essential Eight gaps are **patch applications** and **patch operating systems**. MFA is one strategy in a broader set. It cannot make an unpatched computer safe, any more than a locked front door fixes a broken window.

This matters to Australian small and medium businesses because Essential Eight questions increasingly appear in procurement, insurance and customer security reviews. A useful answer starts with knowing what the framework asks for—and what your business actually does.

What is the ASD Essential Eight?

The Essential Eight is a set of eight mitigation strategies published by the Australian Signals Directorate (ASD). The Australian Cyber Security Centre (ACSC), which is part of ASD, provides guidance and resources to help organisations understand and implement them.

The strategies were selected to help reduce the likelihood and impact of common cyber threats, including malware, credential theft and exploitation of software vulnerabilities. They are especially relevant to organisations using Windows computers and Microsoft 365, but the underlying practices apply much more broadly.

The Essential Eight is not a product you buy or a certificate you earn by switching on one setting. It is a set of practical controls that need to be implemented, maintained and checked. The ASD also defines maturity levels for assessing how consistently an organisation has implemented the strategies. A maturity level is not a substitute for understanding your actual security gaps.

Why do SMBs keep hearing about it?

Many smaller organisations first hear about the Essential Eight through someone else’s requirements. A customer may send a supplier questionnaire. An insurer may ask about MFA, backups and patching. A tender may ask suppliers to demonstrate alignment with Australian government cyber security guidance.

Adoption is not a universal legal requirement for every Australian business. However, it can become an expected baseline when you work with government, larger organisations or customers handling sensitive information. Cyber insurance applications can also ask about specific controls, such as endpoint protection, MFA and how quickly critical updates are applied. The insurer’s questions and policy conditions—not a general claim of “Essential Eight compliance”—determine what you must disclose or maintain.

Be precise when answering. If a form asks whether operating systems are patched, having MFA enabled does not make the answer “yes”. If you have a process but it is inconsistently followed, say that and describe the gap and remediation plan. Overstating your position can create problems when a claim, tender or supplier review requires evidence.

Which Essential Eight controls are failing if we never patch?

There are two separate patching strategies in the Essential Eight:

- **Patch applications:** Update software such as web browsers, PDF readers, Java components, business applications and other installed programs. Attackers may target flaws in these applications to run malicious code or gain access.
- **Patch operating systems:** Install security updates for Windows and other supported operating systems. These updates address vulnerabilities in the software that manages the computer and its core functions.

These controls overlap in purpose, but they are not interchangeable. A fully updated Windows computer can still be exposed through an out-of-date browser or business application. Likewise, updating applications does not fix weaknesses in an unpatched operating system.

“Never patch” is therefore a serious gap in both strategies. It leaves known vulnerabilities in place after fixes are available. Attackers do not need to discover a new flaw if they can exploit one that organisations have left unaddressed.

MFA helps protect accounts by requiring an additional authentication factor. It can reduce the damage from stolen passwords, but it does not prevent every form of account compromise, and it does not stop an attacker exploiting a vulnerable application or operating system. The controls work together; one does not cancel out the absence of another.

The eight strategies in plain language

Strategy Plain-language purpose Example to check Application control Allow only approved software to run, reducing the chance that unknown or malicious programs will execute. Are users able to run unapproved applications without review? Patch applications Fix security weaknesses in installed programs by applying updates promptly. Are browsers and business applications covered by a patching process? Configure Microsoft Office macro settings Reduce the risk of malicious macros in Office files being used to run harmful code. Are macros restricted, especially when files come from the internet? User application hardening Reduce risky features in everyday applications, particularly features commonly abused by attackers. Are unnecessary browser features disabled or controlled? Restrict administrative privileges Give users only the access they need, and limit powerful admin accounts. Do staff use standard accounts for daily work rather than local admin accounts? Patch operating systems Install security updates for Windows and other operating systems. Are supported devices receiving and installing updates on a defined schedule? Multi-factor authentication Require more than a password to sign in to important systems and services. Is MFA required for remote access, email and administrative accounts? Regular backups Keep recoverable copies of important data and systems so the business can restore after an incident. Can you restore it? Has that been tested?

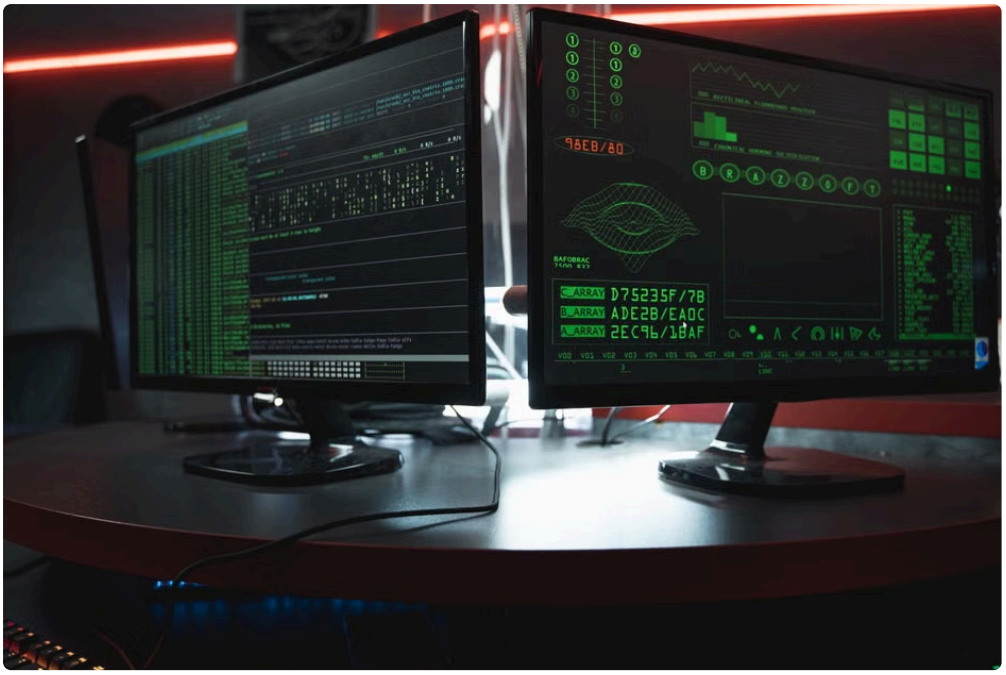
What does “patching” need to mean in practice?

You know what's funny? a vague statement such as “we keep things up to date” is difficult to verify. A workable patching process identifies the devices and applications in scope, assigns responsibility, sets timeframes, checks that updates install successfully and deals with failures.

For a Windows and Microsoft 365 business, start by confirming which computers are in use, whether they are supported, and how updates are managed. Check that security updates are not simply available but actually installed. Then identify important applications that need their own update process. Some software updates automatically; other applications require an administrator or supplier to plan and apply them.

Define how urgent updates are handled, including what happens when a critical security issue is announced. Set a regular review point for devices that have missed updates or are offline. Keep evidence such as update reports, device inventories and records of exceptions. A process that exists only in someone's memory can fail when that person is busy or leaves the business.

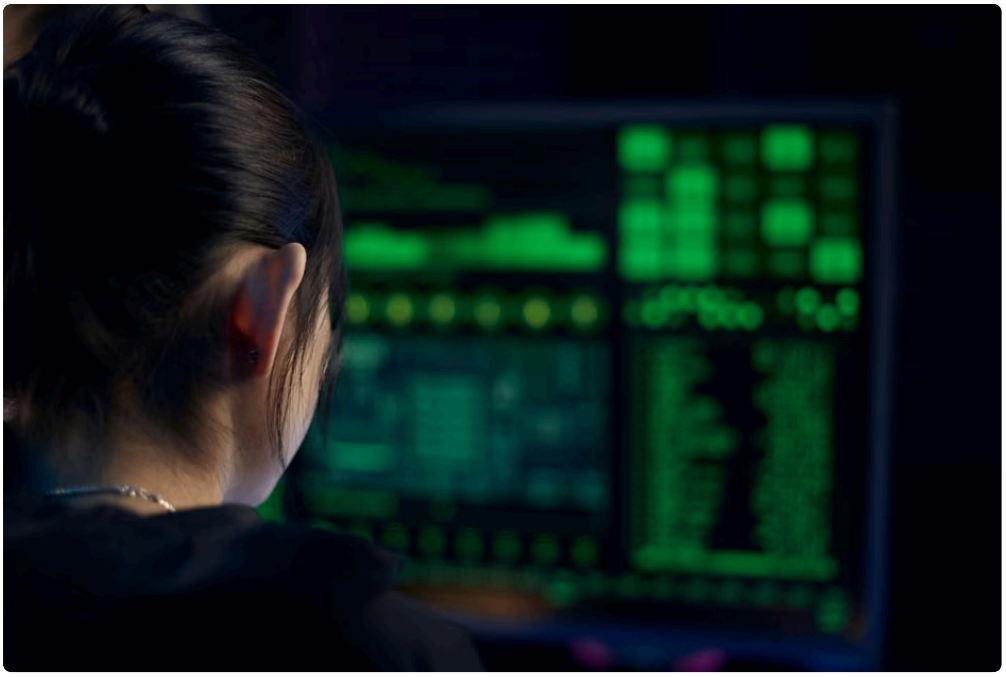
Do not ignore patching because it is inconvenient. If updates cause compatibility problems, test them on a small group first, schedule maintenance windows and agree how to roll back a faulty change. That is a reason to manage patching—not to leave security gaps indefinitely.



Voluntary adoption, expected practice and evidence

The Essential Eight is commonly treated as a practical security baseline, but organisations should avoid claiming more than they can demonstrate. A statement such as "we are basically Level Two" is not a useful assessment. Which maturity level? Which strategies were assessed? What evidence supports the claim? Are there exceptions or systems outside the scope?

For cyber insurance forms and supplier questionnaires, answer the question asked. If asked techguide.com whether MFA is enabled, explain which accounts or services it covers. If asked about patching, describe the systems covered, how often updates are applied and how exceptions are handled. If the control is not yet consistent, say so and provide a dated plan to improve it.



Evidence might include a documented patching procedure, reports showing update status, a list of unsupported devices, and records of approved exceptions. For MFA, evidence could include settings showing where it is required. The right evidence depends on the question and the services in scope.

A sensible first plan for an SMB

1. **List what you need to protect.** Record computers, operating systems, key applications and important cloud services. You cannot manage patches on devices you do not know exist.
2. **Check support status.** Identify computers and applications that no longer receive security updates. Plan to upgrade, replace or isolate them rather than treating them as normal devices.
3. **Establish patching ownership.** Decide who checks updates, who approves urgent changes and who follows up when devices fail to update.
4. **Apply and verify updates.** Set a routine schedule and confirm that updates have installed. Include both operating systems and applications.
5. **Review the other strategies.** Check admin rights, application controls, Office macro settings, user application hardening, MFA coverage and backup restoration.
6. **Keep records and communicate honestly.** Document what is in place, what is not, and what will be fixed next. Use that evidence when completing insurance or supplier forms.

MFA is good. It is not a patching strategy.

If your organisation has MFA but never patches, you have made progress on one Essential Eight strategy while leaving two important strategies—patch applications and patch operating systems—unaddressed. That is not a reason to dismiss MFA. It is a reason to complete the picture.

Start with a clear inventory, a repeatable update process and evidence that updates are installed. Then review the remaining strategies in a way that fits your systems and risks. When a questionnaire asks about patching, answer based on what you can prove—not what you intend to do.

And when someone says, “We have backups,” ask the next question: **can you restore it?** Security controls matter most when they work in practice, not just when they appear on a form.