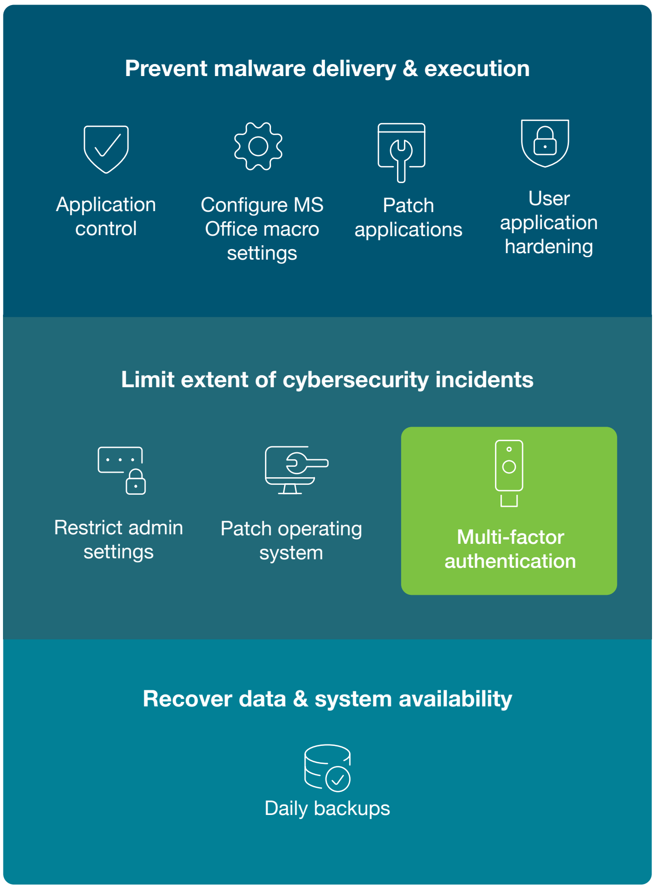
yubico

YubiKey for the Essential Eight

The Essential Eight is a series of eight mitigation strategies from the Australian Signals Directorate (ASD) and the Australian Cyber Security Centre (ACSC) as a baseline recommendation for organisations to minimise the potential impact of cyber security incidents. These mitigation strategies are a complement to the advice included in the Australian Information Security Manual (ISM).

Multi-factor authentication (MFA) is the most effective tool to protect your digital identity and one of the most effective controls an organisation can implement to protect against cyber threats, such as phishing, MiTM attacks, malware and ransomware

Essential Eight mitigation strategies



Prevent malware delivery & execution

Application control

Configure MS Office macro settings

Patch applications

User application hardening

Limit extent of cybersecurity incidents

Restrict admin settings

Patch operating system

Multi-factor authentication

Recover data & system availability

Daily backups

Australian Government
Australian Signals Directorate

ACSC
Australian
Cyber Security
Centre

www.cyber.gov.au/publications/essential-eight-explained

Essential Eight Maturity Model

The Maturity Model supports organisations to implement the Essential Eight mitigations and clearly defines three maturity levels for each mitigation strategy. Organisations should determine a target maturity level and associated mitigation strategies, based on their overall risk profile. For example, Government agencies are required to adopt at least Maturity Level 2.

ASD/ACSC continually reviews the cyber threat landscape. The November 2023 update includes significant changes, specifically to the MFA mitigation strategy, in response to these threats.

What is Multi-factor Authentication (MFA)?

Multi-factor Authentication (MFA) is a security control that requires two or more verification factors to grant access to online services. MFA requires a combination of two or more of the following:

- **Something you know**: a memorised secret such as a PIN, password or passphrase
- **Something you have**: a security key (e.g., a YubiKey), Smart Card, smartphone or one-time password token
- **Something you are**: a biometric identification such as fingerprint pattern or facial geometry

Not All MFA is created equal

While any form of multi-factor authentication provides significant advantages over traditional username and password, some methods are more effective than others. **Phishing-resistant MFA** provides a secure authentication mechanism that is not as susceptible to cyber threats as legacy authentication methods. Legacy methods such as passphrases, mobile authenticator apps, SMS messages, emails or voice calls can all be phished.

As a consequence, ASD/ACSC advise that phishing-resistant MFA should be implemented for all online services (including online customer services), systems and data repositories.

Phishing-resistant MFA requires hardware-backed public key cryptography on a Trusted Platform Module (TPM) along with user intent. The most effective method uses FIDO (Passkey) or PIV (Smart Card) protocols bound to a specifical device, such as a YubiKey. Methods such as Windows Hello for Business and synced passkeys also offer a level of phishing-resistance.

Phishing-resistant methods are the only MFA solutions that meet the requirements of Maturity Level 2 and 3.

Maturity levels for multi-factor authentication

	Maturity level 1	Maturity level 2	Maturity level 3
Applicability	Online Customer Services Organisations Online Services	All System users Online Customer Services Organisations Online Services	All data repositories All System users Online Customer Services Organisations Online Services
Authentication	Something User has AND knows Something User has, unlocked by something user knows/is +	**Phishing Resistant** Something User has AND knows Something User has, unlocked by something user knows/is Smartcard/PIV FIDO	**Phishing Resistant** Something User has AND knows Something User has, unlocked by Something User knows/is Smartcard/PIV FIDO
Reporting		Event logging and incident reporting	Event logging and incident reporting

Authentication methods

Multi-factor authentication uses at least two of the following authentication factors:

- Passwords with six or more characters
- Smart Card
- FIDO Security Keys
- Physical OTP tokens
- Biometrics
- Mobile app OTP
- SMS, email
- Voice calls
- Software certificates
- PIN

Implementing multi-factor authentication

The YubiKey supports multiple protocols on the same physical device, all at the same time. This means the YubiKey combines the functionalities of **phishing-resistant protocols** such as FIDO (U2F, FIDO2) and Smart Cards (PIV) with **legacy protocols** such as physical one-time password (OTP) tokens, and mobile authenticator apps—on a single device.

In addition, a fundamental feature of the YubiKey is support for “user presence” capability, as defined in the FIDO specification. This enforces human presence as a requirement when submitting credentials for authentication. A user simply has to touch the gold dial on the YubiKey or tap the YubiKey to an NFC-reader to prove the physical human presence in the authentication process. This ensures that any remote attack will be unsuccessful. The YubiKey Bio allows for fingerprint authentication, offering the additional convenience of even faster authentication.

The Australian Signals Directorate recognises that a FIDO2 security key, such as a YubiKey, is the most secure form of MFA. The US Cybersecurity & Infrastructure Security Agency (CISA) also recognises FIDO2 security keys as the Gold Standard of MFA.

All currently-supported YubiKeys allow organisations to implement strong phishing-resistant MFA and ensure best possible compliance with Essential Eight. Supporting multiple protocols, the YubiKey streamlines authentication for existing systems while paving the way forward to a passwordless future.

The YubiKey Family

The YubiKey is available in multiple form factors for desktop, laptops and mobile devices.

Contact us
yubi.co/contact

Learn more
yubi.co/yk5

References

Australian Government Information Security Manual
Essential Eight Explained
Strategies to Mitigate Cyber Security Incidents
Essential Eight Maturity Model
Implementing Multi-factor Authentication

Yubico (Nasdaq First North Growth Market Stockholm: YUBICO) is the inventor of the YubiKey, the gold standard in phishing-resistant multi-factor authentication (MFA), and a creator and contributor to FIDO open authentication standards. The company is a pioneer in delivering hardware-based passkey authentication to customers in 160+ countries. For more information, visit: www.yubico.com.