



A Privilege-First Path through the ACSC Essential Eight

You can’t patch your way out of an identity attack. Control privilege and the Paths to Privilege™ attackers use.

The bind you’re in

The ACSC Essential Eight is a “show me”, not just “tell me”, framework. Maturity Level Two is the Federal Government baseline, yet only 22% of government entities reached it in 2025¹. The three mitigation strategies that arguably deliver the greatest risk reduction—restricting administrative privileges, application control, and user hardening—are also among the most challenging to implement, and each depends on effective privilege management.

Most attacks don’t start with a zero-day; they begin with a single compromised credential that provides a foothold, and standing privileges that allow them to expand that access. The Australian Signals Directorate (ASD) reported that 42% of incidents in 2024–25 involved compromised accounts or credentials². Additionally, as organisations accelerate their adoption of machine identities and AI agents, non-human identities are increasingly gaining access to critical systems.

Taking the Right Approach

For the Essential Eight framework, a strategy counts as fully implemented when each requirement is met directly or through suitable compensating controls. Risk acceptance and cyber insurance don’t count, they result in a Maturity Level Zero.

How BeyondTrust maps to the eight

Strategy	Role	What we do
Restrict admin privileges	Lead	Remove standing admin rights, vault and rotate credentials, implement just-in-time access, record remote sessions, find dormant and over-privileged accounts.
Application control	Lead	Control what executes at the endpoint with just-in-time privilege for approved apps. QuickStart policies enable protection in hours, not months.
User application hardening	Lead	Trusted Application Protection (TAP) blocks Office, browser, and PDF apps from spawning child processes, injecting code, or loading untrusted DLLs.
Multi-factor authentication	Strengthen	Apply MFA on every privileged session and at privilege elevation, including phishing-resistant options. Organisation-wide MFA pairs with your IdP.
Regular backups	Protect access	Manage backup-admin credentials and time-limited, recorded access that stops attackers from deleting backups.
Configure Office macros	Compensating	TAP breaks macro attack chains by blocking child processes and payloads. Macro policy stays in Microsoft tooling.
Patch applications	Compensating	Block known-vulnerable, end-of-life, and unpatched versions from running, with discovery of what runs where.
Patch operating systems	Partner	Report on OS versions and cyber risks. Scanning and patching belong to dedicated tools, provided by our technology alliance partners.

¹The Commonwealth Cyber Security Posture in 2025. Australian Government, Australian Signals Directorate. Feb. 2026.

²Annual Cyber Threat Report 2024 – 2025. Australia Signals Directorate: Australian Cyber Security Centre. Oct. 2025.

Start your Essential Eight compliance

- **Map where you really are:** Our award-winning and complimentary Identity Security Risk Assessment reads your on-premises and cloud identity sources and shows privileged accounts, dormant access, missing MFA, and attack routes. Set up integrations in hours, get results within a day.
- **Pilot where privilege bites:** Prove the value of removing administrative rights and enforcing application control on a small set of high-risk endpoints before scaling across the enterprise.
- **Mature evenly, keep the evidence:** Advance all eight mitigation strategies together toward your target maturity level, then turn privileged activity monitoring, access reviews, and entitlement reporting into audit-ready evidence.

From assessment to assurance

Start with an [Identity Security Risk Assessment](#) to baseline identity risk within your environment, then use Identity Security Insights for continuous monitoring. Where remediation is needed, Identity Security Insights® informs the BeyondTrust Pathfinder Platform's privilege-centric identity security portfolio, including Password Safe®, Endpoint Privilege Management, Privileged Remote Access, and Entitle, to enforce least privilege and secure credentials.

Four solutions IRAP PROTECTED-assessed · 20,000 customers, 75 of the Fortune 100

This document is informational. BeyondTrust is not claiming to be assessed against the Essential Eight. Sources: ASD (cyber.gov.au, Annual Cyber Threat Report 2024–25, and The Commonwealth Cyber Security Posture in 2025). Gartner® and Magic Quadrant™ are trademarks of Gartner, Inc. and/or its affiliates. The Essential Eight is © Commonwealth of Australia.

See it in your environment

Book a complimentary [Identity Security Risk Assessment](#) with BeyondTrust. No cost, no obligation. For further information on our approach to the Essential Eight, read the companion whitepaper: [A Privilege-First Path to Essential Eight Maturity](#).