CyberArk 應用程式身份管理器

移除資料中心與應用程式基礎架構中應用程式與腳本寫死的憑證或帳密，全面化解資安挑戰。

```
使用者名稱 = "app"
密碼 = "y7qeF$1"
主機 = "10.10.3.56"
ConnectDatabase（主機、使用者名稱、密碼）
```

```
使用者名稱 = "app"
密碼 = GetPassword(...password query...)
主機 = "10.10.3.56"
ConnectDatabase（主機、使用者名稱、密碼）
```

CyberArk 應用程式身份管理器讓企業可以移除應用程式腳本、設定檔及軟體程式碼中的寫死的憑證或帳密，進而保護業務系統中的資料。

挑戰

在當前複雜的 IT 環境中，多種腳本、流程與應用程式需要存取多平台資源來檢索與保存敏感資訊。這些應用程式有權使用專用帳號，通常可以無限制地存取企業最敏感的資產。因此，這些帳號經常成為具針對性持久攻擊的目標。確實，最近報導的很多複雜攻擊最初皆是從攻擊者獲取寫死的特權憑證或帳密開始。

保護、管理與自動更換這些嵌入式與本地保存的憑證或帳密，使 IT 部門面臨嚴峻挑戰而且成本很高。因此，很多企業從來不修改應用程式中寫死的嵌入式密碼或本地端保存的 SSH 金鑰，使企業面對攻擊不堪一擊。

不受管理的嵌入式特權憑證或帳密與 SSH 金鑰會為企業帶來很大的風險，包括：

- **外部與內部攻擊**。應用程式密碼幾乎從不修改，通常以純文字形式保存而且被很多 IT 人員、外部開發人員與下包商，甚至是已經離職的員工所知。由於這些帳號可存取後端系統，因此洩露的應用程式憑證或帳密可能會使攻擊者以不受控制的方式隨意存取高度敏感的企業資訊。
- **無法稽核**。特權憑證或帳密越來越受到資安監管與標準機構的關注。今天，大多數監管條例皆制定如何控制對寫死的與嵌入式應用程式憑證或帳密的使用方面的規定。
- **停機**。關鍵應用程式要求高可用性以確保業務連續性。手動管理應用程式憑證或帳密，會導致關鍵業務應用程式的定期停機；這是無法接受的，因為這可能會導致業務損失與成本昂貴的故障停機。

解決方案

為了緩解這些風險，企業可以使用 CyberArk 企業密碼金庫 (Enterprise Password Vault) 來輪換寫死的憑證或帳密，如設定檔中的憑證或帳密。CyberArk 企業密碼金庫是保護應用程式憑證或帳密的理想解決方案。然而，保護應用程式憑證或帳密的最佳實踐建議是徹底消除寫死的憑證或帳密。

CyberArk 應用程式身份管理器有助於企業從應用程式腳本、設定檔及軟體程式碼中移除寫死的憑證或帳密，進而保護保存在業務系統中的資料。此外，CyberArk 解決方案可用於保存與輪換應用程式向目標系統進行身份驗證所使用的憑證或帳密，進而降低未經授權使用風險。

CyberArk 應用程式身份管理器利用 CyberArk 獲得專利的數位金庫技術，設計用於滿足保護特權憑證或帳密與應用程式憑證或帳密方面的最高要求。應用程式身份管理器提供完整的功能來管理應用程式密碼與 SSH 金鑰，包括：

- **移除寫死的密碼**。企業可以從所有腳本、應用程式原始碼及設定檔中移除靜態的憑證或帳密，使開發人員與技術支援人員無法看到憑證或帳密。
- **安全保存與輪換應用程式憑證或帳密**。CyberArk 數位金庫技術被用於保存與輪換應用程式憑證或帳密，並提供多種身份驗證、加密與資料保護方面的必要資安功能。應用程式密碼與 SSH 金鑰可以根據原則自動進行輪換而不影響應用程式性能或造成停機。
- **對應用程式進行身份驗證**。應用程式身份管理器利用先進的方法，根據路徑、雜湊（簽名）、OS 使用者等應用程式特徵來對請求憑證或帳密的應用程式進行身份驗證，確保僅有獲得授權的應用程式可以存取所需的憑證或帳密。
- **安全的本地端帳密快取**。確保最高的可用性與性能，而不受網路可用性影響，可以確保關鍵任務應用程式的業務連續性。
- **支援多種平台**。應用程式身份管理器是靈活的解決方案，設計用於支援使用多種不同平台的大型企業環境。

1 Gartner 新聞《Gartner 稱企業尚未為 2018 年歐洲資料保護條例做好準備》，http://www.gartner.com/newsroom/id/3701117

應用程式身份管理器部署選項

企業一般有多種不同應用程式：從關鍵任務應用程式（如客戶使用的 Web 應用程式）一直到不太重要的應用程式（如桌面應用程式）。應用程式身份管理器是靈活的解決方案，設計用於透過多種部署選項來支援各種業務應用程式，為每種業務應用程式提供適當的應用程式安全性。部署選項包括：

Credential Provider (CP)：對於高度敏感、要求最高安全性而不降低性能與可用性的關鍵任務業務應用程式，推薦使用 Credential Provider。CP 部署包含一個代理程式（agent）。該代理程式位於應用程式的主機上，並透過 API 通信來根據要求從 CyberArk 金庫中獲取安全的憑證或帳密。該代理程式還包含一個安全的本地端快取，可確保應用程式始終能夠安全存取自己的服務帳號，而不受網路可用性影響或影響性能。

Application Server Credential Provider (ASCP)：ASCP 是用於應用程式伺服器（包括 IBM WebSphere、Oracle Weblogic、JBoss 與 Tomcat）中保護與管理 Data Source 帳密的解決方案。 這種整合包括一次性組態設定，而不要求在應用程式中進行程式碼修改。Data Source 帳密可以根據企業原則進行定期更換，而不需要應用程式停機，因此可以確保業務連續性。

Central Credential Provider (CCP)：CCP 是一種無代理程式的部署，推薦用於部署非關鍵應用程式。在這種部署中，終端設備上不需要安裝代理程式；而是將一個代理程式安裝在集中位置上，為多種應用程式提供服務，使應用程式可以透過 Web Service 通信，來依據要求從 CyberArk 金庫中安全地獲取憑證或帳密。CCP 負責對憑證或帳密的資安快取，以減輕金庫的負載，並為應用程式提供更高的性能。CCP 可以安裝在靠近應用程式的多個網路區段中，而且可以實現負載平衡。由於這種部署不要求在伺服器或終端設備上進行安裝與管理，因此非常適合雲端服務解決方案與桌面應用程式。

DevOps 環境

CyberArk 提供專門設計用於支援高度動態的高性能 DevOps 環境及 CI/CD 流程的 CyberArk Conjur。CyberArk Conjur 有企業與社群 (開放原始碼) 兩種版本。

總結

應用程式身份管理器使企業可以：

緩解內部與外部威脅。從應用程式、腳本與設定檔中移除寫死的應用程式帳密，從伺服器中移除 SSH 金鑰（應用程式與腳本在伺服器中使用 SSH 金鑰），進而確保包含最敏感性資料的關鍵企業系統可受到嚴格保護。

達到稽核與合規性要求。達到定期更換密碼與 SSH 金鑰的內部與監管要求，監控特權存取。

確保業務連續性。保護核心業務系統，確保高可用性與性能而不受網路可用性影響，以降低應用程式停機風險。

CyberArk 應用程式身份管理器是 CyberArk 特權帳號安全解決方案的組件。CyberArk 特權帳號安全解決方案是一款全方位解決方案，可以保護、監控、偵測特權帳號，發出告警並做出回應。CyberArk 特權帳號解決方案包含可以獨立或組合管理的各種產品，有助於打造適用於不同作業系統、資料庫、應用程式、系統管理程式、網路設備及資安設備等的連貫、全方位解決方案。CyberArk 特權帳號解決方案基於 CyberArk 共用技術平台（Shared Technology Platform）。該平台可以達到企業級的安全性，允許客戶部署一套基礎架構，然後擴展該解決方案以滿足不斷變化的業務要求。

規格

加密演算法：
- AES-256，RSA-2048
- HSM 整合
- 符合 FIPS 140-2 的加密技術

高可用性：
- 叢集支援
- 持久性本地端安全的快取
- 多個災難備援副本
- 整合企業備份系統

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

應用程式平台：
- AIX
- Docker（RHEL、Centos 與 SLES）
- Linux/Unix（RHEL、SUSE、Ubuntu、Oracle

Linux、CentOS、Fedora
- Mac OS X
- Solaris
- Windows
- z/OS

應用程式 SDK：
- C/C++
- CLI
- COM
- Java
- .NET
- Web Service