WHITEPAPER

Complying with the Australian Cyber Secure Centre (ACSC) Mitigation Strategies

BeyondTrust

Table of Contents

Introduction to the ACSC Essential Eight

Originally published in February 2010, the Australian Signals Directorate (ASD) developed a list of strategies to mitigate targeted cyber intrusions. 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.

The mitigation strategies can be customised based on each organisation's risk profile and the adversaries they are most concerned about. This can be done by picking the maturity level your organisation wishes to meet and mapping your controls against the required criteria. In 2017, four additional recommendations were added, creating the Essential Eight. From time to time the ACSC updates the Essential Eight, clarifying or refining the details of the strategies. This guidance promotes the adoption of sound security and operational practices for managing technology used within Australian Government agencies and departments. However, it is also frequently used by private sector organisations looking to adhere to cybersecurity best practices.

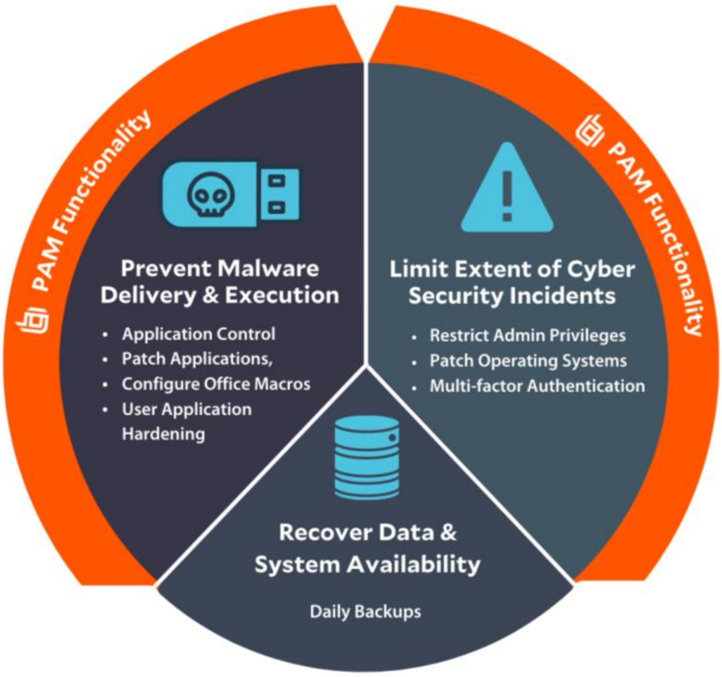
The Essential Eight maps to the Australian Government Information Security Manual (ISM). The ISM provides additional details on the security controls that should be implemented by organisations.

The ISM framework is broken down into cybersecurity principles and guidelines. The principles are strategic in their guidance and are grouped into four key activities: govern, protect, detect and respond. The guidelines provide more practical guidance and cover governance, physical security, personnel security, and information and communications technology security matters.

According to the Australian Cyber Security Centre, 'while no single mitigation strategy is guaranteed to prevent cyber security incidents, organisations are recommended to implement eight essential mitigation strategies as a baseline. This baseline, known as the Essential Eight, makes it much harder for adversaries to compromise systems.'

Meeting the ACSC Essential Eight Requirements with BeyondTrust

In the pages that follow, this compliance brief provides an overview of the Essential Eight and explains how BeyondTrust's Privileged Access Management (PAM) solutions can significantly help organisations to meet seven of the Essential Eight mitigation strategies, including all the Top 4.


PAM Functionality
Prevent Malware Delivery & Execution
• Application Control
• Patch Applications,
• Configure Office Macros
• User Application Hardening
PAM Functionality
Limit Extent of Cyber Security Incidents
• Restrict Admin Privileges
• Patch Operating Systems
• Multi-factor Authentication
Recover Data & System Availability
Daily Backups

MITIGATION STRATEGIES TO PREVENT MALWARE DELIVERY AND EXECUTION

1. **Application Control** (TOP 4)

Control of approved/trusted programs to prevent execution of unapproved and malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA), installers, compiled HTML, HTML applications, control panel applets and drivers to an organisation-approved set.

In addition, application control rulesets are validated on an annual or more frequent basis. Allowed and blocked executions on workstations and servers are centrally logged and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

Why: All non-approved applications (including malicious code) are prevented from executing reducing the impact of malware – including ransomware – should it evade standard endpoint security detection.

How BeyondTrust can help: previously known as 'application whitelisting', this control was perceived as a difficult project to undertake by many organisations. Even in a state of true least privilege, endpoints such as workstations continue to present a sizable attack surface, necessitating the implementation of further controls to effectively secure and control standard user accounts.

By default, standard users have the freedom to execute an unprivileged application without restriction, whether it is part of the operating system or has been downloaded by the user. This capability has given rise to a range of attack techniques and associated threats, which abuse this freedom, notably ransomware. Industry advice is consistent in its recommendation of application whitelisting as not only an effective control, but the most effective cyber threat mitigation.

Similarly, organisations often struggle with the challenges of supporting a whitelisted environment, both in terms of administrative effort required to configure the solution, but also to support and assist end users operating on an endpoint with whitelisting enforced, as their needs change and evolve. With BeyondTrust's Endpoint Privilege Management Solution, you can assign just-in-time (JIT) privileges only to approved applications, scripts, tasks, and commands. This allows you to strike a balance between security and productivity and reduce service desk calls by automatically elevating a user's privileges to trusted apps.

Asserting this control over applications can be done in a matter of hours instead of months by using our Quick Start feature. Leveraging data from thousands of deployments over a decade, QuickStart is unique in the industry, allowing you to operationalise overnight and offer a smarter approach to Privilege Management deployment across your environments to restrict the use of executables, scripts, installers, control panel applets and the installation of approved drivers.

Trusted Application Control to protect the integrity of running processes and guard against malware

With flexible risk-based policies enforcing least privilege and application control decisions, BeyondTrust's Trusted Application Control is essential to preventing advanced malware attacks, enabling you to easily block unauthorised applications, handle diverse user needs flexibly, and defend against zero day and targeted attacks. The Trusted Application Protection capability of EPM is part of the Application Control feature and uses pre-built templates to stop attacks involving trusted apps, catching bad scripts and infected email attachments immediately. It can be used to protect trusted applications such as Word, PowerPoint, Excel, Adobe Reader, common web browsers, and more by controlling their child processes and DLLs. It works by preventing these applications from launching unknown payloads and potentially risky applications such as PowerShell. It also offers protection by preventing untrusted DLLs being loaded by these applications, another common malware technique.

2. **Patch Applications** (TOP 4)

Patch applications like Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers within 48 hours if a vulnerability exists. Use the latest version of applications and remove non-supported applications.

Why: Security vulnerabilities in applications can be used to execute malicious code on systems.

How BeyondTrust can help: While BeyondTrust does not offer patching, we can provide mitigating controls. As a "last line of defense" against versions of applications we know contain potential attack vectors – BeyondTrust allows you to create policies to block an easily compromised application that (for some reason) has not had a patch applied.

This can be performed via the discovery dashboard provided by BeyondTrust Endpoint Privilege Management (EPM), described in the Application Control section, above. This dashboard can provide detailed information on what applications are being run – including their version and where the process is being executed.

The EPM Trusted Application Control, previously described in the Application Control section, can be used to run process control for outdated, legacy line of business applications that are critical to businesses yet cannot be retired/disabled.

3. Configure Microsoft Office macro settings

To 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.

Why: Microsoft Office macros can be used to deliver and execute malicious code on systems.

How BeyondTrust can help: We highly recommend configuring Microsoft Office macro settings to avoid malicious code from entering your systems. Unfortunately, in some cases it is not possible for organisations to implement these controls as it may hinder existing, inflexible processes or legacy systems that are still required. Enabling these controls may not be feasible initially, if at all.

While BeyondTrust doesn't provide a specific solution for this strategy as it is something that needs to be done within the Microsoft application itself, the deployment of our EPM solution and Trusted Application Protection (TAP) will further enhance these security measures, particularly in situations where macros are required for legacy systems or processes. TAP is described in the Application Control section, above.

In addition, malicious macros attempting to execute potentially damaging processes such as command or PowerShell scripts will be visible via the reporting dashboard in the BeyondTrust Endpoint Privilege Manager.

4. User application hardening

Configure web browsers to block Flash (ideally uninstall it), ads and Java on the internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers. Windows Powershell 2.0 is disabled or removed. In addition, blocked PowerShell script executions are centrally logged and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

Why: Flash, ads, Java and Powershell are popular ways to deliver and execute malicious code on systems.

How BeyondTrust can help: To disable unneeded features on Microsoft Office you need to address this in your configuration settings. However, as mentioned above, BeyondTrust Trusted Application Protection, as part of EPM, will block the execution child processes, code injection into other processes and creating executable content.

EPM also includes the ability to implement effective whitelisting, greylisting and blacklisting, where unknown applications can be prohibited from executing (if required). This approach significantly reduces the attack vector on the end points and mitigates 70% of the critical vulnerabilities in the Windows 10 Operating System.

EPM provides a rich set of preconfigured dashboards and reports for executed applications, elevated applications, blocked applications and discovered applications. The latter gives you a breakdown of the applications in your environment and allows you to clearly see what is being what is being used within the organisation, giving visibility into any systems that may require attention.

MITIGATION STRATEGIES TO LIMIT THE EXTENT OF CYBER SECURITY INCIDENTS

5. Restrict administrative privileges

Restricting admin privileges to operating systems and applications based on user duties. Regularly revalidate the need for privileges. Don't use privileged accounts for reading email and web browsing. Additionally, the use of privileged access and changes to privileged accounts or groups is centrally logged and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

The Essential Eight also recommends that credentials for local administrator accounts and service accounts are unique, unpredictable and managed.

Why: Admin accounts are the 'keys to the kingdom'. Adversaries use these accounts to gain full access to information and systems.

How BeyondTrust can help: BeyondTrust recommends organisations employ a multi-layered approach to protect all accounts – whether privileged or standard users – on both servers and workstations.

Leveraging BeyondTrust Password Safe enables enterprise-wide Privileged Access Management (PAM). An automated password and session management solution, BeyondTrust Password Safe provides secure access control, auditing, alerting and recording for any privileged account — for example, a local or domain shared administrator account; a user's personal admin account; operating system local accounts, network device, database (A2DB) and application (A2A) accounts; and even SSH keys, cloud, social media and service accounts.

By improving the accountability and control over privileged passwords, organisations can reduce security risks and achieve compliance objectives. Secondly, restricting privileges on user workstations should be considered an essential part of an organisation's privilege access journey. On average, 88% of Microsoft Critical vulnerabilities could have been mitigated in the last five years if admin rights were removed.

Our market-leading Endpoint Privilege Management solution allows you to remove local admin rights from day 1, without impacting end user productivity. Organisations utilising best practice when it comes to administrative privileges often have two accounts – one to use day-to-day, and another for administrative purposes. Unchecked admin rights carry unnecessary risk and removing them is no longer the time-consuming headache companies assume it to be.

By combining best-in-class privilege management and application control, we have made admin rights removal simple to ensure compliance, security, and efficiency. It deploys in hours and leverages more than two dozen validation criteria to elevate applications securely and flexibly, and elegantly scales to meet the demands of even the largest and most complex organisations. It is however worth remembering that, even if you have removed admin rights, there is still more to be done – such as pragmatic application control, deploying MFA and keeping up to date with patching.

Finally, BeyondTrust Password Safe can generate reports which provide superior visibility into the activities and status of privileged accounts within an environment. Reports include account inactivity – so you can see which accounts are being used and which should be removed or disabled. This includes periodic or scheduled reports on who has access to what in the platform which can be used for governance and/or visibility when performing revalidation of access levels.

6. Patch operating systems

Patch/mitigate computers (including network devices) with ‘extreme risk’ vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.

Why: Security vulnerabilities in operating systems can be used to further the compromise of systems.

How BeyondTrust can help: While BeyondTrust does not patch operating systems, we can do advanced reporting on application versions being run, helping to highlight any issues/risks across your environment. So while BeyondTrust does not help to directly fix patching issues, we can help to locate and identify problems in this area.

7. Multi-Factor Authentication

Multi-factor authentication (MFA) is used to authenticate privileged users of systems and to authenticate users accessing important data repositories. including VPNs, RDP, SSH and other remote access.

Why: Stronger user authentication makes it harder for adversaries to access sensitive information and systems

How BeyondTrust can help: While BeyondTrust does not provide MFA solutions specifically, our Password Safe solution is a simple, cost effective and quick way to integrate MFA for all privileged sessions. Our Application Control solution, EndPoint Privilege Management for Windows and Mac, also includes integration with MFA.

BeyondTrust EndPoint Privilege Management Windows and Mac introduces the ability to integrate policy-based End User Messages with any identity provider (IdP) that supports OpenID Connect (OIDC) for MFA when certain executables, applications or processes are run. Adopting the widely used OIDC protocol means that customers can leverage their existing IdP infrastructure and apply MFA for users operating in higher flex roles, such as developers who need more privileges than other roles.

The MFA feature for EPM is highly configurable and can be combined with other existing types of authentication offered by BeyondTrust to ensure the usability is balanced with security. This feature is ideal as an added layer of security for privileged applications as well as sensitive and higher risk tasks, to ensure that the user is validated with an additional factor.

MITIGATION STRATEGIES TO RECOVER DATA AND SYSTEM AVAILABILITY

8. Daily backups

Backups of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.

Why: To ensure information can be accessed following a cyber security incident (e.g. a ransomware incident).

How BeyondTrust can help: While BeyondTrust do not provide a backup solution, our products provide a great ability to perform scheduled backups.

The Essential Eight Maturity Model

To assist organisations in determining the maturity of their implementation of the Essential Eight, as of July 2021, four maturity levels have been defined for each mitigation strategy. The maturity levels are based on mitigating increasing levels of cyber "tradecraft" and are defined as:

- **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

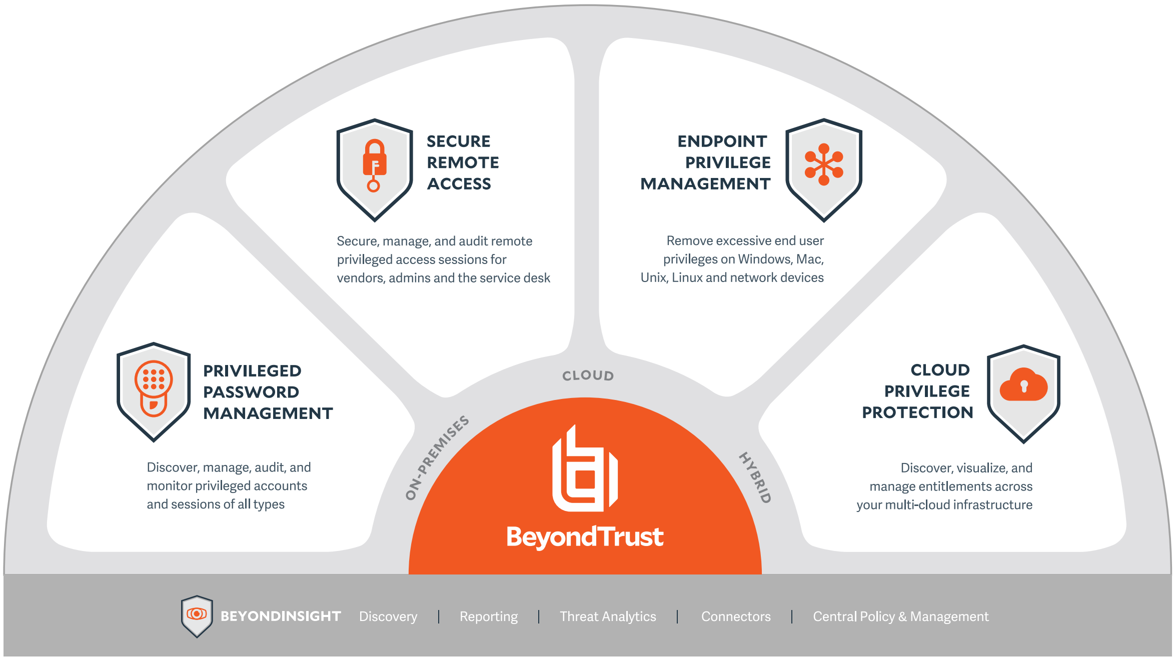
Implementing BeyondTrust Privileged Access Management solutions helps organisations to accelerate their maturity level, in many cases to level three, ensuring they meet compliance/recommendations without hindering users.

The BeyondTrust Privileged Access Management Platform

The BeyondTrust Privileged Access Management (PAM) portfolio is an integrated solution set that provides visibility and control over the entire universe of privileges—identities, endpoints, and sessions.

BeyondTrust delivers what industry experts consider to be the complete spectrum of privileged access management solutions. In the Magic Quadrant for Privileged Access Management, Gartner named BeyondTrust as a leader for all solution categories in the PAM market.

BeyondTrust's extensible, centrally managed platform allows you to roll out a complete set of PAM capabilities at once, or phase in capabilities over time at your own pace.


SECURE REMOTE ACCESS
Secure, manage, and audit remote privileged access sessions for vendors, admins and the service desk
ENDPOINT PRIVILEGE MANAGEMENT
Remove excessive end user privileges on Windows, Mac, Unix, Linux and network devices
PRIVILEGED PASSWORD MANAGEMENT
Discover, manage, audit, and monitor privileged accounts and sessions of all types
CLOUD PRIVILEGE PROTECTION
Discover, visualize, and manage entitlements across your multi-cloud infrastructure
CLOUD
ON-PREMISES
HYBRID
BeyondTrust
BEYONDINSIGHT
Discovery
Reporting
Threat Analytics
Connectors
Central Policy & Management

BeyondTrust's Universal Privilege Management approach provides the most practical, complete, and scalable approach to protecting privileged identities (human and machine), endpoints, and sessions by implementing comprehensive layers of security, control, and monitoring. The complete BeyondTrust solution allows you to address the entire journey to Universal Privilege Management, to drastically reduce your attack surface and threat windows.

By uniting the broadest set of privileged security capabilities, BeyondTrust simplifies deployments, reduces costs, improves usability, and reduces privilege risks.

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.

The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving organisations the visibility and control they need to reduce risk, achieve compliance, and boost operational performance. Our products enable the right level of privileges for just the time needed, creating a frictionless experience for users that enhances productivity.

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.