CYBERARK®

WHITEPAPER

Addressing the Australian Essential Eight Cyber Security Maturity Model

CyberArk Identity Security Platform

Table of Contents

Federal government agencies and their contractors are frequent targets in today's advanced attacks. Whether the goal is to compromise sensitive government data, steal personally identifiable information (PII) or disrupt normal operations, the increasing sophistication of attacks is making it more difficult to safeguard the federal government's critical cyber infrastructure.

The Australian Signals Directorate's Australian Cyber Security Centre (ACSC) has developed prioritised Strategies to Mitigate Cyber Security Incidents. These strategies help organisations deal with cyber threats in accordance with best practices the most effective of these mitigation strategies are known as the Essential Eight

CyberArk as a trusted partner, the world's leading organisations can more effectively defend against attacks, enable the digital business, drive operational efficiencies, and satisfy audit and compliance. CyberArk recognises that these key value drivers are required when helping you address "Essential Eight" risk management strategies.

For over 20 years CyberArk has been the undisputed market leader in securing privileged identities. During this time, we have observed a shift in the security mindset of organisations to one in which identity is becoming the modern approach to securing enterprises. At CyberArk we believe that the definition of what a privileged identity is has evolved dramatically. We see ANY user now under the right circumstances being able to perform actions that are now considered as privileged.

This is reflected in our evolving Identity Security Platform which takes a risk-based approach to helping customers determine which capabilities they require. This approach ensures that CyberArk is not just a technology solution but can show a tangle risk reduction against well understood risks.

CyberArk's Identity Security Business Value Assisting Government

Defend Against Attacks — Protect against the leading cause of breaches — compromised identities & credentials.

Enable the Digital Business — Improve business agility to deliver great digital experiences that balance security with a frictionless user experience.

Drive Operational Efficiencies — Reduce complexity and burden on IT from identity security solutions while improving protection of the business.

Satisfy Audit and Compliance — CyberArk help you deliver on extensive compliance requirements from regulations, frameworks & standards with a unified solution.

Defence Against Attacks:
Secure

- Foundational, risk-based PAM controls
- Adaptive and contect based Access
- Least Privilege, JIT access
- Human and machine identities
- Broad, Hybrid platforms
- Trusted advisor, CyberArk Labs

Drive Operational Efficiencies:
Simplify

- Consistently enable privileged users
- Centralized visibility and control
- Self service
- Native access
- SaaS model
- Technology partnerships
- CyberArk Blueprint

Enable the Digital Business:
Accelerate

- Deliver trusted customer experiences
- Platform for current and future IT environment
- Broadest out-of-the-box integrations
- Velocity and agility
- API first
- Maximum uptime and availability
- Cloud agnostic

Satisfy Audit and Compliance:
Standardize

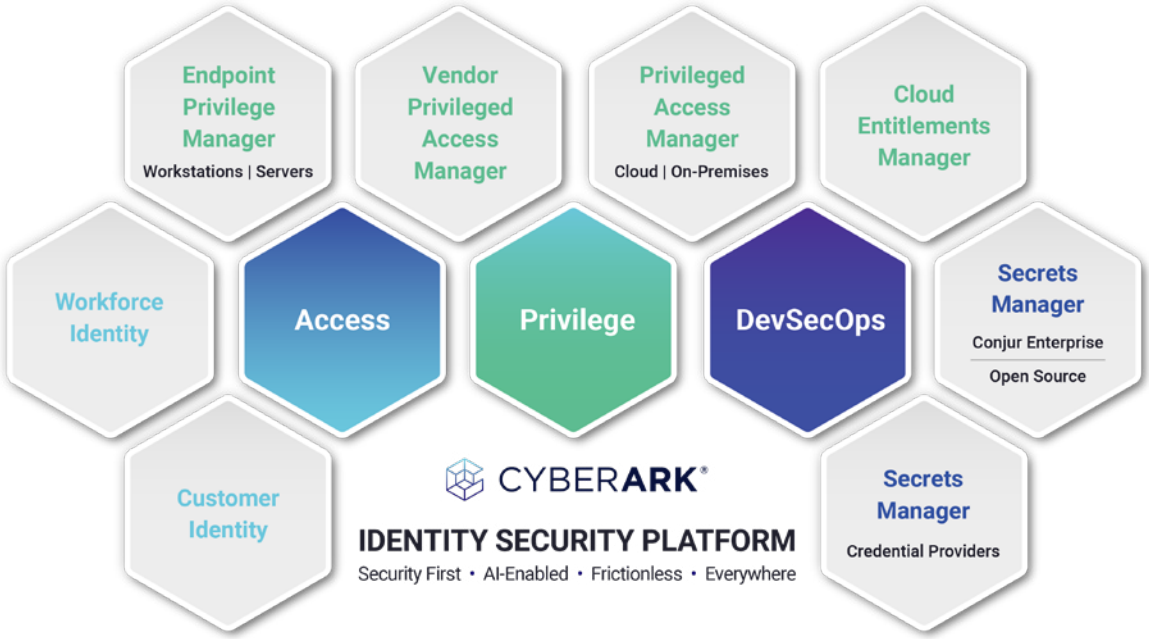
- Brand reputation
- Financial impact
- Alignment with industry standard risk frameworks and regulations
- Centralized visibility with full audit trail
- Reallocate staff to strategic priorities
- Continuous compliance

CyberArk's Identity Security Platform

Identity Security recognises that the nature of privilege is rapidly changing and expanding in a world where the number, the types, and the interrelationships of identities are exploding. This dynamic is creating whole new dimensions to the threat landscape that, improperly secured, can provide an attack path to an organization's most valuable assets.

Identity Security focuses on securing individual identities throughout the cycle of accessing critical assets. This means authenticating that identity accurately, authorising that identity with the proper permissions, and providing access for that identity to privileged assets in a structured manner -- all in a way that can be audited (or accounted for) to ensure the entire process is sound.

CyberArk's Identity Security Platform is built on the pillars of management for Access, Privilege, and DevSecOps to deliver authentication, authorisation, access, and audit in an integrated, seamless manner — ensuring security at every step in the Identity Security lifecycle. Our intelligent approach balances the need for better security with making end-users' access more productive. We do this by using real-time intelligence and analytics to create a context-based, adaptive approach to the Identity Security lifecycle. CyberArk does this for all identities, across all systems and apps, using any device.



CyberArk Privilege Access Manager (PAM)

Each solution within the CyberArk Identity Security Privilege Platform addresses a different requirement for securing privilege, and are all designed to work together to provide a complete, secure solution for operating systems, endpoints, cloud infrastructure and workloads, servers, databases, applications, hypervisors, network devices, security appliances, and more. The CyberArk PAM solutions span on-premises, cloud, industrial control systems (ICS) environments as well as the DevOps pipeline. The CyberArk Identity Security Platform components can be consumed Software as-a-Service, cloud, on-premises or hybrid.

The CyberArk PAM solution provides the following core capabilities within your organisation.

- Discover all of your privileged identities, accounts and credentials
- Protect and manage privileged credentials used by users and applications
- Control, secure and monitor privileged access to servers and databases, websites, SaaS applications and cloud consoles
- Provide Dynamic Privileged Access implementing time-bound just-in-time access and significantly reduces standing access to cloud and on-prem.
- Provide least privilege access on workstations and in the cloud for business users and IT administrators
- Control applications on endpoints and servers
- Use real-time privileged access intelligence to detect and respond to in-progress attacks

Learn more about CyberArk's Privilege Access Manager here.

Endpoint Privilege Manager

Endpoint Privilege Manager is designed to prevent attacks that originate on the endpoint by removing local administrative rights on the endpoint (Windows and Mac desktops/Servers and laptops). The solution allows for JIT elevation and access on a "by request" basis for a pre-defined period of time, with full audit of privileged activities. Full administrative rights or application-level access can be granted, with access being time limited and revoked as needed.

The solution reduces configuration drift on endpoints with minimal impact to the end user through the Application Control feature, enabling IT operations and security teams to allow approved applications to run, and restrict the ones that are not approved. These unknown applications can run in a 'Restricted Mode' which prevents them from accessing corporate resources, sensitive data or the Internet. These applications can be sent to Endpoint Privilege Manager's cloud-based Application Analysis Service, which in turn can integrate with data feeds from our technology partners , as well as other services for additional analysis. The solutions also provides Step-Up Authentication using Multi-Factor Authentication when accessing high risk applications and admin tasks.

Endpoint Privilege Manager helps organisations protect against threats that take advantage of unmanaged local admin access. The solution reduces security risk and configuration drift, while reducing help desk calls from end users.

Learn more about CyberArk's Endpoint Privilege Manager here.

Vendor Privilege Access Manager

CyberArk® Vendor Privileged Access Manager is a SaaS solution that combines Zero Trust access, biometric multi-factor authentication and Just-in-Time (JIT) provisioning to secure external vendors that require privileged access to critical internal resources. The solution enables security teams to provide external vendors with only the access they need. Vendor PAM fully integrates with the CyberArk Privileged Access Manager solution for full audit, session isolation and remediation capabilities. Vendor Privileged Access Manager is designed to provide fast, easy and secure privileged access to external vendors who need access to critical internal systems.

By not requiring VPNs, agents or passwords Vendor Privileged Access Manager removes operational overheard for administrators and makes organisations more secure.

- Integrates with CyberArk Privileged Access Manager to provide additional layer of security for critical systems
- Introduces a more secure solution than traditional token-based or VPN approaches
- Enables administrators to onboard external vendors Just-in-Time without the need to add them to Active Directory
- Removes operational overhead associated with managing VPNs, agents and passwords

Learn more about CyberArk's Vendor Privilege Access Manager here.

Cloud Entitlements Manager

The CyberArk Cloud Entitlements Manager is a SaaS solution that reduces risk by implementing Least Privilege across cloud environments. From a centralized dashboard, Cloud Entitlements Manager provides visibility and control of Identity and Access Management (IAM) permissions across an organization's cloud estate. Within this single display, Cloud Entitlements Manager leverages Artificial Intelligence to detect and remediate risky permissions, helping organisations strategically reduce risk without disrupting necessary access for cloud operations. Key benefits include:

- Gain cloud-agnostic visibility of permissions and act swiftly to reduce risk
- Implement Least Privilege for all human and machine identities throughout the cloud estate
- Operate cloud permissions securely and efficiently
- Proactively reduce risk and measure progress

Cloud Entitlements Manager requires no dedicated infrastructure and offers unprecedented time to value. Within an hour of registration, users can leverage intelligent recommendations to remediate excessive permissions across their AWS, AWS EKS, Azure, and GCP environments.

Learn more about CyberArk's Cloud Entitlements Manager here.

Access Management Solution

CyberArk Identity provides Workforce and Customer identity access is a SaaS-delivered suite of services designed to help organisations securely manage identity and access for their employees, partners, and customers. CyberArk Identity enables organisations to reduce the risk of weak or default passwords – the primary cause of security breaches.

CyberArk Identity suite includes all fundamental pillars of Identity and Access Management (IAM) – Single Sign-On (SSO), Adaptive Multi-Factor Authentication (MFA), Identity Lifecycle Management (LCM) and User Behaviour Analytics (UBA).

- **CyberArk Identity Single Sign-On:** CyberArk SSO is an easy-to-manage service for one-click access to your cloud, mobile, and legacy apps. CyberArk SSO enables a secure and frictionless sign-in experience for internal and external users that adjusts based on risk. Users simply sign in to a web portal using their existing corporate credentials to access all their assigned applications from one place.
- **CyberArk Identity Adaptive Multi-Factor Authentication:** CyberArk Adaptive MFA adds an extra layer of protection before access to corporate applications is granted. Leveraging device, network, and user behaviour context, CyberArk MFA intelligently assigns risk to each access event and allows you to create dynamic access policies that are triggered when anomalous behaviour is detected.

- **CyberArk Secure Web Sessions:** CyberArk Secure Web Sessions is a cloud-based service that gives customers the ability to record and monitor standard business users along with privilege user activity within web applications and cloud consoles protected by CyberArk Identity. With Secure Web Sessions, companies can record high risk web application user activities without relying on extensive app customisations, complicated integrations with 3rd party tools, or manual log reviews.
- **CyberArk Identity Lifecycle Management:** CyberArk LCM simplifies routing of application access requests, creation of application accounts, management of entitlements for those accounts, and revoking of access when necessary. With CyberArk LCM, you can enable users to request access to applications from the CyberArk Identity App catalogue, provide specific users the ability to approve or reject these access requests, and automatically create, update and deactivate accounts based on user roles.
- **CyberArk Identity User Behaviour Analytics:** CyberArk UBA enables you to determine the risk of every user and access request by collecting and analyse a rich set of contextual factors. Leveraging Machine Learning, User Behaviour Analytics engine builds user profiles that model standard behaviour and automatically flags anomalous activity. With UBA, you can generate access related insights, investigate security incidents, and define remediation actions when potential breach attempts are detected.

Learn more about CyberArk's Access Management Solution here.

DevSecOps Solution

CyberArk Secrets Manager enables organisations to centrally secure and manage, secrets and credentials used by the broadest range of applications, including internally developer applications, COTS, BOTS, automation platforms and CI/CD tools, running in hybrid, cloud-native and containerized environments. Mission critical applications running at scale can securely access high-value resources, including databases and IT infrastructure, to improve business agility while reducing operational complexity.

Loved by security teams and developers, Secrets Manager offers the most out-of-the-box integrations which helps developers simplify securing applications and DevOps environments. Secrets Manager provides organizations with a critical capability to help secure applications and tools across the software supply chain. Additionally, with the CyberArk Identity Security Platform organizations can consistently manage credentials used by human and non-human identities across the entire enterprise.

Secrets Manager is designed to provide a strong security solution that enables organizations to control, manage, and audit all nonhuman privileged access for the broadest range of application types, across the broadest range of environments.

- **For cloud-native applications built using DevOps methodologies:** Conjur Secrets Manager Enterprise provides a secrets management solution tailored specifically to the unique requirements of cloud native and DevOps environments. The solution integrates with a wide range of DevOps tools, PaaS/Container orchestration platforms, and supports hybrid and multi-cloud environments, including native integrations with Jenkins, Ansible, OpenShift, Kubernetes, AWS, Azure and GCP. The solution integrates with the CyberArk Identity Security Platform to provide a single enterprise-wide platform for securing privileged credentials. An open source, developer version is available at **www.conjur.org**.
- **For securing commercial off-the-shelf solutions (COTS):** Credential Providers can rotate and manage the credentials that third-party tools and solutions such as security tools, RPA, automation tools, IT management, etc. need to complete their jobs. For example, a vulnerability scanner typically needs high levels of privilege to

scan systems across the enterprise's infrastructure. Instead of storing privilege credentials in COTS solutions, they are managed by CyberArk. To simplify how an enterprise allows third party solutions to access privileged credentials, CyberArk offers the most validated out-of-the-box COTS integrations for solving identity security challenges.

- **For internally-developed traditional applications:** Credential Providers help protect high volume, mission critical applications, sensitive business data and simplify operations by eliminating hard-coded credentials from internally developed static applications. The solution provides a comprehensive set of features for managing application passwords and SSH keys, and supports a broad range of static application environments, including application servers, Java, .NET Core, and scripting running on a variety of platforms and operating systems including Unix/Linux, Windows and zOS.

Learn more about CyberArk's Secrets Management Solution here.

Meeting ACSC's Essential Eight Mitigation Strategies with CyberArk

The following table reviews five of the "Essential Eight" mitigation strategies recommended by the ACSC and shows how CyberArk's solutions can be used to address ACSC recommendations to achieve up to **Maturity Level Three**:

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. The solutions also provides Step-Up Authentication using Multi-Factor Authentication when accessing high risk applications and admin tasks.
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, local disk, memory, and system registry.
User application Hardening to block web browser access to Adobe Flash (uninstall if possible), web advertisement and untrusted java code on the internet. **Why:** Flash, java and web ads have long been popular ways to deliver malware to infect computers	**CyberArk Endpoint Privilege Manager** application policy can be defined to block the creation of child processes for applications such as PDF software, Microsoft applications, installers, scripts and more. The addition of the greylisting capability of applications can restrict execution of unknown applications as well as their ability to access the internet, local disk, memory, and system registry.

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.	**Privilege Access Management** solution provides organisations with the ability to automatically discover where privileged accounts exist on servers, workstations, network devices, virtual environments and cloud. 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. **Privileged Session Manager** 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. **Privileged Threat Analytics** provides intelligence-driven analytics that enable you to identify suspicious and malicious privileged user behaviour within your organisation. PTA distinguishes, in real-time, between normal and abnormal user behaviour, raising alerts when abnormal activity is detected. **Cloud Entitlements Manager** is a SaaS solution that reduces risk by implementing Least Privilege for all human and machine identities across cloud environments. From a centralised dashboard, Cloud Entitlements Manager provides visibility and control of Identity and Access Management (IAM) permissions across an organisation's cloud estate. Within this single display, Cloud Entitlements Manager leverages Artificial Intelligence to detect and remediate risky permissions. **Dynamic Privilege Access** provides time-bound just-in-time access and significantly reduces standing access to cloud and on-prem providing a Zero Trust architecture. **CyberArk Secure Web Sessions** provides the ability to record and monitor high risk activities from standard business users or privilege users within web applications and cloud consoles protected by CyberArk Identity.
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.	**Access Management Solution** is a SaaS-delivered suite of services designed to assist organisations securely manage identity and access in to privilege and non-privilege systems. The Identity suite provides all fundamental pillars of Identity and Access Management (IAM) – Single Sign-On (SSO), Adaptive Multi-Factor Authentication (MFA), Identity Lifecycle Management (LCM) and User Behaviour Analytics (UBA). **Vendor Privileged Access Manager** is a SaaS solution that combines Zero Trust access, biometric multi-factor authentication and Just-in-Time (JIT) provisioning to secure external vendors that require privileged access to critical internal resources. The solution enables security teams to provide external vendors with only the access they need. Vendor PAM fully integrates with the CyberArk Privileged Access Manager solution for full audit, session isolation 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 Defence 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

Learn more about CyberArk's Security Standards and Frameworks here.

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.

Next Steps

Learn more about how CyberArk can assist you in mitigating the Essential Eight controls. Contact a designated CyberArk sales representative now.

About CyberArk

CyberArk is the global leader in Identity Security. Centered on privileged access management, CyberArk provides the most comprehensive security offering for any identity — human or machine — across business applications, distributed workforces, hybrid cloud workloads and throughout the DevOps lifecycle. The world's leading organizations trust CyberArk to help secure their most critical assets. 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.

CYBERARK®