CYBERARK

DATA SHEET

CYBERARK APPLICATION ACCESS MANAGER™

The Challenge

Enterprises typically rely on both commercial and internally developed applications to run their businesses, and today enterprises are increasingly leveraging automated IT infrastructure and DevOps methodologies to increase business efficiency and accelerate innovation. Application and IT environments can vary significantly within the same organization. For example, some IT environments are largely static, while others, such as containerized environments, are highly dynamic. Regardless, each application, script, automation tool, and other non-human identity relies on some form of privileged credential to access other tools, applications, and data.

Privileged credentials pose a variety of challenges for IT security, operations, and compliance teams:

- **Non-human credentials are widespread** – they include embedded hard-coded credentials in business-critical applications including both internally developed and commercial off-the-shelf solutions (COTS), security software such as vulnerability scanners, application servers and IT management software, Robotic Process Automation (RPA) platforms, and the CI/CD (Continuous Integration/Continuous Deployment) tool chain.
- **Non-human credentials need to be managed** – in addition to eliminating hard-coded credentials in code and scripts, many of the same approaches and techniques used to protect privileged access by people can also be used. Examples of common approaches include strong authentication, least privilege, role-based access controls, credential rotation, management, and audit.
- **Automated processes are incredibly powerful** – they can access protected data, scale at unparalleled rates, leverage cloud resources, and execute business processes instantaneously to drive tremendous value. However, as well-publicized security breaches demonstrate, automated processes are susceptible to sophisticated cyberattacks, which can occur suddenly and spread rapidly. Businesses must protect privileged credentials assigned to non-human identities, to defend against attacks and mitigate risks.

Additionally, privileged access security credentials for non-human identities are typically assigned and managed by people such as IT and DevOps administrators. Consequently it is critical that their access privileges are also managed and secured consistently across the extended enterprise.

Key Benefits

For Security Teams

- Eliminate embedded application credentials and consistently manage and audit privileged access for applications across on-premises, hybrid and multi-cloud environments. Support an enterprise-wide centralized privileged access solution for human and non-human identities.

For Operations

- Improve IT operational efficiency by automating the management and rotation of application credentials for applications running at scale.

For Developers

- Simplify securing applications without impacting velocity. Use open source solutions to simplify and accelerate usage.

For Compliance and Audit

- Enforce internal and regulatory requirements for managing and monitoring application credentials. Generate detailed audit trails.

The Solution

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

- **For securing commercial off-the-shelf solutions** – Application Access Manager can be used to provide 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 commercial vulnerability scanner typically needs very high levels of privileged access across the enterprise's infrastructure to scan systems and make an assessment. Application Access Manager enables organizations to avoid the need to store privilege credentials, passwords, keys, etc., within COTS solutions, and instead easily and securely use the required credentials from the CyberArk Vault. To make third party integrations easier CyberArk offers the widest eco-system of validated COTS integrations for securing privileged access.

- **For internally-developed traditional applications** – Application Access Manager can be used to protect business-system data and simplify operations by eliminating hard-coded credentials from internally developed applications and scripts. The solution helps protect against unauthorized privileged account access and mitigate risks, providing a comprehensive set of features for managing application passwords and SSH keys. The solution supports a broad range of application environments and platforms, including application servers, Java, .Net, scripting running on a variety of platforms and operating systems including Unix/Linux, Windows and zOS.
- **For cloud-native applications built using DevOps methodologies** – Application Access Manager provides a secrets management solution tailored specifically to the unique requirements of native-cloud and DevOps environments. The solution manages secrets and credentials used by non-human identities including DevOps and PaaS tools, and containers. The solution integrates with a wide range of DevOps tools such as Ansible, Jenkins, Puppet; PaaS/Container orchestration platforms such as Red Hat OpenShift, Pivotal Cloud Foundry, and Kubernetes, whether running on-premises, hybrid or on multiple cloud platforms. The solution also integrates with CyberArk's Enterprise Password Vault to provide a single enterprise-wide platform for securing privileged access.

  To better meet the needs of the developer community an open source version of Application Access Manager is available as Conjur Open Source at www.conjur.org.

Application Access Manager provides robust enterprise-grade capabilities designed to meet the enterprise's stringent performance and availability requirements. It also integrates with existing Active Directory, LDAP, and SIEM systems, helping organizations protect and extend previous investments, and preserve established security models and practices.

Capabilities

Application Access Manager is designed to provide a strong security solution that enables organizations to control, manage, and audit all non-human privileged access for applications, across on-premises, hybrid, containerized and multi cloud environments. The solution helps organizations:

- **Establish strong authentication** – by leveraging the native attributes of applications, containers, and other non-human identities to eliminate the "secret zero bootstrapping" challenge and potential vulnerability.
- **Simplify integrations** – by supporting validated integrations with a wide range of commercial software platforms, applications and tools, such as business applications, security tools, RPA platforms, CI/CD toolsets, and container platforms.
- **Accelerate deployment and usage** – by providing developers with an easy-to-use solution to secure secrets in application and DevOps environments – allowing them to focus on developing software. Additionally, the open source solutions make it easy for developers and DevOps admins to evaluate, deploy, and secure their DevOps environments.
- **Ensure a comprehensive audit on any access** – by tracking all access and providing tamper-resistant audit.
- **Consistently apply access policies** – by applying role-based access controls on non-human identities, leveraging integrations with other CyberArk and partner solutions to centralize policy management across the enterprise, and other policy-based controls.
- **Ensure business continuity and other enterprise requirements** – including scalability, availability, redundancy and resiliency, alerting, policy-based rotation, and other enterprise requirements.

Overview

COTS Application Integrations

- Security Software: Vulnerability Management, Discovery Solutions, etc.
- IT Management Software
- Robot Process Automation and other Automation Solutions

Application Servers:

- IBM WebSphere Application Server, WebSphere Liberty
- JBoss
- Oracle WebLogic Server
- Tomcat
- Wildfly

Cloud native and DevOps Integrations:

- Tools/Toolchains: Ansible, Jenkins, Puppet, Terraform
- PaaS/Container Orchestration: Kubernetes, Red Hat OpenShift, Pivotal Cloud Foundry
- DevOps Security: Aqua, Twistlock

Enterprise grade:

- Active Directory and LDAP
- Hardware Security Module (HSM) integration
- Security Information and Event Management (SIEM) Tools
- AES-256, RSA-2048

SDK and Development Libraries:

- DevOps: Go, Java, Ruby, Python
- Application SDK: C/C++, CLI, Java, .NET, Web Service/REST

CyberArk Privileged Access Security Solution

CyberArk Application Access Manager is part of the CyberArk Privileged Access Security Solution, a comprehensive solution to protect, monitor, detect, alert, and manage privileged accounts and other credentials for both human and non-human users and identities. Elements in the solution can be deployed independently, or combined to form a cohesive, end-to-end privileged access solution that delivers enterprise-class privileged access security across on-premises, hybrid, multi-cloud, PaaS, and DevOps environments. The comprehensive solution helps businesses significantly reduce attack surfaces by applying consistent privileged access security policies to human and non-human users and identities across the extended enterprise.