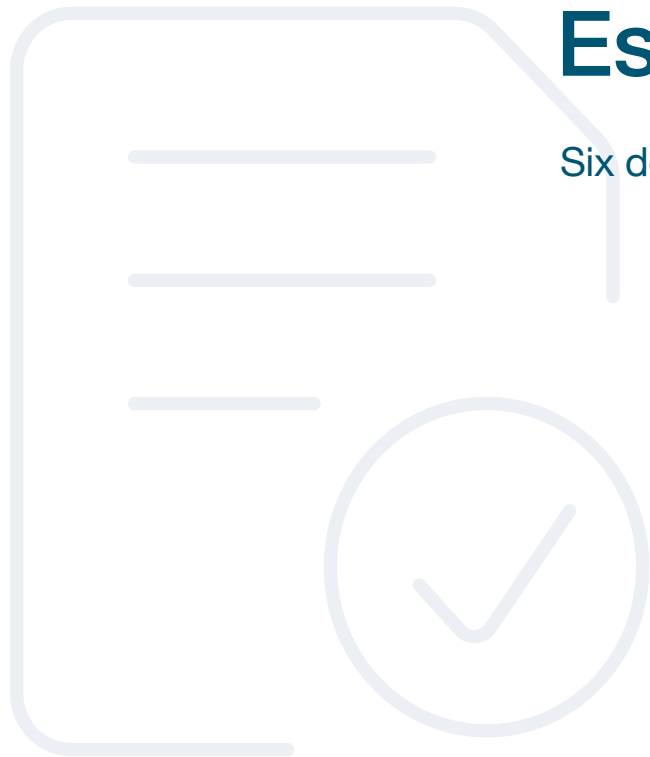


BEST PRACTICES GUIDE

How to get started with phishing-resistant MFA for Essential Eight compliance

Six deployment best practices to accelerate adoption at scale



68%



of cybersecurity breaches involve the human element ¹

\$3.1 billion



lost by Australian organisations to scams in just one year ²

4,500+ scams



on the myGov platform, according to Government services minister Bill Shorten

Choosing the right MFA approach for Essential Eight compliance

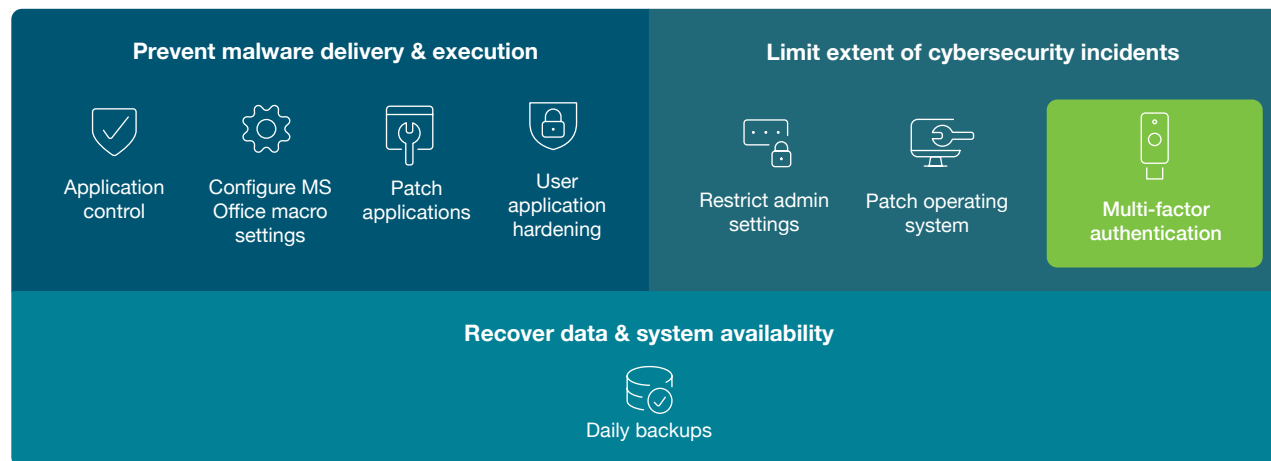
The **Essential Eight** is a series of eight mitigation strategies from the Australian Signals Directorate (ASD) and the Australian Cyber Security Centre (ACSC) as a baseline recommendation for organisations to minimise the potential impact of cyber security incidents.³ These mitigation strategies are a complement to the advice included in the Australian Information Security Manual (ISM).⁴

With increasing cyber threats, and high profile cyber attacks, the need for stronger resilience against cyber attacks has never been higher. In 2023 alone, 4,500 successful breaches resulted in \$3.1 billion in losses for Australian organisations. Phishing remains the dominant attack vector leading to successful data breaches with multi-factor authentication (MFA) one of the most effective controls an organisation can implement to protect against cyber threats, such as phishing, MiTM attacks, the effects of malware and deployment of ransomware.

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 greatly reduces cyber threats in comparison to legacy authentication methods. Legacy methods such as passphrases, mobile authenticator apps, SMS messages, emails or voice calls can all be phished.

As part of the recently released Australian National Cyber Security Strategy 2030, the Australian Government has upgraded their advice for multi-factor authentication through the Essential Eight and now advise that phishing-resistant MFA should be implemented for all online services (including online customer services), systems and data repositories.

Essential Eight mitigation strategies










Maturity levels for multi-factor authentication

The **Essential Eight Maturity Model** supports organisations implementing 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.

	Maturity level 1	Maturity level 2	Maturity level 3
Applicability	<p>Online Customer Services Organisations Online Services</p>	<p>All System users Online Customer Services Organisations Online Services</p>	<p>All data repositories All System users Online Customer Services Organisations Online Services</p>
Authentication	<p>Something User has AND knows Something User has, unlocked by something user knows/is</p> 	<p>Phishing-resistant Something User has AND knows Something User has, unlocked by something user knows/is</p> 	<p>Phishing-resistant Something User has AND knows Something User has, unlocked by Something User knows/is</p> 
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
-  Physical OTP tokens
-  PIN
-  Smart Card
-  Biometrics
-  FIDO Security Keys
-  Mobile app OTP

Two forms of MFA meet the requirements for Essential Eight Maturity Levels 2 & 3: **PIV/Smart Card** and the modern **FIDO2/WebAuthn** authentication standard.

What is phishing-resistant MFA?

Phishing-resistant multi-factor authentication (MFA) refers to an authentication process that stops attackers from intercepting or tricking users at login with the intent of taking over their account. Phishing-resistant authentication utilises hardware-backed public key cryptography on a Trusted Platform Module (TPM) and requires each party to provide evidence of their identity and for the user to communicate their intention to log in through deliberate human action.

The most secure and simple method uses FIDO2 passkeys on a physically separate device, such as a YubiKey. Other methods such as Smart Card, Windows Hello for Business and synced passkeys offer phishing-resistance with differing degrees of security and scalability. Phishing-resistant methods are the only MFA solutions that meet the requirements of Essential Eight Maturity Level 2 and 3.



YubiKey offers phishing-resistant MFA

Yubico created the **YubiKey**, a hardware security key that supports **phishing-resistant two-factor, MFA and passwordless authentication at scale with an optimised user experience.**

The YubiKey is a multi-protocol security key, supporting both PIV/Smart Card and FIDO2/WebAuthn standards along with OTP, which integrates seamlessly into both legacy and modern environments, helping organisations bridge to a passwordless future.

YubiKeys works with hundreds of products, services and applications including leading identity and access management (IAM) platforms, privileged access management (PAM) solutions and cloud services. With flexible 'YubiKey as a Service' offerings, the YubiKey is a cost-effective solution to support shared workstation and kiosk environments subject to high turnover and seasonal staff, along with being highly durable to support the fast-paced and agile workforce.

Modern hardware security keys such as the YubiKey are an ideal option for strong phishing-resistant MFA because they don't require external power or batteries, or a network connection—a user can use a single key for secure access to hundreds of applications and services with the secrets never shared between services. Many authentication solutions are exposed to vulnerabilities via remote attacks due to the compromises necessary to integrate them on a mobile device, such as a smartphone or tablet. The purpose-built hardware, including the touch sensor, on the YubiKey verifies that the person logging in is a real physical human, and not a trojan or remote hacker.

What about passkeys?

Passkeys are a new name for FIDO2 credentials, a standard that's replacing password-only logins with more secure passwordless experiences.

- **Synced passkeys** live on a smartphone, tablet or laptop and can be copied between devices. While synced passkeys enable potentially easier account recovery in the case of a lost or stolen phone or laptop, the FIDO credential is harder to centrally track, so it is most suitable for lower security assurance scenarios.
- **Device-bound passkeys** exist only on a hardware key purpose-built for security, e.g. a YubiKey, suitable for the highest levels of authentication security and compliance assurance. Not relying on a mobile phone for authentication in customer-centric settings (i.e. on sales floors, a front desk, or high traffic areas) provides extra reassurance that a worker is providing undivided attention to a customer.

The YubiKey is proven to **reduce risk by 99.9%**⁵ while delivering a great user experience, letting users securely log in with a single tap or touch:

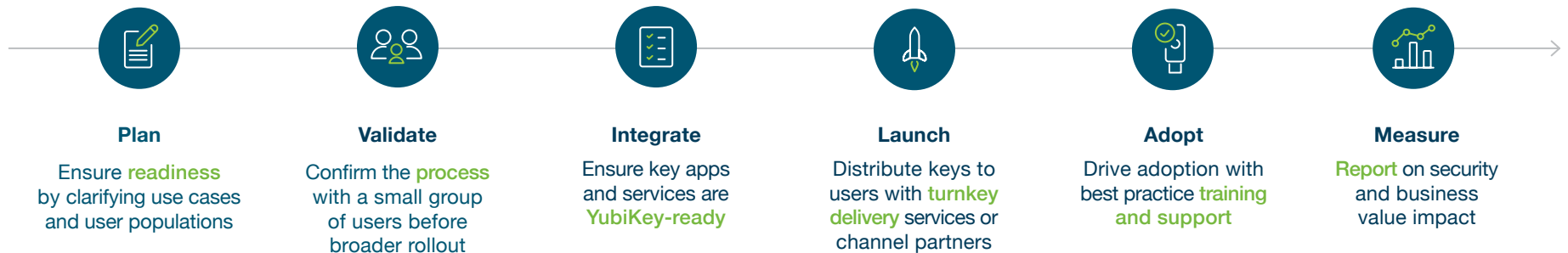


Given the threat landscape, the need for modern phishing-resistant MFA gets clearer on a daily basis. **But how do you start the journey?** The remainder of this guide will detail six key best practices Australian organisations can follow for a successful MFA and YubiKey deployment to meet Essential 8 compliance.



Six key best practices to accelerate the adoption of phishing-resistant MFA

Getting started is easy. Based on Yubico's experience assisting hundreds of customers to deploy phishing-resistant MFA, we have created a six step deployment process to plan for and accelerate the frictionless adoption of phishing-resistant MFA at scale as well as corporate secrets and OT environments.



01. Plan

Clarify use cases and ensure readiness

A **phased approach** is the best way to ensure a frictionless deployment. Put your **high value users and data first**, then expand. Rank use cases and user populations based on risk, workforce location, business impact and ease of technical integration.

Determine use cases

Top scenarios for modern, phishing-resistant MFA



Privileged access

Protect sensitive data and targeted employees who have elevated access to systems or data.



Shared devices

Enable secure and efficient access to shared devices (e.g. shared workstations or kiosks, POS terminals, RFID scanners).



Remote work

Add an extra layer of protection, providing secure access to VPN, IAP, IAM, & IdP platforms.



Software supply chain

Protect code access and implement trusted code-signing.



Customer-facing locations

Mix of users, and shared devices that tie into the brand's corporate environment.



Mobile restricted

Secure areas where mobile devices are not allowed (e.g. call centres, manufacturing environments, server rooms, clean rooms).

User groups



Office and hybrid workers

Sophisticated attacks and lateral escalations make every user a privileged user. Improve security and productivity for office workers.



Call centre

Verify call centre agent identity to provide access to key systems and shared workstations, in mobile-restricted environments.



Customer-facing workers

Use shared devices that tie into the brand's corporate environment (e.g. retail stores, hospitality locations, cruise ships).



Third party

Protect third-party or franchisee access to systems and data.



End customers

Protect customer accounts from fraud & build loyalty and trust with deployments to key customer segments.

“ We are taking great strides in protecting the safety of our guests and colleagues by requiring phishing-resistant MFA methods for all applications that can expose both PII and Card Holder data. We also believe that having Guest Services colleagues looking down at their phone to complete an MFA response or approval does not portray the message we want, to someone walking past the front desk. It lends itself to the perception the colleague is engaged in their cell phone for social media or other personal activity. Using a YubiKey not only provides a more seamless experience for the colleague while keeping our data safe, but also allows those colleagues to keep their cell phones stored away while performing guest-facing roles.”

Art Chernobrov | Director of Identity, Access, and Endpoints Hyatt Hotels Corporation




Assemble key stakeholders

While the number of resources on the project can vary based on the size and breadth of the YubiKey deployment, key stakeholders within the following departments can positively influence the implementation of phishing-resistant MFA across the organisation. It's important to have buy-in across all teams to ensure a smooth rollout:



Engage Yubico experts as needed

Yubico, building on its years of helping secure some of the most security conscious organisations in the world, is focused on helping federal agencies easily access security products and services in a flexible and cost-effective way to heighten security. Agencies can benefit highly from a YubiKeys as a Service model and our Professional Services team offers best-in-class technical and operational guidance in support of your YubiKey implementation and rollout.

YubiEnterprise Services*	Yubico Professional Services	
 YubiEnterprise Subscription	 Deployment 360	 Deployment planning
Simplifies how organisations procure, upgrade and support YubiKeys	Turnkey planning, technical integration and deployment support	Jump start with workshops & projects to review use cases or develop a customised strategy

* YubiEnterprise Services are available for organisations of 500 or more users.



Works with YubiKey

YubiKeys, the industry's #1 security keys, work with hundreds of products, services, and applications. To browse YubiKey compatibility go to yubi.co/wwwyk.



02. Validate

Validate the process with a priority use cases

Validate with a small set of users across a priority use case to gain quick feedback, leveraging Yubico best practice resource guides, videos and engagements. **Practice, learn and then move forward with expansion.**

03. Integrate

Ensure your environment is YubiKey-ready

YubiKeys can work with any number of professional and personal services with no shared secrets between the services, enabling high security and privacy at scale. A single key can work across over 1000 applications and services and secure your users' work and personal digital lives. To ensure that YubiKeys are integrated seamlessly with key applications and services you wish to secure, below are some critical questions to think about. It's a good best practice to first answer these questions for your pilot program, then circle around for each expanded deployment.



Who

Who needs access?

Employees, contractors, third parties, supply chain



What

What authentication approach will you take?

MFA (Password and strong second factor), passwordless



Where

Where in your environment do you require strong authentication?

Critical infrastructure elements, network, applications, developer tools.

How do you manage access?

IAM, IdP, PAM, SSO, VPN, ZTNA



How

How does location impact deployment?





Remote, hybrid, on-premise, multi-office

What types of devices need to be supported?

Owned, BYOD, desktop, laptop, smartphone, tablet

Prepare to deploy

After ensuring that your environment is YubiKey ready, it's time to create a plan to deploy YubiKeys across your organisation. Optimizing deployment involves organisational change management through effective communication, training and support. Yubico offers a variety of Professional Services to help you deploy quickly:

Yubico Professional Services			
 Deployment planning Rollout plan development	 Integration services Architecture and infrastructure review, vendor integration analysis	 Implementation projects Technical engagements to implement YubiKeys in your environment	 Service bundles Flexible consulting hours for when and how you need them



What?

Increase awareness

Build up **user training and support** materials



Why?



Boost engagement

Demonstrate value to the **organisation** and the **user**

04. Launch

Get keys in hands and plan Go Live events

We want your deployment to be as frictionless as possible for all teams and all users. This includes simplifying deployment plans, helping you answer critical questions about how you will distribute keys to users and how you will manage the YubiKey lifecycle.

 Distribution	 Key management
Self-service Channel Partner Delivery	Onboarding Support Offboarding

Why users love the YubiKey



Faster



Easier



More Secure

YubiKey rollout best practice recommendations

Once your users have their YubiKeys, the next step involves registering the keys with the applications and devices they will use. We recommend that each user has a second YubiKey as a backup, and if users cannot locate a YubiKey, revoking and replacing keys is the recommended next step. If a user leaves the organisation, some organisations retrieve YubiKeys prior to their departure while others prefer to allow departing users to keep their YubiKeys and continue using it for their own personal accounts.



Offer **flexibility and choice** since YubiKeys are available in a variety of form factors



Two YubiKeys per person for backup



Future-proof with **extra keys** to cover for churn or lost/stolen keys



Encourage **security** with personal use policies



Plan an event to make the future of your organisation's security exciting

Go Live events

Support the launch with a series of kick-off communications that introduce the YubiKey to users. The ideal Go Live communications make users **excited** about the modern features of the YubiKey.





How to?

Educate users

Have clear calls to action on **how to get started** and **how to get help**



Instead of YubiKey being a highly recommended solution for our clients, we're moving towards making them a required solution. We are building it into our hosting suite, and into our user fees."

Dustin Morse | Business Operations Manager, Retail Control Systems



05. Adopt

Support adoption and boost engagement

At Yubico, we believe success should not be measured by how many YubiKeys you have, but by **how many keys are being used**.

While the Go Live communications educate users on the '**what YubiKeys are**' and the '**why they are important**', support teams need to be prepared to explain the **how**, with FAQs available to help with any questions that may arise for onboarding and troubleshooting (e.g. what to do in case of a lost key).



06. Measure


Report on security and business impact

We know the truth is in the numbers. Validate the pilot against these metrics, then expand to other users to increase the overall business impact.



Ready for scale

yubico



Professional Services

Expert consulting services, including operational and technical workshops, implementation projects on-demand resources and custom engagements, designed to jump-start and accelerate your YubiKey deployment

Services Offered

Deployment 360 Program
A turnkey program packaging all of the essential elements and expertise to ensure your successful YubiKey deployment

Workshops
Interactive sessions designed to help jump-start YubiKey integrations and deployments.

Yubico is leading the charge toward a more secure and passwordless authentication future. For terms of service, contact us.

To download the Professional Services Solution Brief go to yubi.co/ps.

YubiEnterprise Services*	Yubico Professional Services		
YubiEnterprise Subscription	Launch planning	Training & support	Analytics & reporting
Cost effective and flexible YubiKey procurement	Create a marketing and communication plan tailored to your users	Best practice training & support materials and processes	Customised metrics & dashboard design

* YubiEnterprise Services are available for organisations of 500 or more users.



YubiEnterprise Subscription

Gain leading, phishing-resistant authentication security for less than the price of a cup of coffee per user, per month. YubiKeys as a service, via subscription, delivers peace of mind in an uncertain world.

Learn more yubi.co/yes



Ready to get started?

There is no question that phishing-resistant MFA is the solution to secure Australian organisations against modern cyber threats and to streamline critical authentication experiences. Though the path to phishing-resistant MFA and passwordless can seem daunting, it doesn't have to be.

YubiEnterprise Services*



YubiEnterprise Subscription



Deployment 360

Service hour bundles



Workshops

Implementation projects

* YubiEnterprise Services are available for organisations of 500 or more users.



Don't know where to start? The good news is that you don't need to know all the answers upfront about how many keys to buy, what kind, how to integrate them into your environments, preconfiguration options or how to get keys in the hands of end users. No matter where you are on your MFA journey, we'll meet you there.

Modern enterprises recognise that security as a service can take all the guesswork out of achieving success. When you choose YubiKeys as a service, you make decisions as you go with our insight and help, simplifying the process of scaling YubiKeys to wider circles of users as your business needs grow. We include success guides and priority support to help you be successful as quickly as possible.

If you want a closer partnership on any of the six steps of this plan, [Yubico's Professional Services](#) team is here to help.



Contact us
yubi.co/contact



Learn more
yubi.co/ps

Sources

¹ Verizon, [2024 Data Breach Investigations Report](#), (May 30, 2024))

² ACCC, [Targeting scams: Report of the ACCC on scams activity 2022](#), (April 17, 2023)

³ Essential Eight | [cyber.gov.au](#), (May 30, 2024)

⁴ Information Security Manual (ISM) | [cyber.gov.au](#), (May 30, 2024)

⁵ Forrester, [The Total Economic Impact of Yubico YubiKeys](#), (September 2022)



About Yubico

Yubico (Nasdaq First North Growth Market Stockholm: YUBICO) is the inventor of the YubiKey, a hardware security key that is the gold standard in phishing-resistant multi-factor authentication (MFA). Yubico's solutions offer organisations and users deployment expertise and operational flexibility as YubiKeys work across hundreds of consumer and enterprise applications and services.

Yubico is a creator and core contributor to the FIDO2/passkey, WebAuthn, and FIDO Universal 2nd Factor (U2F) open authentication standards, and is a pioneer in delivering modern, hardware-based passkey authentication security at scale to customers in over 160 countries.

For more information, please visit: www.yubico.com.