CYBERARK®

WHITE PAPER

ADDRESSING THE AUSTRALIAN ESSENTIAL EIGHT CYBER SECURITY MATURITY MODEL

The role of Privileged Access Management in meeting the ACSC's strategies to mitigate cyber security incidents

Table of Contents

An information-security best practices primer to minimise the risks of exposure of sensitive information in case of a data breach.

CyberArk Privileged Access Security Solution helps address five key areas of the "Essential 8".

Executive Summary

The Australian Signals Directorate's Australian Cyber Security Centre (ACSC) has developed prioritised **Strategies to Mitigate Cyber Security Incidents**, to help organisations mitigate cyber security incidents caused by various cyber threats. The most effective of these mitigation strategies are known as the **Essential Eight**.

One of the biggest risks identified by the ACSC is the incidence of "spear phishing" attacks. Often used by criminals wanting to compromise a particular company's network, spear phishing involves an email crafted to look like something seemingly innocent, such as a current job application, which is then emailed to the HR manager. According to the ACSC, these types of attacks have been extremely successful in compromising Australian networks.

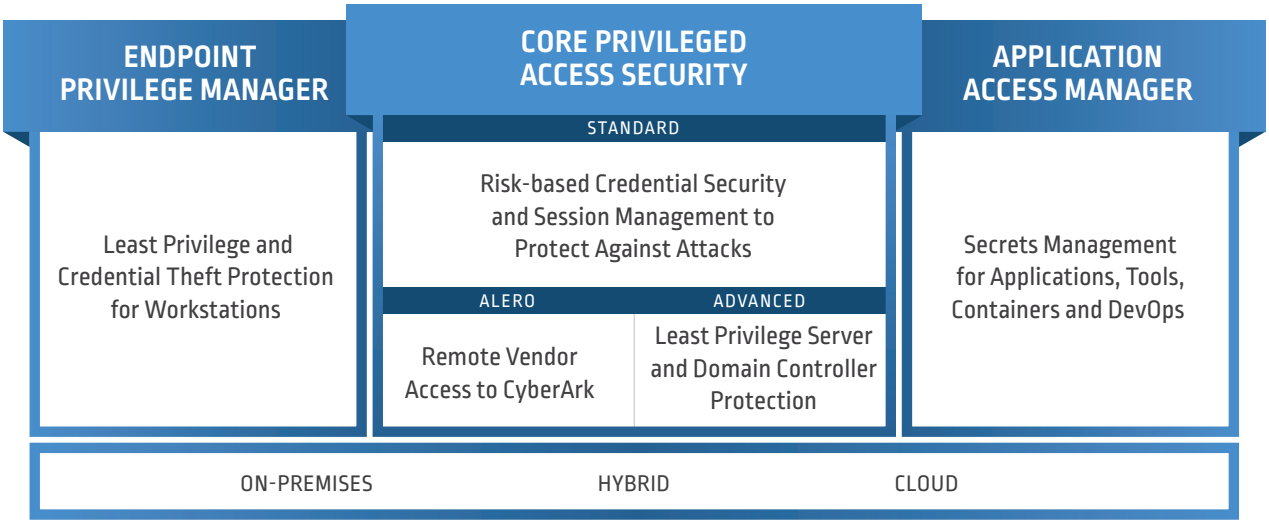
Due to their highly targeted nature, such attacks are difficult to protect against without introducing draconian security measures, which themselves could seriously hamper individual workers or even entire departments from properly executing their job function. However, if a user, application, or any network element is compromised, businesses need to be able to ensure that the security breach is quickly isolated and the network is locked down, this way stopping the intruder from accessing core systems.

CyberArk Privileged Access Security solutions provide comprehensive protection, accountability and intelligence for your privileged accounts, helping you to address five of the "Essential Eight" risk mitigation strategies.

The **CyberArk Core Privileged Access Security Solution** provides lifecycle management, securing privileged access to critical systems and automating the controls needed for privileged access management, thus better protecting the organisation. The solution allows organisations to manage, track and audit their most privileged identities, avert internal and external threats, and prevent the loss of sensitive information.

CyberArk's Privileged Access Security Solutions

CyberArk is the trusted expert in Privileged Access Management (PAM), securing over 5000 enterprises including 50% of the fortune 500. Analyst firms Gartner, Forrester and KuppingerCole have consistently ranked CyberArk as the market leader. Designed from the ground up with a focus on security, CyberArk has developed a powerful, modular technology platform that provides the industry's most comprehensive Privileged Access Security Solution. Each product can be managed independently or combined, offering you a cohesive and complete solution for operating systems, databases, applications, hypervisors, network devices, security appliances and more. The solution is designed for all systems on-premises and in the cloud, from every endpoint, through the DevOps pipeline.



All privileged administrator credentials and audit logs are securely stored and archived in CyberArk's Digital Vault – a 'Digital Safe Haven' within the organisation and accessed only by authorised users, such as IT staff, administrators, control room personnel and others, while providing full accountability. The multiple security layers (including firewall, VPN, strong authentication, access control, encryption, and more) at the heart of the CyberArk solution offer a secure outlet for storing and sharing credentials, and protecting audit logs from modification or deletion.

Furthermore, the CyberArk Core Privileged Access Security Solution enables organisations to isolate, control and monitor privileged activity on sensitive target systems in the data centre – whether in real time to detect suspicious behaviour or as a recorded playback for forensic analysis at times of audit or change management review.

CyberArk Core Privileged Access Security Solution Features

- **Discover and Manage Credentials:** Continuously scan the environment to detect privileged access, validate privilege by adding discovered accounts to pending queue or automatically onboard and rotate accounts and credentials based on enterprise policy
- **Isolate Credentials and Sessions:** Establish a secure control point to prevent credential exposure and isolate critical assets from end users with transparent connections to target systems via a variety of native workflows
- **Record and Audit Sessions:** Automatically record and store privileged sessions within a centralized encrypted repository, prioritize the audit of recorded and active sessions with video playback that streamlines the review of the most suspicious activity
- **Monitor Privileged Activity:** Administrators can view specific activities or keystrokes within video recordings, detect and alert on anomalous behaviour that bypasses or circumvents privileged controls
- **Remediate Risky Behaviour:** Automatically suspend or terminate privileged sessions based on risk assignment, and initiate automatic credential rotation in the event of privileged compromise or theft
- **Least Privilege Server Protection:** Centrally manage and enforce granular access controls, establish super-user accountability on both Windows and *NIX servers and centralize the audit trail of all privileged access activity across server environments
- **Domain Controller Protection:** Continuously monitor the network and detect in-progress Kerberos attacks including Golden Ticket and Pass-the-Hash and block suspected credential theft and harvesting attempts on domain controllers

CyberArk Endpoint Privilege Manager

CyberArk Endpoint Privilege Manager enables organisations to remove local administrator privileges from business users and control applications on Windows endpoints and servers, reducing the attack surface without halting business user productivity or overwhelming IT teams. This approach aligns with industry best practice recommendations and provides privilege on demand.

Enforcing the principle of least privilege, the solution helps organisations eliminate local administrator privileges from business users while seamlessly elevating privileges as needed for business purposes. It also delivers application controls that are designed to manage and control which applications are permitted to run to prevent malicious applications from penetrating the environment.

Both CyberArk PAS solution and EPM combined provides organisations a "Zero Trust" access model to provide temporary elevated access using Just-In-Time (JIT) provisioning. JIT provides customers with the ability to temporarily provide local admin access to Windows workstations, servers, and Mac OS on a by-request, timed basis and to remove access when time expires. JIT Elevation and Access with EPM provides a full audit trail for privileged activities with the ability to terminate applications and sessions in real time.

Securing Remote Vendor Access with CyberArk Alero

Building upon the **Core Privileged Access Security Solution** Cyberark has recently developed Alero to help manage remote vendor access.

Alero integrates Zero Trust access, biometric multi-factor authentication, just-in-time provisioning and full integration with CyberArk Core Privileged Access Security for full visibility and audit for administrators, into one single SaaS solution. By requiring remote users to authenticate their identities using biometric capabilities of smartphones, organisations are able to introduce a Zero Trust framework for remote users seeking access to critical assets being managed by CyberArk Core Privileged Access Security. Security administrators can provision access to users for a specific amount of time and/or a specific number of sessions. This provides remote vendors with the minimum amount of access they need, and automatically deprovisions access when it is no longer required.

Alero eliminates the need for VPNs, agents or passwords that can frustrate users, add risk and create administrative headaches. Instead, remote vendors authenticate using native smartphone facial or fingerprint recognition functionality and are provisioned and authenticated for secure access to the CyberArk Core Privileged Access Security Solution via Alero. Once authenticated, all privileged sessions are automatically recorded for full audit and monitored in real-time.

Securing Applications with Application Access Manager

CyberArk recognises that privileged credentials exist everywhere including within applications and the DEV OPS pipeline.

CyberArk Application Access Manager is designed to provide comprehensive privileged access, credential, and secrets management for widely used application types and non-human identities. The Application Access Manager secures credentials for commercial off-the-shelf applications, traditional internally developed applications, scripts, as well as containerised applications built using DevOps methodologies.

Application Access Manager is designed to provide a strong security solution that enables organisations to control, manage, and audit all non-human privileged access for applications, across on-premises, hybrid, containerised and multi cloud environments and can integrate with the **Core Privileged Access Security Solution providing a single powerful capability**.

CyberArk's Privilege Cloud

CyberArk has also recognised many organisations want to offload the overhead of managing an on-premise instance of the **Core Privileged Access Security Solution**. As of January 2020, CyberArk launched Privilege Cloud within Australia. With more and more agencies looking to use SaaS based offerings, CyberArk has provisioned this inside a PROTECTED environment. Privilege Cloud is built to protect, control, and monitor privileged access across on-premises, cloud, and hybrid infrastructures. Designed from the ground up for security, CyberArk's solution helps organisations efficiently manage privileged account credentials and access rights, proactively monitor and control privileged account activity, and quickly respond to threats. This offering also takes the burden off organisations needing to manage the infrastructure in-house.

CyberArk Privilege Cloud Features include:

- **Secure the management console** - detect, manage and monitor both human and non-human access to cloud management consoles and portals
- **Secure the organization's cloud infrastructure** - automatically secure dynamically provisioned compute instances and other cloud resources.
- **Secure API access keys & secrets** - secure and manage keys and secrets used to access cloud resources and for application-to-application interactions.
- **Manage the DevOps pipeline** - secure and manage passwords, access keys, secrets and credentials used to access management consoles.
- **Native and secure access to XaaS platforms** - transparent access to cloud (IaaS and PaaS), SaaS and social media with built-in isolation, monitoring and audit.
- **Run privileged access security in the cloud** - easily replace embedded credentials with api calls, so as to meet security policies and requirements.
- **Threat analytics in the cloud** - enabling monitoring in the cloud to ensure privileged users are operating within policy and mitigating risk from advanced.

CyberArk Privileged Access Security (PAS) Solutions Helping Organisations Reach ACSC Essential Eight Maturity

Cyberark can help specifically address the Essential 8 within our capability portfolio in the following way.

MITIGATION STRATEGIES TO PREVENT MALWARE DELIVERY AND EXECUTION	
Mitigation Strategies	**CyberArk Solution**
Application whitelisting of approved/trusted programs to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers. **Why:** All non-approved applications (including malicious code) are prevented from executing.	**CyberArk Endpoint Privilege Manager** enables organisations remove the barriers to enforcing least privilege and allows organisations to block and contain attacks at the endpoint, reducing the risk of information being stolen or encrypted and held for ransom. Application Control allows whitelisting of applications that can be launched on the endpoint and applications that will run in an elevated context. This functionality can block known blacklisted malware such as ransomware and software tools used during an attack, as well as restricting unknown, or grey-listed, application's access to resources such as the local file system, intranet or internet. **Least Privilege Server Protection for *NIX** provides a comprehensive solution that empowers IT and enables complete visibility and control of *NIX super users and privileged accounts across the enterprise.

MITIGATION STRATEGIES TO PREVENT MALWARE DELIVERY AND EXECUTION	
Mitigation Strategies	**CyberArk Solution**
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.	**CyberArk Endpoint Privilege Manager** policy can be defined to allow vetted macros in trusted locations or limit write access which prevents macros from executing potential malicious payloads. Trusted sources functionality extends to greylisting of applications to allow restricted execution of unknown applications to certain capabilities e.g. removing the ability to access the internet. CyberArk Endpoint Privilege Manager has the ability to prompt for MFA when elevation of privileges is required to access IT resources.

MITIGATION STRATEGIES TO LIMIT THE EXTENT OF CYBER SECURITY INCIDENTS	
Mitigation Strategies	**CyberArk Solution**
Restrict administrative 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. **Why:** Admin accounts are the 'keys to the kingdom'. Adversaries use these accounts to gain full access to information and systems.	**Core Privileged Access Security Solution** provides organisations with the ability to automatically discover where privileged accounts exist on servers, workstations, network devices and virtual environments. It then securely provides its users with only the necessary privileged access they need in order to complete their role, based on pre-defined policies. CyberArk removes the cloak of anonymity typical to shared administrative accounts and attributes every privileged access to an individual, for full accountability. Just-in-Time access to Windows Servers introduces a new way to control admin access and maintain security without using permanent credentials. Just-in-Time strengthens local admin security by providing Windows administrators just-in-time access to Windows targets on-demand for a specific period of time through user requests capabilities within the CyberArk's Core Privilege Access Security solution. **The solution** provides a jump server architecture which enables isolated administration, session monitoring, and recording with full audit capability as well as remote session termination for detection of any suspicious or non-compliant activity. **Furthermore, the solution delivers** intelligence-driven analytics that enable you to identify suspicious and malicious privileged user behaviour within your organisation. The Core Privileged Access Security Solution distinguishes, in real-time, between normal and abnormal user behaviour, raising alerts when abnormal activity is detected.

MITIGATION STRATEGIES TO LIMIT THE EXTENT OF CYBER SECURITY INCIDENTS	
Mitigation Strategies	**CyberArk Solution**
Multi-factor authentication including for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive/high-availability) data repository. **Why:** Stronger user authentication makes it harder for adversaries to access sensitive information and systems.	**CyberArk Privileged Access Security Solution** easily integrates with common multi-factor authentication systems to enable an extra layer of protection. This additional control ensures that all credentials stored within the CyberArk Privileged Access Security Solution can only be accessed by those authorised to do so. This will mitigate against common credential theft techniques, such as basic key loggers or more advanced attack tools that are capable of harvesting plaintext passwords. **CyberArk Alero** combines Zero Trust access, biometric multi-factor authentication and just-in-time to provide fast, easy and secure privileged access to remote vendors who need access to critical internal systems. Alero ensures that remote vendors only access what they need by fully integrating with CyberArk Core Privileged Access Security for full audit, recording and remediation capabilities.

CyberArk Government and Compliance Overview

CyberArk is committed to supporting Federal, State, Local Government & Enterprise organisations by continuously certifying its technology.

CyberArk holds the industry's most comprehensive set of privileged access management government certifications, including the international Common Criteria certification by the National Information Association Partnership (NIAP). The Common Criteria certification validates that the CyberArk Privileged Access Security Solution meets strict security requirements for Federal Government agencies. This certification is mutually recognised by ASD along with 31 member countries globally to assess security solutions.

The acknowledgement from NIAP extends the list of CyberArk solutions that have achieved Common Criteria certification. The CyberArk solution was previously awarded an Evaluation Assurance Level (EAL) 2+ under the Common Criteria Recognition Agreement (CCRA). CyberArk is also included on the U.S. Department of Defense Information Network Approved Products List (DoDIN APL) and the U.S. Army Certificate of Networthiness (CoN) under the Cybersecurity Tools (CST) device type (Tracking Number (TN) 1712401). CyberArk helps US federal agencies meet compliance requirements including FISMA/NIST SP 800-53, Phase 2 of the Department of Homeland Security Continuous Diagnostics and Mitigation (CDM) program, NERC-CIP, HSPD-12 and more.

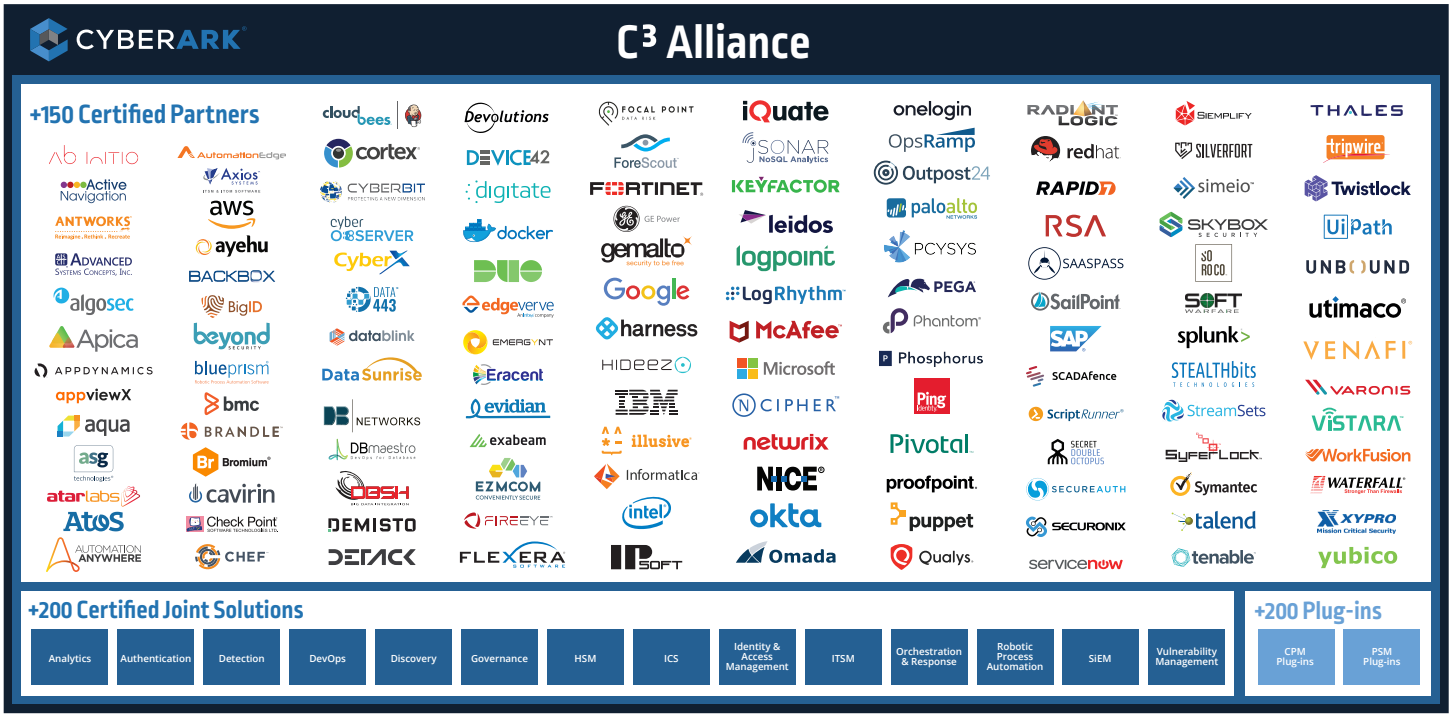
These certifications underscore CyberArk's commitment to helping agencies and global enterprises secure privileged accounts – the "keys to the IT kingdom" – before cyber attackers can steal and exploit them to gain access to sensitive data and systems.

CyberArk can also assist enterprises addressing the following Audit & Compliance requirements:

- FISMA/NIST SP800-53
- The General Data Protection Regulation (GDPR)
- ISO/IEC 27002
- Payment Card Industry Data Security Standard
- Sarbanes Oxley (SOX)
- SWIFT

CyberArk C3 Alliance

Protecting high value assets and data in an increasingly complex environment requires high levels of innovation and collaboration to defend against evolving, increasingly damaging attacks. The C3 Alliance's pre-integrated, certified and supported solutions include offerings from leading enterprise software, infrastructure, and security providers.



About CyberArk

CyberArk (NASDAQ: CYBR) is the global leader in privileged access security, a critical layer of IT security to protect data, infrastructure and assets across the enterprise, in the cloud and throughout the DevOps pipeline. CyberArk delivers the industry's most complete solution to reduce risk created by privileged credentials and secrets. The company is trusted by the world's leading organizations, including more than 50 percent of the Fortune 100, to protect against external attackers and malicious insiders. The company has offices throughout the Americas, EMEA, Asia Pacific, Japan, Sydney, Melbourne and Canberra. To learn more about CyberArk, visit www.cyberark.com, read the CyberArk blogs or follow on Twitter via @CyberArk, LinkedIn or Facebook.