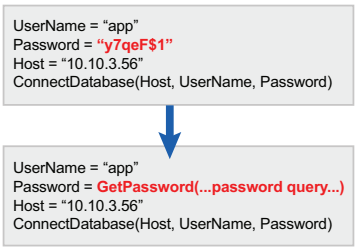
Application Identity Manager™

Fully address the security challenges of eliminating hard-coded application and script credentials across your data center and application infrastructure.



CyberArk Application Identity Manager enables organizations to protect data residing in business systems by eliminating hard-coded credentials from application scripts, configuration files and software code.

The Challenge

In today's complex IT environments, multiple scripts, processes and applications need to access multi-platform resources to retrieve and store sensitive information. Such applications are granted use of dedicated accounts, usually allowing unlimited access to an enterprise's most sensitive assets. As a result, these accounts are often the victim of ongoing targeted attacks. Indeed, many of the recent sophisticated attacks reported stemmed from the compromise of hard-coded privileged credentials.

Securing, managing and automatically replacing these embedded and locally stored credentials can impose significant challenges and overhead costs to IT departments. Consequently, many organizations never change hard-coded, embedded passwords or locally stored SSH keys for applications, leaving the organization vulnerable to an attack.

Unmanaged embedded privileged credentials and SSH keys pose great risk to an organization including:

- External and Internal Attack. Application passwords are almost never changed, often stored in clear text and known by a wide variety of IT personnel, external developers and sub-contractors, and even ex-employees. Because these accounts provide access to back end systems, a compromised application credential may lead to uncontrolled access to highly-sensitive business information.
- Failed Audits. Privileged credentials have increasingly gained attention from information security regulations and standards. Today, most regulations include controls around the use of hard-coded and embedded application credentials.
- Downtime. Critical applications require high availability to ensure business continuity. Manual management of application credentials can result in periodic downtime to a critical business application which is simply not an option since this can result in loss of business and costly outages.

The Solution

To mitigate these risks, organizations can rotate hard-coded credentials, e.g. within configuration files, with CyberArk Enterprise Password Vault which is a good first step toward protecting application credentials. However, best practices for securing application credentials recommend eliminating hard-coded credentials altogether.

CyberArk Application Identity Manager enables organizations to protect data residing in business systems by eliminating hard-coded credential from application scripts, configuration files and software code. Moreover, the solution can be used to store and rotate credentials used by applications to authenticate to target systems, thereby reducing the risk of unauthorized use.

CyberArk Application Identity Manager utilizes CyberArk's patented Digital Vault Technology® designed to meet the highest security requirements for securing privileged and application credentials. Application Identity Manager delivers a comprehensive set of features for managing application passwords and SSH keys, including:

- Eliminate Hard-Coded Passwords Organizations can remove static credentials from all scripts, application code and configuration files, making them invisible to developers and support staff.
- Securely Store and Rotate Applications Credentials. The CyberArk Digital Vault Technology® is used to store and rotate application credentials and provide numerous underlying security capabilities for authentication, encryption, and data protection. Application passwords and SSH keys can be automatically rotated based on policy without impact to application performance or downtime.

- Authenticate Applications. Application Identity Manager utilizes advanced means to authenticate applications requesting credentials based on application characteristics such as path, hash (signature), OS user and more, ensuring only authorized applications can access required credentials.
- Secure Local Cache of Credentials. Ensure the highest availability and performance, independent of network availability, for business critical applications to maintain business continuity.
- Support for Multiple Platforms. Application Identity Manager is a flexible solution that is designed to support large enterprise environments in which various platforms are being used.

Application Identity Manager Deployment Options

Organizations typically have a variety of applications ranging from mission-critical such as consumer-facing web applications to less critical such as desktop applications. Application Identity Manager is a flexible solution that is designed to meet the range of business applications with a variety of deployment options to best match each business application with the appropriate application security. The deployment options include:

Credential Provider is recommended for mission-critical business applications that are highly sensitive, and require the highest security without sacrificing performance and availability. The Credential Provider deployment includes an agent that resides on the application server and communicates via an API to retrieve secured credentials from the CyberArk Vault upon request. The agent also stores a secure local cache which is designed to ensure that applications will always have secure access to their service accounts, in- dependent of network availability or performance.

Application Server Credential Provider is a solution for securing and managing data source credentials in Application Servers including IBM WebSphere, Oracle Weblogic, JBoss, Tomcat. The integration involves a one-time configuration and does not require code changes in the application. Data source credentials can be changed based on the enterprise policy, without any downtime to applications, ensuring business continuity.

Central Credential Provider is an agentless de- ployment that is recommended for deployments of non-critical applications. In this deployment, no agent is required on the endpoint; instead, an agent is installed in a central location which serves multiple applications and allows them to communicate via a web service call to retrieve secured credentials from the CyberArk Vault upon request. The Central Credential Provider manages a secure cache of credentials to reduce load from the Vault, and provides improved performance for calling applications. It can be installed in multiple network zones, close to calling applications, and can be load balanced. Because this deployment requires no installation or management on servers or endpoints, it is a good fit for cloud service solutions and desktop applications.

Conclusion

Application Identity Manager enables organizations to:

Mitigate Internal and External Threats. Ensure critical business systems with the most sensitive data are tightly protected by eliminating hard- coded application passwords found in applications, scripts and configuration files, and removing SSH keys from servers, where they are used by applications and scripts.

Meet Audit and Compliance Requirements. Comply with internal and regulatory requirements for regularly replacing passwords and SSH keys and securely monitoring privileged access.

Ensure Business Continuity. Secure core business systems with high availability and performance, independent of network availability, to reduce the risk of downtime to applications.

CyberArk Application Identity Manager is a component of the CyberArk Privileged Account Security Solution, a complete solution to protect, monitor, detect, alert, and respond to privileged accounts. Products in the solution can be managed independently, or combined for a cohesive and complete solution for operating systems, databases, applications, hypervisors, network devices, security appliances and more. The solution is based on the CyberArk Shared Technology Platform which delivers enterprise- class security and allows customers to deploy a single infrastructure and expand the solution to meet changing business requirements.

Specifications

Encryption Algorithms:
- AES-256, RSA-2048
- HSM integration
- FIPS 140-2 validated cryptography

High Availability:
- Clustering support
- Persistent secure local cache
- Multiple Disaster Recovery sites
- Integration with enterprise backup system

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

Application Platforms:
- AIX
- Docker (RHEL, Centos, SLES)
- Linux/Unix (RHEL, SUSE, Ubuntu, Oracle Linux, CentOS, Fedora)
- Mac OS X
- Solaris
- Windows
- z/OS

Application SDK:
- C/C++
- CLI
- COM
- Java
- .NET
- Web Service