BeyondTrust

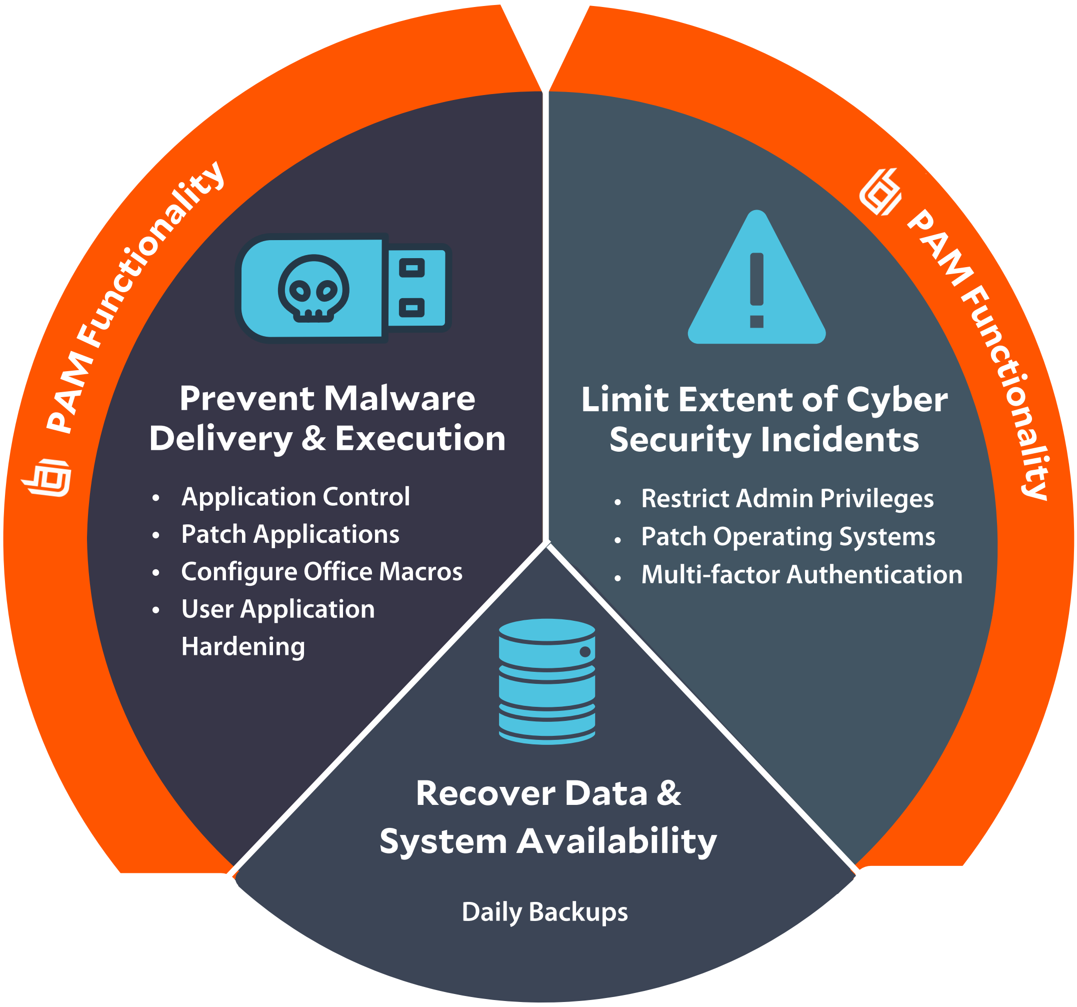
The Essential Eight
& Privileged Access Management

What is Australia's Cyber Security Mandate?

Published by the Australian Cyber Security Centre (ACSC), the Strategies to Mitigate Cyber Security Incidents includes a prioritised list of mitigation strategies to assist organisations in protecting their systems against a range of adversaries.

Privileged Access Management (PAM) solutions can significantly help organisations to meet seven of the Essential Eight mitigation strategies, including all of the Top 4.

Essential 8 Cybersecurity Mitigation Strategies



Prevent Malware Delivery & Execution

- Application Control
- Patch Applications
- Configure Office Macros
- User Application Hardening

Limit Extent of Cyber Security Incidents

- Restrict Admin Privileges
- Patch Operating Systems
- Multi-factor Authentication

Recover Data & System Availability

Daily Backups

Source: ACSC Essential Eight

Maturing with the Essential Eight

The Essential Eight has four maturity levels. Organisations adopting the Essential Eight need to assess their own security priorities to determine their approach to risk mitigation.

Level Zero: Signifies weaknesses that could be exploited by attackers
Level One: Partly aligned with the intent of the mitigation strategy
Level Two: Mostly aligned with the intent of the mitigation strategy
Level Three: Fully aligned with the intent of the mitigation strategy

How BeyondTrust PAM Supports the Essential 8 Requirements

EPM = Endpoint Privilege Management SRA = Secure Remote Access PPM = Privileged Password Management

Mitigation Strategy	Guidance	Levels	EPM	SRA	PPM
Application Control	Prevent all non-approved applications (including malicious code) from executing.	*1-3*	●		
Patch Applications	Patch or mitigate applications with 'extreme risk' vulnerabilities withing 48 hours; use the latest version of applications.	*1-3*	○		
Configure MS Office Macro Settings	Block macros from the Internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.	*1-3*	○		
User Application Hardening	Configure web browsers to block (or uninstall) Flash, ads and Java on the internet; disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.	*1-3*	●		
Restrict Administrative Privileges	Limit access to operating systems and applications based on user duties using the concept of least privilege, and regularly revalidate the need for privileges based on roles and not authentication with administrative privileges for reading email or accessing the Internet.	*1-3*	●	○	
Patch Operating Systems	Patch or mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours; use only the latest operating system version and no unsupported versions.	*1-3*	○		
Multi-factor Authentication	Enable for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive or high-availability) data repository.	*1-3*	○[1]	○	○[2]
Regular Backups	Back up critical data, systems and configs regularly and retain for appropriate length of time; unprivileged and privileged users, outside of backup admins, are not able to modify backups.	*N/A*			

[1] Requires the use of a compatible third party MFA solution or integration with an ITSM for change control approval
[2] Requires the use of a compatible third party MFA solution based on Radius or SSO solution based on SAML

● - Full Coverage ○ - Partial Coverage

Achieve Your Compliance Goals with BeyondTrust

As a Privileged Access Management (PAM) technology leader, BeyondTrust offers a holistic approach to securing every privileged user, session, and endpoint. This Universal Privilege Management model is an expansive approach to securing your entire universe of privileges along a journey that allows you to quickly address your biggest risk areas and immediately shrink your attack surface.

> **“While no single mitigation strategy is guaranteed to prevent cyber security incidents, organisations are recommended to implement eight essential mitigation strategies as a baseline, [making] it much harder for adversaries to compromise systems.”**
>
> **- Australian Cyber Security Centre (ACSC)**

BeyondTrust's Secure Remote Access (SRA), Endpoint Privilege Management (EPM), and Privileged Password Management (PPM) solutions enable organizations to centrally manage remote access for service desks, vendors, and operators, enforce least privilege across Windows, Mac, Linux, and Unix endpoints, and discover, manage, audit, and monitor privileged accounts and credentials.

These powerful capabilities and rapid time-to-value enable you to quickly meet many of the key mitigation strategies of the Essential Eight. Learn more details in our whitepaper, 'Complying with the ACSC Mitigation Strategies'.

GET WHITEPAPER

ABOUT BEYONDTRUST

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organisations to secure and manage their entire universe of privileges. Our integrated products and platform offer the industry's most advanced PAM solution, enabling organisations to quickly shrink their attack surface across traditional, cloud and hybrid environments.

With a heritage of innovation and a staunch commitment to customers, BeyondTrust solutions are easy to deploy, manage, and scale as businesses evolve. We are trusted by 20,000 customers, including 70 percent of the Fortune 500, and a global partner network.

Learn more at beyondtrust.com.

BeyondTrust