CYBERARK

產品簡介

CYBERARK 應用程式存取管理器 ™

挑戰

通常，企業依賴商用及內部開發的應用程式展開業務運營，如今，企業日益增加地利用自動化 IT 基礎架構及 DevOps 方法來提高經營效率並加速創新。即使在同一企業內部，應用程式及 IT 環境也可能存在巨大差異。例如，一些 IT 環境基本上保持靜態，而其他環境（如容器化環境）卻始終在不斷變化。儘管如此，每個應用程式、腳本、自動化工具及其他非人類身份皆依賴某種形式的特權憑證來存取其他工具、應用程式及資料。

特權憑證使 IT 資安、營運及內稽團隊面臨許多挑戰：

- 廣泛使用非人類憑證 — 非人類憑證包括關鍵業務應用程式 [包括內部開發及商用現成解決方案（COTS）]、資安軟體（如弱掃軟體）、應用程式伺服器及 IT 管理軟體、機器人流程自動化（RPA）平台以及 CI/CD（連續整合 / 連續部署）工具鏈中的嵌入式寫死的帳密憑證。
- 需要管理非人類憑證 — 除了消除程式碼及腳本中寫死的帳密憑證以外，還可以使用許多相同的方法及技術來保護人類的特權存取。一些常用的方法包括嚴格身份驗證，最小授權，基於角色的存取控制，密碼憑證更替、管理及稽核。
- 自動化處理程序異常強大— 自動化處理程序可以存取受保護的資料，以前所未有的速度進行擴展，利用雲端資源，並快速執行業務程序來創造巨大的價值。但是，一些廣為人知的資安事件表明，自動化處理程序易於受到複雜的網路攻擊，而且網路攻擊可能會突然發生並快速擴散。企業必須保護分配給非人類身份的特權憑證，以防範攻擊並降低風險。

此外，非人類身份的特權存取安全憑證通常由 IT 及 DevOps 管理員等人員進行分配及管理。因此，至關重要的是，還必須在整個擴展型企業內一致地管理及保護他們的存取特權。

主要優勢

對於資安團隊

- 消除嵌入式應用程式帳密憑證，並一致地管理及稽核本地、混合雲端及多雲端環境中應用程式的特權存取。針對人類及非人類身份，支援全企業集中式特權存取解決方案。

對於運營

- 對於大規模運行的應用程式，自動管理及更替應用程式中的密碼及憑證，進而提高 IT 運營效率。

對於開發人員

- 簡化應用程式安全保護，而不會影響速度。利用開放原始碼解決方案來簡化及加速使用。

對於合規與稽核

- 強制實施內部及監管要求，管理及監視應用程式憑證。產生詳細的稽核記錄。

解決方案

CyberArk 應用程式存取管理器（Application Access Manager）旨在提供全面的特權存取、帳密憑證及秘密資訊管理，適用於廣泛使用的各種應用程式及非人類身份。例如，應用程式存取管理器可保護商用現成應用程式、內部開發的傳統應用程式、腳本以及使用 DevOps 方法建構的容器化應用程式所需的憑證。

- 對於保護商用現成解決方案 — 應用程式存取管理器可用於資安工具、RPA、自動化工具、IT 管理等協力廠商工具及解決方案，提供完成其作業所需的帳密憑證並管理這些帳密憑證。例如，商用弱掃工具通常需要在擁有整個企業基礎架構內極高級別的特權存取權限，以掃描系統並進行評估。使用應用程式存取管理器，企業無需在 COTS 解決方案中儲存特權憑證、密碼、金鑰等，而可以輕鬆安全地從 CyberArk 金庫中獲取所需憑證。為了進一步簡化整合，CyberArk 提供最廣泛的已驗證 COTS 整合生態系統來保護特權存取的安全。

- 對於內部開發的傳統應用程式 — 應用程式存取管理器可用於保護業務系統中的資料，並消除內部開發的應用程式及腳本中寫死的憑證來簡化運營。此解決方案提供全方位功能特性來管理應用程式密碼及 SSH 金鑰，可協助阻止未授權特權帳戶存取並降低風險。此解決方案支援一系列應用程式環境及平台，包括應用程式伺服器、Java、.Net、在各種平台及作業系統（包括 Unix/Linux、Windows 及 zOS）上運行的腳本。
- 對於使用 DevOps 方法建構的雲端原生應用程式 — 應用程式存取管理器提供專門量身訂製的秘密資訊管理解決方案來滿足雲端原生及 DevOps 環境的獨特需求。此解決方案整合一系列 DevOps 工具（如 Ansible、Jenkins、Puppet）及 PaaS/ 容器協調流程平台（如 Red Hat OpenShift、Pivotal Cloud Foundry 及 Kubernetes），而不論是在本地、混合還是多雲端環境中運行。此外，此解決方案還整合 CyberArk 企業密碼金庫，可提供單一企業範圍平台來保護特權存取的安全。

  為了更好地滿足開發人員社群的需求，我們還以 Conjur Open Source 的形式提供應用程式存取管理器的開放原始碼版本，請瀏覽 www.conjur.org。

應用程式存取管理器提供可靠的企業級功能，旨在滿足企業嚴格的性能及可用性要求。應用程式存取管理器還可以整合現有的 Active Directory、LDAP 及 SIEM 系統，協助企業保護並繼續利用原來的投資，同時保留既有的安全模式及實踐。

功能

應用程式存取管理器旨在提供強大的安全解決方案，協助企業控制、管理並稽核本地、混合、容器化及多雲端環境中的應用程式所需的所有非人類特權存取。此解決方案可協助企業：

- 建立嚴格的身份驗證 — 利用應用程式、容器及其他非人類身份的原生屬性應對「秘密資訊零引導」（secret zero bootstrapping）挑戰並消除潛在的漏洞。
- 簡化整合 — 通過驗證，支援整合一系列商用軟體平台、應用程式及工具，如業務應用程式、資安工具、RPA 平台、CI/CD 工具集及容器平台。
- 加速開發及使用 — 為開發人員提供易於使用的解決方案來保護應用程式及 DevOps 環境中的秘密資訊，讓開發人員集中精力開發軟體。此外，利用開放原始碼解決方案及元件（包括無秘密資訊代理（Secretless Broker）），開發人員可以輕鬆評估、部署 DevOps 環境並確保其安全。
- 確保可全面稽核任何存取 — 追蹤所有存取並提供防篡改稽核記錄。
- 一致性的應用存取原則 — 對非人類身份應用基於角色的存取控制，利用與其他 CyberArk 及合作夥伴解決方案的整合，在整個企業內部進行集中化原則管理，並實施其他基於原則的控制。
- 確保業務連續性並滿足其他企業要求 — 包括延展性、可用性、冗餘及彈性。

概述

COTS 應用程式整合

- 安全軟體：漏洞管理、弱點掃描解決方案等
- IT 管理軟體
- 機器人流程自動化及其他自動化解決方案

應用程式伺服器：

- IBM WebSphere 應用程式伺服器、WebSphere Liberty
- JBoss
- Oracle WebLogic Server
- Tomcat
- Wildfly

雲端原生和 DevOps 整合：

- 工具 / 工具鏈：Ansible、Jenkins、Puppet、Terraform
- PaaS/ 容器協調流程：Kubernetes、Red Hat OpenShift、Pivotal Cloud Foundry
- 無秘密資訊代理（Secretless Broker）：Red Hat OpenShift、Kubernetes
- 容器安全性：Aqua、Twistlock

企業級：

- Active Directory 和 LDAP
- 硬體安全模組（HSM）整合
- 安全資訊及事件管理（SIEM）工具
- AES-256，RSA-2048

SDK 及開發庫：

- DevOps：Go、Java、Ruby、.NET
- 應用程式 SDK：C/C++、CLI、Java、.NET、Web 服務 /REST

CyberArk 特權存取安全解決方案

CyberArk 應用程式存取管理器是 CyberArk 特權存取安全解決方案的一部分，CyberArk 特權存取安全解決方案提供全方位解決方案來保護、監控、偵測、告警並管理人類及非人類使用者及身份所需的特權帳戶及其他憑證。該解決方案的各個元件可以獨立部署，也可以組合在一起而構成整體式端對端特權存取解決方案，在本地、混合、多雲端、PaaS 及 DevOps 環境中交付企業級特權存取安全性。此全方位解決方案可對擴展型企業中的人類及非人類使用者及身份應用一致的特權存取安全性原則，協助企業顯著減小攻擊面。