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).

This document provides commentary and links to reference documents to demonstrate how a YubiKey solution complies with the mitigation strategy to limit the extent of cyber security incidents by implementing strong multi-factor authentication.

Multi-factor authentication (MFA) is a security enhancement that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction. MFA is one of the most effective controls an organisation can implement to limit the extent of cybersecurity incidents, such as phishing, MiTM attacks, malware etc.

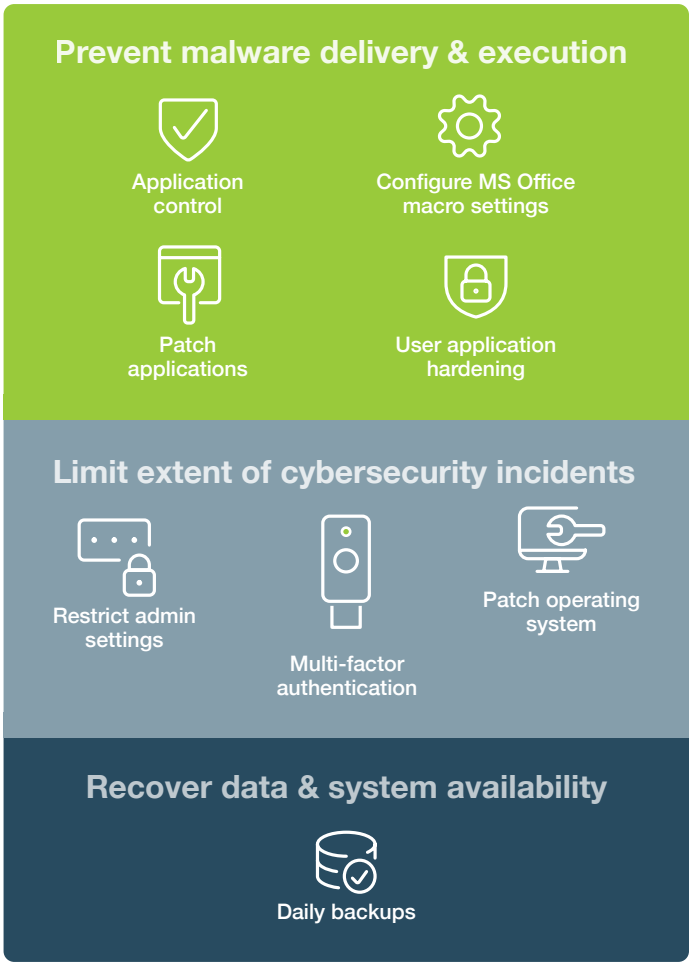
The multiple factors that make up MFA derive from two or more of the following:

- Something you know: a PIN, password or response to a challenge
- Something you have: a physical token, smartcard or software certificate
- Something you are: fingerprint or iris scan

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.

Essential Eight mitigation strategies



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

It is recognised that some organisations, such as government agencies and financial institutions, 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 (previously referred to as Maturity Level Four). As a baseline, ACSC recommends that organisations aim to reach Maturity Level Three within each mitigation strategy.

Maturity levels for multi-factor authentication

	Maturity level 1 Partly aligned with intent of mitigation strategy	Maturity level 2 Mostly aligned with intent of mitigation strategy	Maturity level 3 Fully aligned with intent of mitigation strategy
Applicability	Remote access	Privileged users Remote access	Access Important data Privileged users Remote access
Authentication	+	+	+

User groups

Remote access: all users of remote access solutions

Privileged users: all privileged users and any other positions of trust

Access to important data: all users accessing important data repositories

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
- smart card
- biometrics
- voice calls
- U2F 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 FIDO security keys (U2F, FIDO2), physical one-time password (OTP) tokens, smart cards (PIV) and mobile authenticator apps.

In addition, a key feature of the YubiKey is the “touch” or “user presence” capability, as defined in the FIDO specification. This enforces human presence as a requirement when submitting credentials for authentication. The user simply has to touch the gold dial on the YubiKey or tap the YubiKey to an NFC-reader to prove the presence of a human being in the authentication process. This way remote attacks can be prevented. The YubiKey Bio with fingerprint authentication has been announced and will be available in 2021.

The Australian Signals Directorate states for maximum security and effectiveness organisations should only use security keys that have been certified to the latest U2F specification version. All currently supported YubiKeys are certified for this purpose, allowing organisations to implement strong 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.

References

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