CYBERARK ALERO

挑戰

目前，很多企業依賴遠端廠商來管理其 IT 基礎架構的某些部分。為了成功完成任務，這些外部服務機構自然需要企業 IT 系統的特權存取。然而，在使用傳統使用者身份驗證及授權方法時，將企業特權存取安全解決方案落實及擴展到外部廠商是一項極具挑戰性的工作。

傳統的企業身份識別管理系統及存取控制解決方案主要設計用於對公司員工及公司設備進行身份驗證，並不是特別適合保護當今環境中的協力廠商人員及外部設備。大多數企業對於企業網路中遠端存取操作的可視性及管控微乎其微甚至為零。由於多種原因，為每個廠商提供公司專用的工作站顯然不是可行的方法，而在其它公司的筆記型電腦或桌上型電腦上部署 VPN 或代理程式（agent），通常會導致 IT 團隊疲於管理。此外，協力廠商人員及存取要求也可能會每天或每週發生變化，使基於使用者 ID 及密碼的傳統身份識別管理機制無所適從。

隨著企業邊界的消失及對外包商操作的依賴性日益增加，企業 IT 維運及資安團隊都需要找到創新的途徑，允許外部廠商遠端安全地存取特權帳號而不中斷維運。

安全且快速地連接負責管理貴公司 IT 資產的外部廠商——而不需要 VPN、代理程式或密碼

規格

- CyberArk Alero 組成部分
  - Alero 行動應用程式（Alero Mobile App）
  - Alero 連接器（Alero Connector）
  - Alero 雲端（Alero Cloud）
  - iOS 10 或更高版
  - Android 6 或更高版
- CyberArk 組成部分
  - Core PAS v10.3 或更高版
  - HTML5 閘道

解決方案

有些外部廠商需要存取受 CyberArk 管理的關鍵內部系統；CyberArk Alero 專門設計用於為外部廠商提供快速、簡便且安全的遠端特權存取。Alero 是提供基於雲端的多因子身份驗證，利用智慧手機的生物識別功能，使經過授權的外部廠商只需一瞥或輕觸手指就可以獲得及時、安全的特權存取。

Alero 徹底告別讓使用者沮喪、增加風險且引發管理問題的 VPN 客戶端、安全代理程式或密碼。相反的，外部廠商可以使用智慧手機本身的臉部或指紋識別功能來進行身份驗證，然後就可以通過身份驗證並獲得授權，經由 Alero 安全地存取 CyberArk 核心特權存取安全解決方案。Alero 在一套 SaaS 解決方案中整合 Zero-Trust 存取、生物特徵多因子身份驗證及即時佈建（just-in-time provisioning）技術，而且可全面整合 CyberArk 核心特權存取安全解決方案，為管理者提供全面的可視性及稽核功能。

如何開始

Alero 行動應用程式可在 iOS 和 Android 手機上執行, 當應用程式下載完畢後，外部廠商會收到一份發自公司要求存取 Alero 網站的電子郵件。外部廠商輸入簡訊中的密碼，繼而驗證電子郵件地址及所註冊的手機來確認其身份識別。

此外還使用生物特徵授權來對使用者身份進行驗證及識別，而且可在啟動過程中強制要求執行此操作以確保首次登入成功。生物特徵資料安全地保存在使用者的行動設備中。用戶端使用託管的 Alero 控制台來管理外部廠商帳號並進行活動稽核。

為何選擇 CYBERARK？

CyberArk 是特權存取資安領域的全球領導者——特權存取安全是保護整個企業、雲端及 DevOps Pipeline 內資料、基礎架構及資產的 IT 安全性的關鍵層。

CyberArk 提供業界最方位解決方案，可降低特權憑證及安全憑證引起的資安風險。

公司深得全世界領先企業的信賴，包括 50% 以上的財經 500 大公司。這些公司利用 CyberArk 產品來防止外部攻擊者及內部惡意使用者所發起的攻擊。

工作原理

當外部廠商嘗試登入 CyberArk 的 Web 入口網站時，Alero 會在其工作站上顯示短時間內有效的一次性 QR 碼。利用 Alero 行動應用程式，使用者可以掃描這個 QR 碼，同時藉由臉部或指紋識別來進行身份驗證。如果 QR 碼及生物特徵資料都通過驗證，遠端使用者就可以安全地從自己的工作站登入 CyberArk Web 入口網站，並獲得授權來存取特權帳號。Web 瀏覽器的連線是被隔離的，在終端使用者進入關鍵IT系統以完成常規工作、維護或其它操作時，特權憑證絕對不會與其工作站共用，且連線已受到端到端加密保護。

CyberArk 核心特權存取安全解決方案可幫助企業高效率管理特權帳號存取權限、積極主動地監控特權帳號活動、智慧地識別可疑活動並以自動方式快速應對資安威脅，進而降低資安風險。Alero 可以無縫地整合 CyberArk 核心特權存取安全解決方案，為外部廠商提供即時佈建及存取功能，確保關鍵資產只在必要時才能存取。這種整合還可以為企業運營及資安團隊提供對外部廠商特權存取活動的全面可視性及管控。

客戶效益

- **降低資安風險：**為連接到 CyberArk Core PAS 的外部廠商實施零信任存取，提高總體安全性，且對特權帳號用戶進行即時佈建，同時避免使用基於密碼、權杖及網路的存取控制方法，以防止造成漏洞並擴大攻擊面的。
- **降低運營支出及複雜性：**SaaS 解決方案不使用外部廠商存取所需的 VPN、代理程式及憑證，所以可簡化操作，即時進行遠端使用者臨時授權而無需管理者介入，不再需要存取時根據政策來新增刪除使用者。
- **簡化協力廠商的遠端存取。**使經授權的使用者只需一瞥或輕觸手指就可以通過身份驗證，安全地進行特權連線。在行動設備中所保存生物特徵資料，與內部系統隔離，確保最高的隱私性及安全性。
- **增強可視性及監管合規性：**全面整合 CyberArk 核心特權存取安全解決方案，經由隔離的瀏覽器連線來即時監控特權存取活動，偵測正在進行的及潛在的攻擊，防止攻擊者進入關鍵系統並造成無法挽回的損失，同時可產生相關報表，以支援合規性稽核。

©Cyber-Ark Software 有限公司版權所有。保留所有權利。未經 CyberArk Software 公司明確書面許可，不得以任何形式或透過任何方式複製本文的任何部分。CyberArk®、CyberArk 商標以及文中出現的其它商標或服務名稱為 CyberArk Software 公司在美國及其它國家的註冊商標（或商標）。任何其它商標及服務名稱為各自所有者的財產。U.S., 06.19.Doc.365221890

CyberArk 相信本文所包含資訊在發佈之日的準確性。對於本文所包含的資訊，CyberArk 不做任何明確、法定或隱含的保證，而且可能會有修改，恕不另行通知。