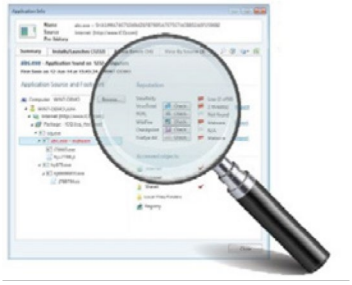
CYBERARK

產品簡介

終端特權管理器

在桌上型電腦、筆記型電腦及伺服器上強制實施特權安全保護措施，同時避免撤銷本機管理者權限（曾使 IT 技術支援不堪重負）的負面影響。



從一個位置上集中查看所有特權原則、應用程式及應用程式信譽度。

平台及部署

Windows 桌上型電腦：

- MS Windows XP 32 位 Service Pack 3
- MS Vista 32/64 位 Service Pack 1
- MS Windows 7 32/64 位
- MS Windows 8 及 8.1 32/64 位
- MS Windows 10

Windows 伺服器：

- MS Windows Server 2003 32/64 位
- MS Windows Server 2008 32/64 位
- MS Windows Server 2008 R2
- MS Windows Server 2012
- MS Windows Server 2012 R2
- MS Windows Server 2014
- MS Windows Server 2016

Mac

- El Capitan 10.11
- Sierra 10.12
- High Sierra 10.13

部署選項

- 本地伺服器
- 軟體即服務

挑戰

在攻擊者成功躲過您的周邊及終端設備資安措施後，您只能依賴偵測技術來快速應對，防止攻擊蔓延。攻擊者會竊取憑證、獲得更大的特權、在網路中暢行無阻、尋找寶貴資訊。在終端設備上實施特權安全保護措施可減小攻擊面，是您的資安計畫的基本組成部分，可幫助增強桌上型電腦、筆記型電腦及伺服器安全，進而降低攻擊風險及可能造成企業的潛在危害。然而，此做法的負面影響是可能會影響到使用者工作效率、增加桌面支援團隊的工作負擔及相關成本。

若想有效率減小攻擊面、降低發生重大資料外洩事件的風險而不影響工作效率，企業應實施適當的工具，在終端設備上強制實施特權安全保護措施，來防範並防止攻擊範圍擴大。企業應實施適合業務及管理者使用者的靈活最小特權原則，控制允許執行的應用程式，確保可以偵測並阻止針對常見首要目標（即憑證）發起的攻擊。如果沒有這種工具，企業將面臨多方面的挑戰：

- 企業工作效率降低。在企業撤銷業務使用者的所有特權後，使用者再也不能高效率完成特定任務或使用日常工作所需的特定應用程式。缺乏靈活性的特權原則可能會導致企業業務營運陷入中斷。
- 很高的技術支援成本。在 IT 原則使業務使用者無法完成必要的日常任務時，使用者不得不呼叫技術支援來恢復必要的權限。這樣就會大幅增加 IT 成本，並使支援團隊不堪重負。
- 「特權蠕變」（privilege creep）引發的更大資安風險。在企業撤銷業務使用者的所有特權後，IT 團隊有時候將需要重新授予特權給使用者，讓使用者可完成具體任務。然而，重新授予的特權很少被收回，因而與過大管理權限相關的安全性漏洞再次暴露。
- 成功的惡意軟體攻擊造成更大風險。對於最大幅度削弱 Windows 設備使用者特權的企業，仍可能受到不需要特權即可執行的惡意軟體侵擾。如果沒有補充工具來控制允許執行的應用程式並保護攻擊者的主要目標——憑證，攻擊者就可以成功地利用惡意軟體攻擊來入侵到公司內部。

解決方案

CyberArk 終端特權管理器可協助消除實施最小特權的障礙，允許企業阻止或遏制終端設備上的攻擊、降低資訊被盜或被加密然後勒索的風險。結合特權管理、應用程式控制及針對性憑證竊取防護，可以有效地阻止入口終端設備上的有破壞性攻擊並防止攻擊蔓延。未知的應用程式以受限制的模式執行，以控制攻擊威脅，而憑證竊取防護可防止憑證竊取企圖。這些重要的保護方法作為單一代理部署，可增強及有效保護所有桌上型電腦、筆記型電腦及伺服器。

CyberArk 終端特權管理器亦可以幫助資安團隊為 IT 管理者實施精細最小特權原則，進而幫助企業有效地劃分 Windows 伺服器上的職責。為了補充這些特權控制措施，該解決方案還交付應用程式控制功能，可管理及控制允許在終端設備及伺服器上執行哪些應用程式。

運用 CyberArk 終端特權管理器，企業可以：

- 根據業務要求自動建立原則。根據 SCCM、軟體分發程式 (software distributor)、更新程式 (updater)、URL 等受信任來源（Trusted Sources）來建立應用程式控制及特權升級原則。原則範本（Policy Template）可協助針對特定伺服器類型（如 Microsoft SQL Server）實現快速實施，進而節約時間，幫助所有使用者角色填補特權安全性原則方面的空白。

規範

全面的應用程式支援：

- 可執行腳本
- MSI，MSU
- 管理任務
- 管理主控台外掛程式
- 腳本
- 登錄設定
- ActiveX 控制項
- COM 物件
- Web 應用程式

靈活且安全的應用程式規則：

- 檔案路徑匹配
- 命令列匹配
- 檔案雜湊（File hashing）（SHA-1）
- 產品及檔案資訊
- 受信任發行者（Trusted publisher）
- 受信任來源 SCCM
- 受信任軟體分發系統
- 受信任更新程式
- 受信任網路
- 受信任電腦映像
- 受信任 AD 群組
- 受信任產品
- 受信任 URL

以下項目的憑證保護：

- Windows Credential Manager
- Local Security Authority（LSA）
- Local Security Authority Subsystem Service（LSASS）
- Security Account Manager（SAM）
- Domain Credentials Cache（msvcachedv2）
- AD Directory Data Store（NTDS.dit）
- Virtual Secure Module（包括安全模式）
- Crypto RSA 機器金鑰
- AWS 金鑰
- Internet Explorer
- Microsoft Edge
- Chrome
- Firefox
- SQL Server Management Studio（SSMS）
- Quest Toad
- Remote Desktop Connection Manager
- FileZilla
- MRemoteNG

附註：某些功能可能不能用於所有部署及 OS 選項

- **實施適合 Windows 管理者的精細最小特權原則。**資安團隊根據具體角色來以精細方式控制允許每個 IT 管理者在 Windows 伺服器上執行的命令及任務。
- **安全地管理本機管理者。**使用來自 CyberArk 企業密碼金庫的受保護憑證來在本機管理終端設備特權帳戶，不管是在網路內還是網路外。
- **在需要時無縫地升級業務使用者特權。**撤銷業務使用者的本機管理者權限後，CyberArk 終端特權管理器可在受信任應用程式需要時根據原則來升級特權。
- **快速識別並阻止惡意應用程式。**利用 CyberArk 的應用程式風險分析來快速判定與任何應用程式相關的風險，可簡化原則定義，輔助阻止在環境中執行惡意應用程式。
- **偵測並阻止憑證竊取企圖。**憑證竊取在任何攻擊中都扮演著重要角色。進階保護可幫助企業偵測並阻止企圖竊取 Windows 憑證及常用網路瀏覽器中保存的憑證的行為。
- **立即可用的防勒索軟體功能。**OOTB 原則定義可防止惡意軟體攻擊，包括使用數十萬種惡意軟體樣本進行測試的最小特權控制。
- **允許未知應用程式以受限制模式安全地執行。**未知應用程式既不受信任，也不能肯定一定是惡意的。這些應用程式能夠以「受限制模式」執行，防止應用程式存取企業資源、敏感性資料或網際網路。
- **利用與威脅偵測工具的整合來分析未知應用程式。**CyberArk 終端特權管理器可將未知應用程式發送給 Check Point、FireEye 及 Palo Alto Networks 威脅偵測解決方案，幫助進行自動檔案分析。
- **識別環境中的所有應用程式。**利用每個受保護機器上的代理程式，該解決方案可以立即找到整個環境中某種應用程式的所有實例及每個應用程式的來源。

優勢

- 提供關鍵保護層，防止攻擊者避開傳統周邊及終端資安控制裝置
- 獨特的技術組合，可抵抗、阻止及控制終端設備上的攻擊，減輕對企業的潛在危害
- 增強您現有終端安全解決方案的保護及偵測功能
- 使桌面團隊可輕鬆實施安全性原則，同時最大幅度減少對業務的影響
- 防止使用者安裝未經批准的應用程式，避免造成工作站不穩定、增加技術支援呼叫及支援成本
- 在不降低使用者工作效率及增加技術支援呼叫的情況下撤銷擁有本機管理者權限的業務使用者
- 保護並更替本機管理者密碼，而不受終端設備位置影響
- 自動化原則建立可幫助輕鬆完成部署；OOTB 原則範本可簡化桌面 IT 團隊的負擔，而獨立代理可提供對氣隙（airgap）網路的支援
- 幫助桌面團隊滿足資安 / 風險管理團隊的要求，同時減輕團隊的工作負擔
- 控制惡意軟體在整個網路中的蔓延，縮短修復時間並減輕工作量

功能全方位解決方案

CyberArk 終端特權管理器是 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是一款全方位解決方案，旨在積極主動地防止利用管理特權來進入企業核心、竊取敏感性資料及毀壞關鍵系統的進階攻擊。該解決方案可幫助企業消除不必要的本機管理者特權並增強特權帳戶安全性，進而減小攻擊面。該解決方案包含的各種產品可獨立進行管理，也可組合形成一款連貫且全方位特權帳戶安全解決方案。