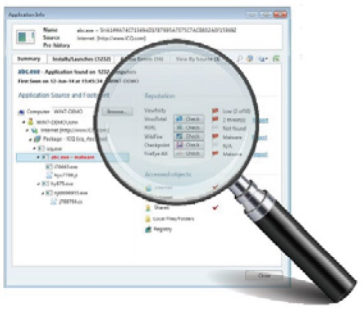
終端特權管理器

在終端上強制執行特殊權限安全，而不會造成取消本機管理者權限的負面影響。



在單一位置查看所有權限原則、應用程式及應用程式信譽。

挑戰

如果攻擊突破疆界及終端的安全防護，您可以依賴偵測技術做出快速回應，嘗試阻止攻擊擴散。攻擊者會竊取憑證，提升權限並在整個網路暢行無阻，查找重要資訊。在終端上強制執行特權安全以減少受攻擊面是安全計畫的基本組成部分。但是，此做法的缺點在於可能會影響使用者工作效率，增加 Windows 終端支援團隊的負擔並導致相關的成本。

為了有效減少受攻擊面，降低嚴重資料外洩風險，而不影響工作效率，企業應利用工具在終端上強制執行特權安全，以阻止及遏制攻擊。他們應對業務及管理者套用彈性的最小權限原則，控制應允許哪些應用程式執執行，並確保能夠偵測並阻止針對首要目標 - 憑證及帳密 - 的攻擊。如果不採用這類工具，企業將面臨各種挑戰：

- **企業工作效率下滑**。如果企業取消業務使用者的所有特權，使用者可能無法再執行某些任務，或使用其履行日常職責所需的應用程式。如果權限原則缺乏靈活性，可能會導致業務陷入停頓。
- **技術支援成本增加**。如果 IT 原則導致業務使用者無法執行必要的日常任務，使用者必須致電技術支援部門以復原所需的權限。這可能會顯著提高 IT 成本，使支援團隊應接不暇。
- **「特殊權限蠕變」導致的安全風險增加**。如果企業取消業務使用者的所有特殊權限，某些時候，IT 團隊將需要為特定任務重新授予特權。但是，重新授予的特權極少被撤銷，這再次導致管理權限過高相關的安全性漏洞。
- **面臨惡意軟體攻擊的風險增加**。即使企業最大幅度減小 Windows 設備上的使用者特殊權限，Windows 設備仍然易於受到不需要特權即可執執行的惡意軟體的攻擊。如果不採用互補性工具來控制應允許哪些應用程式執行並保護被攻擊的主要目標，攻擊者就可以成功利用惡意軟體攻擊以侵入企業內部。

解決方案

CyberArk 終端特權保護器 (Endpoint Privilege Manager) 有助於消除這類障礙，強制執行最小權限，並允許企業在終端上阻止及遏制攻擊，從而降低資訊被竊取或惡意加密並以此為要脅來索取贖金的風險。特權安全加上應用程式控制能夠降低感染惡意軟體的風險。未知應用程式將在受限模式下執行，以遏制威脅，而行為分析可阻止嘗試竊取憑證及帳密的不執行為。這些至關重要的保護技術均可於單一 Agent 部署完成，以強化現有終端的安全性。

CyberArk 終端特權管理器還可幫助安全團隊對 IT 管理者強制執行精細的最小權限原則，幫助企業在 Windows 伺服器上有效劃分職責。憑藉這些特權控制，該解決方案還可強制執行應用程式控制，對允許管理及控制終端及伺服器上執行的應用程式管理更輕鬆。

為什麼選擇 CyberArk ？

CyberArk 致力於協助企業在被迫停止業務之前阻止網路攻擊，是值得您信賴的業界專家。

使用 CyberArk 終端特權管理器，企業可以：

- **根據業務需求制定原則。**根據受信任的來源（如 SCCM、軟體發布者、更新程式等）制定應用程式控制及權限提高原則。
- **對 Windows 管理者強制執行精細的最小權限原則。**安全團隊可以進行精細控制，根據角色確定允許每名 IT 管理者在 Windows 伺服器上執行的命令及任務。
- **根據需要無縫提升業務使用者的特殊權限。**取消業務使用者的本機管理者權限後，CyberArk 終端特權管理器將根據受信任的應用程式的要求、依據原則提升其權限。
- **快速確定並阻止惡意應用程式。**自動比較未知應用程式與商用黑名單資料庫（如 VirusTotal 及 NSRL），更快確定已知的惡意軟體並更新全域原則，以防止這些應用程式在環境中執行。
- **偵測並阻止嘗試竊取憑證及帳密的行為。**竊取憑證是任何攻擊中的重要一環。行為分析有助於企業偵測並阻止嘗試竊取憑證的行為，保護 Windows 憑證及儲存在常用 Web 瀏覽器中的帳密。
- **允許未知應用程式在受限模式下安全執行。**未知應用程式（既不受信任，也無法確定其是否為惡意程式）可以在「受限模式」下執行，防止未知應用程式存取公司資源、敏感性資料或網際網路。
- **充分利用已整合的威脅偵測工具來分析未知應用程式。**CyberArk 終端特權管理器可以將未知應用程式發送到 Check Point、FireEye 及 Palo Alto Networks 威脅偵測解決方案，以自動執行檔案分析。
- **確定環境中的所有應用程式。**該解決方案可以透過在每台受保護的機器上的 Agent，立即定位環境中的所有應用程式實例及其來源。

優勢

- 在攻擊者突破傳統疆界及終端安全控制時提供額外的關鍵保護層
- 獨特的技術組合可防範、阻止並遏制針對終端的攻擊，減少可能的業務損失
- 增強現有終端安全性解決方案的保護及偵測能力
- 幫助用戶端支援團隊輕鬆實作安全性原則，儘可能降低企業可能受到的影響
- 防止使用者因為安裝未經批准的應用程式而造成工作站不穩定，造成需要聯繫技術服務部門而增加支援成本
- 取消本機管理者權限，而不會降低使用者工作效率，且不會導致技術支援工作量增加
- 透過制定原則輕鬆完成部署，減輕用戶端支援團隊的負擔
- 幫助用戶端支援團隊滿足安全 / 風險管理團隊的要求，同時減少其工作量
- 防止惡意軟體在網路中蔓延，從而縮減補救時間及工作量

全方位解決方案

CyberArk 終端特權管理器是 CyberArk 特權帳號安全解決方案的一部分，這個全方位的解決方案可主動防範利用 IT 管理者特殊權限存取企業核心設備、竊取敏感性資料並破壞關鍵系統的複雜攻擊。該解決方案可幫助企業取消不必要的本機管理者特權並強化特權帳號的安全性，進而減少企業的受攻擊面。該解決方案中的產品可進行獨立管理，也可以作為統一的全方位特權帳號安全解決方案進行集中管理。

規格

支援的平台：

Windows 用戶端：

- Windows 7 32 位元和 64 位元
- Windows 8 32 位元和 64 位元
- Windows 8.1 32 位元和 64 位元
- Windows 10

Windows Server：

- Windows Server 2008 32 位元和 64 位元
- Windows Server 2008 R2 64 位元
- Windows Server 2012
- Windows Server 2012 R2

全面的應用程式支援：

- 可執行檔
- MSI、MSU
- 排程任務
- 嵌入式管理主控台
- 程式碼
- Registry 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：

- 檔案路徑比對
- 命令列比對
- 檔案雜湊（SHA-1）
- 產品及檔案資訊
- 受信任的發佈者
- 受信任的來源 SCCM
- 受信任的軟體發佈系統
- 受信任的更新程式
- 受信任的網路
- 受信任的電腦映像
- 受信任的 AD 群組
- 受信任的產品

部署選項：

- Microsoft 群組原則（GPO）
- 本機伺服器
- Software as a Service

註：某些功能可能不可用於所有部署選項