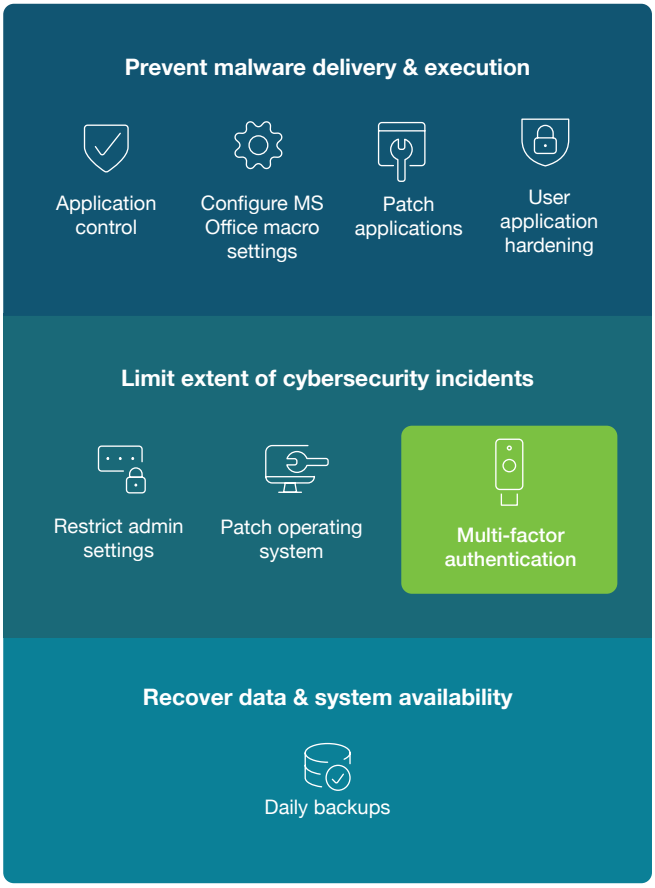
yubico

YubiKey for the Essential Eight

The Essential Eight is a series of eight mitigation strategies recommended by 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 limit the extent of cybersecurity incidents such as phishing, MiTM attacks, malware, ransomware etc.

Essential Eight mitigation strategies



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

What is Multi-factor Authentication (MFA)?

Multi-factor Authentication (MFA) is a security control that requires more than one method of authentication from independent categories of credentials to verify a user's identity for a login or other transaction. 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), smartcard, smartphone or one-time password token
- **Something you are**: a biometric identification such as fingerprint pattern or facial geometry

Essential Eight Maturity Model

To assist organisations in determining the appropriate response and mitigation strategies for their specific business scenario, the Essential Eight is accompanied by a **Maturity Model** with three maturity levels for each mitigation strategy.

As a baseline, ACSC recommends that all organisations aim to reach Maturity Level Three within each mitigation strategy.

It is recognised that some organisations, such as government agencies, financial institutions and critical infrastructure providers are constantly targeted by highly skilled adversaries, or otherwise operate in a higher risk environment and may wish to adopt even stricter controls and mitigation strategies.

Not All MFA is created equal

It is acknowledged that any form of MFA is preferable to none. However, legacy MFA including SMS authentication can still be exploited by hackers. Common methods such as one-time password or authenticator apps offer more protection, but are still vulnerable to increasingly sophisticated cyber attacks.

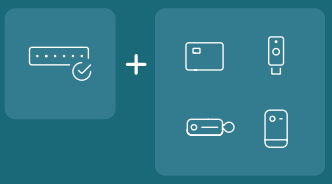
To reliably protect against phishing attacks and prevent attack takeovers, **MFA must be Phishing Resistant**. This only applies to solutions based on FIDO or SmartCard Protocols. As such, these are the **only** MFA solutions that meet the requirements of Maturity Level 3.

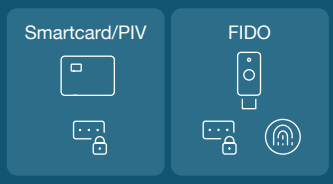
Australian Government
Australian Signals Directorate

ACSC
Australian Cyber Security Centre

Maturity levels for multi-factor authentication

	Maturity level 1	Maturity level 2	Maturity level 3
Applicability	3rd Party Internet facing services Internet facing services	Privileged Users 3rd Party Internet facing services Internet facing services	Important data repositories Privileged Users 3rd Party Internet facing services Internet facing services
Authentication	Any form of 2FA	Something User has AND knows Something User has, unlocked by something user knows	**Phishing Resistant** Something User has AND knows Something User has, unlocked by Something User knows





Authentication methods

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

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

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 smartcards (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 Bio Series and YubiKey 5 Series

From left to right: YubiKey C Bio Fido Edition, YubiKey Bio Fido Edition, YubiKey 5 NFC, YubiKey 5C NFC, YubiKey 5Ci, YubiKey 5C, YubiKey 5 Nano and YubiKey 5C Nano

References

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

Yubico AB
Kungsgatan 44
2nd floor
SE-111 35 Stockholm
Sweden

Yubico Inc.
5201 Great America Pkwy
Suite 122
Santa Clara, CA 95054,
USA