Essential 8

Duo helps organisations with ACSC Mitigation Strategies.

THE CHALLENGE:

Cyberattacks in Australia continue to rise year after year. Over the 2020-21 financial year, Australia saw a 13% increase in reported cybercrime. This is the equivalent of a cyberattack being reported every 8 minutes, with self-reported losses from cybercrime totalling more than $33 billion. These facts are provided by the Australian Cyber Security Centre (ACSC) in their ACSC Annual Cyber Threat Report 2020-21.

The Australian government released Australia's Cyber Security Strategy of 2020, which highlighted the large investment being made to execute the cyber strategy over the next decade. This clearly positions cybersecurity among the most critical issues on the national agenda.

In July 2021, the ACSC updated its *Essential Eight Maturity Model* based on its ongoing cybersecurity experience and the changing threat landscape. Australian organisations of any size can utilise the maturity model to target a level of maturity suitable for their environment.

The key revisions to the Essential Eight Maturity Model include:

- **Organisations should use a risk-based approach to implement the Essential Eight.** The new model is a departure from the compliance-based approach which relied on a strict interpretation of a prescribed set of rules.
- **Maturity levels are now based on degrees of adversary tradecraft sophistication.** The new model acknowledges that a more capable malicious actor (e.g., a state-backed actor) calls for a more comprehensive Essential 8 deployment. Organizations can identify the maturity level that is suitable for their environment.
- **The new model recommends reaching the same level of maturity across all eight areas** before investing effort in higher maturity levels for just one area.
- **Organisations should consider additional mitigation strategies.** Maturity Level 3 will not stop all adversaries. There is a call to consider the remainder of the mitigation strategies from the *Strategies to Mitigate Cyber Security Incidents* and the *Australian Government Information Security Manual*.

ACSC's publications, such as the *Information Security Manual*, the *Essential Eight Maturity Model* and the *Strategies to Mitigate Cyber Security Incidents*, have high visibility in Australia and New Zealand, and many organisations in APAC and beyond have begun using them to improve their cybersecurity posture.

THE SOLUTION:

How Duo Helps

Cisco's Secure Access by Duo can assist to holistically[1] meet ACSC mitigation strategies:

01

Verify User Identities

Leverage **multi-factor authentication** (MFA) to verify your users' identities before granting them access to internet-facing services, privilege-based use of systems, and important data repositories and applications that may contain personal information.

A foundation of a **zero trust security model**, MFA can assist with mitigating cyberattacks that target user passwords and accounts, such as phishing, credential theft, keyloggers and brute-force attacks.

Explore Duo's Secure Access

02

Assess and Monitor the Device Health

Detect when a device accessing an application is running an out-of-date operating system. Gain control over which devices can access corporate applications, based on the security posture of the device. This includes firewall status, drive encryption status, password status and whether an antivirus/anti-malware agent is running.

Duo helps keep information secure with software and operating system policies. Your Duo administrator may choose to inform you when your software is out of date, require software updates before allowing access, or even block access from devices that don't meet your organisation's requirements.

Explore Duo's Device Trust

03

Implement Strong Authentication Controls

Biometrics and the move to passwordless enhance security by reducing the attack surface from password-based attacks, password compromise and the insecurities of users choosing weak or reused passwords.

The move to **Passwordless** authentication provides a single, strong assurance of users' identities to achieve trust.

Use a solution that supports **password-free open standards**, such as WebAuthn, as MFA methods for Security Assertion Markup Language (SAML) applications. This functionality lets you establish a passwordless login workflow for cloud applications, without ripping and replacing existing infrastructures.

Explore Duo's Passwordless Authentication

04

Strengthen Control with Access Policies

Enforce user access **policies** to block logins, based on IP addresses, countries, anonymous networks such as TOR or anonymous VPNs.

Define and enforce rules via granular based per-application policies.

Duo's operating systems policy settings allow you to control which operating systems and versions are allowed to access your applications.

Explore Duo's Policy & Control

05

Highlight Risky Access Events

Analyse real-time authentication data to establish a baseline of normal user behaviour at the point of login.

Observe access patterns, review risky logins to help the security team identify suspicious activity, and aid in the investigation of compromised accounts.

Use solutions that look holistically at access patterns. Log successful and unsuccessful multi-factor authentications.

Duo creates a baseline of normal user and device access behaviour by analysing and modelling Duo authentication data. The feature considers:

- Who typically accesses
- Which applications
- From which devices
- At what times
- From what locations
- Using which authentication methods

Duo scores deviations from the baseline. Visibility into abnormal access attempts enables Duo administrators to detect suspicious activity and tighten access policies.

Explore Duo Trust Monitor

06

Secure Remote Access

Secure access for your remote workforce without compromising on security. By adding multi-factor authentication to your virtual private network (VPN), you can help increase protection against credential theft.

Duo provides flexible options to accommodate your remote access strategy. Whether you want to add an extra layer of protection to an existing VPN or try a VPN-less alternative (Duo Network Gateway), Duo can help.

Duo Network Gateway allows your users to access your on-premises applications and services (e.g., Secure Shell SSH and Remote Desktop Protocol) without having to install or configure remote access software on their devices.

These features are part of **Duo Beyond**, the most comprehensive suite of access management capabilities. It allows organisations to enforce strong access management with MFA, implement single sign-on (SSO) for easy access to multiple applications, identify corporate vs. personal devices with easy certificate deployment, block untrusted endpoints, and give users secure access to internal applications without using VPNs.

Explore Duo Network Gateway

CONCLUSION

With Duo, you can start your journey toward meeting a variety of requirements issued by the ACSC, from the *Information Security Manual to the Essential Eight Maturity Model and the Strategies to Mitigate Cybersecurity Incidents.*

In addition, Duo can help you incrementally achieve a zero trust transformation, a strategic approach to securing your environment. Establishing user and device trust before granting access to applications, ensuring secure access for any user and device connecting to any application, from anywhere – Duo provides the foundation for a zero trust security model.

This trust-centric approach to security for the extended perimeter makes it much more difficult for attackers or unauthorised users to gain access to applications without meeting certain identity, device and application-based criteria.

[1] The six steps outlined below aren't aligned to a single cybersecurity guidance. They are broader and should be interpreted as a set of incremental security-related steps that organisations need to take on their journey to an optimum level of cybersecurity.

Start your free 30-day trial at **duo.com/trial.**